ASCENTRUST LLC
The POWER of ENGINEERING

GLOSSARY OF TERMS
FOR ENCRYPTION
AND
NETWORK SECURITY

ENCRYPTION AND INTERNET SECURITY GLOSSARY

This document is an extensive reference that should help the principals and strategic partners of **IDFS, INC.** and **Advanced Software Development, Inc.** improve the clarity of documentation and discussion in this very important area of Internet technology. This is the area of internet and networking security. However, readers should be aware of the following:

1. The recommendations and some particular interpretations in definitions are those of the senior engineer and reflect his long history in the telephone industry. In other words, the usage rules, wording interpretations, and other recommendations that the Glossary offers are personal opinions of the Glossary's author.

2. The glossary is rich in the history of early network security work, but it may be somewhat incomplete in describing recent security work, which has been developing rapidly.

This Glossary provides definitions, abbreviations, and explanations of terminology for information system security. This document offers recommendations to improve the comprehensibility of written material that is generated in the development of a business model and plan for **IDFS, ASD** and the **Azera Group.** The recommendations will also be used in the development of the **Interlok Encryption Technology.** The recommendations follow the principles that such writing should

(a) Use the same term or definition whenever the same concept is mentioned;

(b) Use terms in their plainest, dictionary sense;

(c) Use terms that are already well-established in open publications; and

(d) Avoid terms that either favor a particular vendor or favor a particular technology or mechanism over other, competing techniques that already exist or could be developed.

3. Format of Entries: Glossary entries are listed in the following manner:

3.1. Order of Entries

Entries are sorted in lexicographic order, without regard to capitalization. Numeric digits are treated as preceding alphabetic characters, and special characters are treated as preceding digits. Blanks are treated as preceding non-blank characters, except that a hyphen or slash between the parts of a multiword entry (e.g., "RED (BLACK separation") is treated like a blank. If an entry has multiple definitions (e.g., "domain"), they are numbered beginning with "1", and any of those multiple definitions that are RECOMMENDED for use in DOCUMENTs are presented before other definitions for that entry. If definitions are closely related (e.g. "threat"), they are denoted by adding letters to a number, such as "1a" and "1b".

3.2. Definition Substitutions

Some terms have a definition published by a non-Internet authority --a government (e.g., "object reuse"), an industry (e.g., "Secure Data Exchange"), a national authority (e.g., "Data Encryption Standard"), or an international body (e.g., "data confidentiality") -- that is suitable for use in our documents. In those cases, this Glossary is recommending its use in our internal and external documents. When making substitutions, this Glossary attempts to avoid contradicting any non-Internet authority. Still, terminology differs between authorities such as the American Bar Association, OSI, SET, the U.S. DoD, and other authorities; and this Glossary probably is not exactly aligned with any of them.

4. Definitions

A1 computer system: See: Tutorial under "Trusted Computer System

ABA Guidelines: "American Bar Association (ABA) Digital Signature Guidelines" [DSG], a framework of legal principles for using digital signatures and digital certificates in electronic commerce.

Abstract Syntax Notation One (ASN.1): A standard for describing data objects. [Larm, X680] (See: CMS.)

Usage: Documents SHOULD use the term "ASN.1" narrowly to describe the notation or language called "Abstract Syntax Notation One". Engineers MAY use the term more broadly to encompass the notation, its associated encoding rules (see: BER), and software tools that assist in its use, when the context makes this meaning clear.

Tutorial: OSI-RM defines computer network functionality in layers. Protocols and data objects at higher layers are abstractly defined to be implemented using protocols and data objects from lower layers. A higher layer may define transfers of abstract objects between computers, and a lower layer may define those transfers concretely as strings of bits. Syntax is needed to specify data formats of abstract objects, and encoding rules are needed to transform abstract objects into bit strings at lower layers. OSI standards use ASN.1 for those specifications and use various encoding rules for those transformations. (See: BER.)

ACC: See: access control center.

Acceptable risk: A risk that is understood and tolerated by a system's user, operator, owner, or accreditor, usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss. (See: adequate security, risk, "second law" under "Courtney's laws".)

Access: The ability and means to communicate with or otherwise interact with a system to use system resources either to handle information or to gain knowledge of the information the system contains. (Compare: handle.) Usage: The definition is intended to include all types of communication with a system, including one-way communication in either direction. In actual practice, however, passive users might be treated as not having "access" and, therefore, be exempt from most requirements of the system's security policy. (See: "passive user" under "user".)

Access Certificate for Electronic Services (ACES): A PKI operated by the U.S. Government's General Services Administration in cooperation with industry partners. (See: CAM.)

Access control:

1. Protection of system resources against unauthorized access.

2. A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.

3. (formal model) Limitations on interactions between subjects and objects in an information system.

4. "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner."

5. (U.S. Government) A system using physical, electronic, or human controls to identify or admit personnel with properly authorized access to a SCIF.

Access control center (ACC): A computer that maintains a database (possibly in the form of an access control matrix) defining the security policy for an access control service, and that acts as a server for clients requesting access control decisions.

Tutorial: An ACC is sometimes used in conjunction with a key center to implement access control in a key-distribution system for symmetric cryptography. (See: BLACKER, Kerberos.)

Access control list (ACL): Information system: A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. (Compare: access control matrix, access list, access profile, capability list.)

Access control matrix: A rectangular array of cells, with one row per subject and one column per object. The entry in a cell -- that is, the entry for a particular subject-object pair -- indicates the access mode that the subject is permitted to exercise on the object. Each column is equivalent to an "access control list" for the object; and each row is equivalent to an "access profile" for the subject.

Access control service: A security service that protects against a system entity using a system resource in a way not authorized by the system's security policy. (See: access control, discretionary access control, identity-based security policy, mandatory access control, rule-based security policy.)

Tutorial: This service includes protecting against use of a resource in an unauthorized manner by an entity (i.e., a principal) that is authorized to use the resource in some other manner. (See: insider.) The two basic mechanisms for implementing this service are ACLs and tickets.

Access level:

1. Synonym for the hierarchical "classification level" in a security level. [C4009] (See: security level.)

2. Synonym for "clearance level".

Access list: (physical security) Roster of persons who are authorized to enter a controlled area. (Compare: access control list.)

Access mode: A distinct type of data processing operation (e.g., read, write, append, or execute, or a combination of operations) that a subject can potentially perform on an object in an information system.

Access policy: A kind of "security policy". (See: access, access control.)

Access profile: Synonym for "capability list".

Access right: Synonym for "authorization"; emphasizes the possession of the authorization by a system entity.

Accountability: The property of a system or system resource that ensures that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions.

Tutorial: Accountability (a.k.a. individual accountability) typically requires a system ability to positively associate the identity of a user with the time, method, and mode of the user's access to the system. This ability supports detection and subsequent investigation of security breaches. Individual persons who are system users are held accountable for their actions after being notified of the rules of behavior for using the system and the penalties associated with violating those rules.

Accounting See: COMSEC accounting.

Accounting legend code (ALC): (U.S. Government) Numeric system used to indicate the minimum accounting controls required for items of COMSEC material within the CMCS. [C4009] (See: COMSEC accounting.)

Accreditation: An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. (See: certification.)

Tutorial: An accreditation is usually based on a technical certification of the system's security mechanisms. To accredit a system, the approving authority must determine that any residual risk is an acceptable risk. Although the terms "certification" and "accreditation" are used more in the U.S. DoD and other U.S. Government agencies than in commercial organizations, the concepts apply any place where managers are required to deal with and accept responsibility for security risks.

Accreditation boundary: Synonym for "security perimeter".

Accreditor: A management official who has been designated to have the formal authority to "accredit" an information system, i.e., to authorize the operation of, and the processing of sensitive data in, the system and to accept the residual risk associated with the system. (See: accreditation, residual risk.)

ACES: See: Access Certificate for Electronic Services.

ACL: See: access control list.

Acquirer:

1. The financial institution that establishes an account with a merchant and processes payment card authorizations and payments.
2. The institution (or its agent) that acquires from the card acceptor the financial data relating to the transaction and initiates that data into an interchange system.

Activation data: Secret data, other than keys, that is required to access a cryptographic module. (See: CIK. Compare: initialization value.)

Active attack: See: secondary definition under "attack".

Active content:

1. Executable software that is bound to a document or other data file and that executes automatically when a user accesses the file, without explicit initiation by the user. (Compare: mobile code.)

   Tutorial: Active content can be mobile code when its associated file is transferred across a network.

2. Electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user. This technology enables mobile code associated with a document to execute as the document is rendered.

Active user: See: secondary definition under "system user".

Active wiretapping: A wiretapping attack that attempts to alter data being communicated or otherwise affect data flow. (See: wiretapping. Compare: active attack, passive wiretapping.)

Add-on security: The retrofitting of protection mechanisms, implemented by hardware or software, in an information system after the system has become operational.

Adequate security: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." (See: acceptable risk, residual risk.)

Administrative security:

1. Management procedures and constraints to prevent unauthorized access to a system. (See: "third law" under "Courtney's laws", manager, operational security, procedural security, security architecture. Compare: technical security.)

   Usage: Administrative security is usually understood to consist of methods and mechanisms that are implemented and executed primarily by people, rather than by automated systems.

2. The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data.

Administrator

1. A person that is responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. (See: administrative security.)

2. A person in contact with the TOE, who is responsible for maintaining its operational capability.

Advanced Encryption Standard (AES): (N) A U.S. Government standard (the successor to DES) that (a) specifies "the AES algorithm", which is a symmetric block cipher that is based on Rijndael and uses key sizes of 128, 192, or 256 bits to operate on a 128-bit block, and (b) states policy for using that algorithm to protect unclassified, sensitive data.

Tutorial: Rijndael was designed to handle additional block sizes and key lengths that were not adopted in the AES. Rijndael was selected by NIST through a public competition that was held to find a successor to the DEA; the other finalists were MARS, RC6, Serpent, and Twofish.

Adversary

1. An entity that attacks a system. (Compare: cracker, intruder, hacker.)

2. An entity that is a threat to a system.

AES: See: Advanced Encryption Standard.

Affirm: A formal methodology, language, and integrated set of software tools developed at the University of Southern California's Information Sciences Institute for specifying, coding, and verifying software to produce correct and reliable programs.

Aggregation: A circumstance in which a collection of information items is required to be classified at a higher security level than any of the items is classified individually.

AH: See: Authentication Header

Air gap: An interface between two systems at which

(a) they are not connected physically and

(b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control). (See: sneaker net. Compare: gateway.)

Example: Computer A and computer B are on opposite sides of a room. To move data from A to B, a person carries a disk across the room. If A and B operate in different security domains, then moving data across the air gap may involve an upgrade or downgrade operation.

ALC: See: accounting legend code.

Algorithm: A finite set of step-by-step instructions for a problem solving or computation procedure, especially one that can be implemented by a computer. (See: cryptographic algorithm.)

Alias: A name that an entity uses in place of its real name, usually for the purpose of either anonymity or masquerade.

American National Standards Institute (ANSI): A private, not-for-profit association that administers U.S.private-sector voluntary standards.

Tutorial: ANSI has approximately 1,000 member organizations, including equipment users, manufacturers, and others. ANSI is the sole U.S. representative to :

(a) ISO and

(b) (via the U.S. National Committee) the International Electro-technical Commission (IEC), which are the two major, non-treaty, international standards organizations. ANSI provides a forum for ANSI-accredited standards development groups. Among those groups, the following are especially relevant to Internet security:

- International Committee for Information Technology Standardization (INCITS) (formerly X3): Primary U.S. focus of standardization in information and communications technologies, encompassing storage, processing, transfer, display, management, organization, and retrieval of information.

- Accredited Standards Committee X9: Develops, establishes, maintains, and promotes standards for the financial services industry.
- Alliance for Telecommunications Industry Solutions (ATIS): Develops standards, specifications, guidelines, requirements, technical reports, industry processes, and verification tests for interoperability and reliability of telecommunications networks, equipment, and software. Example:

American Standard Code for Information Interchange (ASCII): A scheme that encodes 128 specified characters -- the numbers 0-9, the letters a-z and A-Z, some basic punctuation symbols, some control codes that originated with Teletype machines, and a blank space -- into the 7-bit binary integers. Forms the basis of the character set representations used in most computers and many Internet standards.

Anderson report: A 1972 study of computer security that was written by James P. Anderson for the U.S. Air Force.

Tutorial: Anderson collaborated with a panel of experts to study Air Force requirements for multilevel security. The study recommended research and development that was urgently needed to provide secure information processing for command and control systems and support systems. The report introduced the reference monitor concept and provided development impetus for computer and network security technology. However, many of the security problems that the 1972 report called "current" still plague information systems today.

Anomaly detection: An intrusion detection method that searches for activity that is different from the normal behavior of system entities and system resources. (See: IDS. Compare: misuse detection.)

Anonymity: The condition of an identity being unknown or concealed. (See: alias, anonymizer, anonymous credential, anonymous login, identity, onion routing, persona certificate. Compare: privacy.)

Tutorial: An application may require security services that maintain anonymity of users or other system entities, perhaps to preserve their privacy or hide them from attack. To hide an entity's real name, an alias may be used; for example, a financial institution may assign account numbers. Parties to transactions can thus remain relatively anonymous, but can also accept the transactions as legitimate. Real names of the parties cannot be easily determined by observers of the transactions, but an authorized third party may be able to map an alias to a real name, such as by presenting the institution with a court order. In other applications, anonymous entities may be completely untraceable.

Anonymizer: An internetwork service, usually provided via a proxy server, that provides anonymity and privacy for clients. That is, the service enables a client to access servers

(a) without allowing anyone to gather information about which servers the client accesses and

(b) without allowing the accessed servers to gather information about the client, such as its IP address.

Anonymous credential: U.S. Government: A credential that

(a) can be used to authenticate a person as having a specific attribute or being a member of a specific group (e.g., military veterans or U.S. citizens) but

(b) does not reveal the individual identity of the person that presents the credential.

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it mixes concepts in a potentially misleading way. For example, when the credential is an X.509 certificate, the term could be misunderstood to mean that the certificate was signed by a CA that has a persona certificate. Instead, use "attribute certificate", "organizational certificate", or "persona certificate" depending on what is meant, and provide additional explanations as needed.

Anonymous login: An access control feature (actually, an access control vulnerability) in many Internet hosts that enables users to gain access to general-purpose or public services and resources of a host (such as allowing any user to transfer data using FTP) without having a pre-established, identity-specific account (i.e., user name and password). (See: anonymity.)

Tutorial: This feature exposes a system to more threats than when all the users are known, pre-registered entities that are individually accountable for their actions. A user logs in using a special, publicly known user name (e.g., "anonymous", "guest", or "ftp"). To use the public login name, the user is not required to know a secret password and may not be required to input anything at all except the name. In other cases, to complete the normal sequence of steps in a login protocol, the system may require the user to input a matching, publicly known password (such as "anonymous") or may ask the user for an e-mail address or some other arbitrary character string.

ANSI: See: American National Standards Institute.

Anti-jam: "Measures ensuring that transmitted information can be received despite deliberate jamming attempts." (See: electronic security, frequency hopping, jam, spread spectrum.)

Apex trust anchor: The trust anchor that is superior to all other trust anchors in a particular system or context. (See: trust anchor, top CA.)

API: See: application programming interface.

APOP: See: POP3 APOP.

Application Layer: See: Internet Protocol Suite, OSI-RM.

Application program: A computer program that performs a specific function directly for a user (as opposed to a program that is part of a computer operating system and exists to perform functions in support of application programs).

Architecture: See: security architecture, system architecture.

Archive:

A. (noun) A collection of data that is stored for a relatively long period of time for historical and other purposes, such as to support audit service, availability service, or system integrity service. (Compare: backup, repository.)

B. (verb) To store data in such a way as to create an archive. (Compare: back up.)

Tutorial: A digital signature may need to be verified many years after the signing occurs. The CA -- the one that issued the certificate containing the public key needed to verify that signature -- may not stay in operation that long. So every CA needs to provide for long-term storage of the information needed to verify the signatures of those to whom it issues certificates.

ARPANET: Advanced Research Projects Agency (ARPA) Network, a pioneer packet-switched network that:

A. Was designed, implemented, operated, and maintained by BBN from January 1969 until July 1975 under contract to the U.S. Government;

B. Was acknowledged as the leader to the development of today's Internet (The Senior Engineer disagrees with this view. The real internet started by the National Science Foundation came into existence in 1985 and connected five supercomputers across the country with the tcp/ip protocol.

C. Was decommissioned in June 1990,

ASCII: See: American Standard Code for Information Interchange.

ASN.1: See: Abstract Syntax Notation One.

Asset: A system resource that is

(a) required to be protected by an information system's security policy,

(b) intended to be protected by a countermeasure, or

(c) required for a system's mission.

Association: A cooperative relationship between system entities, usually for the purpose of transferring information between them. (See: security association.)

Assurance: See: security assurance

Assurance level: A rank on a hierarchical scale that judges the confidence someone can have that a TOE adequately fulfills stated security requirements. (See: assurance, certificate policy, EAL, TCSEC.)

Example: U.S. Government guidance [M0404] describes four assurance levels for identity authentication, where each level "describes the [U.S. Federal Government] agency's degree of certainty that the user has presented [a credential] that refers to [the user's] identity." In that guidance, assurance is defined as

(a) "the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued" and

(b) "the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued."

The four levels are described as follows:

- Level 1: Little or no confidence in the asserted identity.
- Level 2: Some confidence in the asserted identity.
- Level 3: High confidence in the asserted identity.
- Level 4: Very high confidence in the asserted identity.

Standards for determining these levels are provided in a NIST publication [SP12]. However, as noted there, an assurance level is "a degree of confidence, not a true measure of how secure the system actually is."

Asymmetric cryptography: A modern branch of cryptography (popularly known as "public key cryptography") in which the algorithms use a pair of keys (a public key and a private key) and use a different component of the pair for each of two counterpart cryptographic operations

Tutorial: Asymmetric algorithms have key management advantages over equivalently strong symmetric ones. First, one key of the pair need not be known by anyone but its owner; so it can more easily be kept secret. Second, although the other key is shared by all entities that use the algorithm, that key need not be kept secret from other, non-using entities; thus, the key-distribution part of key management can be done more easily. Asymmetric cryptography can be used to create algorithms for encryption, digital signature, and key agreement:

- In an asymmetric encryption algorithm (e.g., "RSA"), when Alice wants to ensure confidentiality for data she sends to Bob, she encrypts the data with a public key provided by Bob. Only Bob has the matching private key that is needed to decrypt the data.

- In an asymmetric digital signature algorithm (e.g., "DSA"), when Alice wants to ensure data integrity or provide authentication for data she sends to Bob, she uses her private key to sign the data (i.e., create a digital signature based on the data). To verify the signature, Bob uses the matching public key that Alice has provided.
- In an asymmetric key-agreement algorithm (e.g., "Diffie-Hellman-Merkle"), Alice and Bob each send their own public key to the other party. Then each uses their own private key and the other's public key to compute the new key value.

Asymmetric key: A cryptographic key that is used in an asymmetric cryptographic algorithm. (See: asymmetric cryptography, private key, public key.)

ATIS: See: "Alliance for Telecommunications Industry Solutions" under "ANSI".

Attack:

1. An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat. (See: penetration, violation, vulnerability.)
2. A method or technique used in an assault (e.g., masquerade). (See: blind attack, distributed attack.)

   Tutorial: Attacks can be characterized according to intent:

   - An "active attack" attempts to alter system resources or affect their operation.
   - A "passive attack" attempts to learn or make use of information from a system but does not affect system resources of that system. (See: wiretapping.) The object of a passive attack might be to obtain data that is needed for an off-line attack.
   - An "off-line attack" is one in which the attacker obtains data from the target system and then analyzes the data on a different system of the attacker's own choosing, possibly in preparation for a second stage of attack on the target.

   Attacks can be characterized according to point of initiation:

   - An "inside attack" is one that is initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by the party that granted the authorization.
   - An "outside attack" is initiated from outside the security perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Attacks can be characterized according to method of delivery:

- In a "direct attack", the attacker addresses attacking packets to the intended victim(s).
- In an "indirect attack", the attacker addresses packets to a third party, and the packets either have the address(es) of the intended victim(s) as their source address(es) or indicate the intended victim(s) in some other way. The third party responds by sending one or more attacking packets to the intended victim. The attacker can use third parties as attack amplifiers by providing a broadcast address as the victim address (e.g., "smurf attack"). (See: reflector attack.

Attack potential: The perceived likelihood of success should an attack be launched, expressed in terms of the attacker's ability (i.e., expertise and resources) and motivation. (Compare: threat, risk.)

Attack sensing, warning, and response: A set of security services that cooperate with audit service to detect and react to indications of threat actions, including both inside and outside attacks. (See: indicator.)

Attack tree: A branching, hierarchical data structure that represents a set of potential approaches to achieving an event in which system security is penetrated or compromised in a specified way.

Tutorial: Attack trees are special cases of fault trees. The security incident that is the goal of the attack is represented as the root node of the tree, and the ways that an attacker could reach that goal are iteratively and incrementally represented as branches and sub-nodes of the tree. Each sub-node defines a sub-goal, and each sub-goal may have its own set of further sub-goals, etc. The final nodes on the paths outward from the root, i.e., the leaf nodes, represent different ways to initiate an attack. Each node other than a leaf is either an AND-node or an OR-node. To achieve the goal represented by an AND-node, the sub-goals represented by all of that node's sub-nodes must be achieved; and for an OR-node, at least one of the sub-goals must be achieved.

Attribute: Information of a particular type concerning an identifiable system entity or object. An "attribute type" is the component of an attribute that indicates the class of information given by the attribute; and an "attribute value" is a particular instance of the class of information indicated by an attribute type. (See: attribute certificate.)

Attribute authority (AA):

1. A CA that issues attribute certificates.
2. "An authority [that] assigns privileges by issuing attribute certificates." [X509]

Attribute certificate:

1. A digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate. (See: capability token.)
2. "A data structure, digitally signed by an [a]ttribute [a]uthority, that binds some attribute values with identification information about its holder." [X509]

Tutorial: A public-key certificate binds a subject name to a public key value, along with information needed to perform certain cryptographic functions using that key. Other attributes of a subject, such as a security clearance, may be certified in a separate kind of digital certificate, called an attribute certificate. A subject may have multiple attribute certificates associated with its name or with each of its public-key certificates. An attribute certificate might be issued to a subject in the following situations:

- **Different lifetimes:** When the lifetime of an attribute binding is shorter than that of the related public-key certificate, or when it is desirable not to need to revoke a subject's public key just to revoke an attribute.
- **Different authorities**: When the authority responsible for the attributes is different than the one that issues the public-key certificate for the subject. (There is no requirement that an attribute certificate be issued by the same CA that issued the associated public-key certificate.)

Audit: See: security audit.

Audit log: Synonym for "security audit trail".

Audit service: A security service that records information needed to establish accountability for system events and for the actions of system entities that cause them. (See: security audit.)

Audit trail: See: security audit trail.

AUTH: See: POP3 AUTH.

Authenticate: Verify (i.e., establish the truth of) an attribute value claimed by or for a system entity or system resource. (See: authentication, validate vs. verify, "relationship between data integrity service and authentication services" under "data integrity service".)

Deprecated Usage: In general English usage, this term is used with the meaning "to prove genuine" (e.g., an art expert authenticates a Michelangelo painting); but our documents should restrict usage as follows:

- WE SHOULD NOT use this term to refer to proving or checking that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. Instead, use "verify".

- WE SHOULD NOT use this term to refer to proving the truth or accuracy of a fact or value such as a digital signature. Instead, use "verify".
- WE SHOULD NOT use this term to refer to establishing the soundness or correctness of a construct, such as a digital certificate. Instead, use "validate".

Authentication: The process of verifying a claim that a system entity or system resource has a certain attribute value. (See: attribute, authenticate, authentication exchange, authentication information, credential, data origin authentication, peer entity authentication, "relationship between data integrity service and authentication services" under "data integrity service", simple authentication, strong authentication, verification, X.509.)

Tutorial: Security services frequently depend on authentication of the identity of users, but authentication may involve any type of attribute that is recognized by a system. A claim may be made by a subject about itself (e.g., at login, a user typically asserts its identity) or a claim may be made on behalf of a subject or object by some other system entity (e.g., a user may claim that a data object originates from a specific source, or that a data object is classified at a specific security level).

An authentication process consists of two basic steps:

- **Identification step**: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem.
- **Verification step**: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed. (See: verification.)

Authentication code: Synonym for a checksum based on cryptography. (Compare: Data Authentication Code, Message Authentication Code.)

Deprecated Term: DOCUMENTS SHOULD NOT use this uncapitalized term as a synonym for any kind of checksum, regardless of whether or not the checksum is cryptographic. Instead, use "checksum", "Data Authentication Code", "error detection code", "hash", "keyed hash", "Message Authentication Code", "protected checksum".

The term mixes concepts in a potentially misleading way. The word "authentication" is misleading because the checksum may be used to perform a data integrity function rather than a data origin authentication function.

Authentication exchange:

1. A mechanism to verify the identity of an entity by means of information exchange.
2. "A mechanism intended to ensure the identity of an entity by means of information exchange."

Authentication Header (AH): An Internet protocol designed to provide connectionless data integrity service and connectionless data origin authentication service for IP datagrams, and (optionally) to provide partial sequence integrity and protection against replay attacks. (See: IPsec. Compare: ESP.)

Tutorial: Replay protection may be selected by the receiver when a security association is established. AH authenticates the upper-layer PDU that is carried as an IP SDU, and also authenticates as much of the IP PCI (i.e., the IP header) as possible. However, some IP header fields may change in transit, and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. Thus, the values of such fields cannot be protected end-to-end by AH; protection of the IP header by AH is only partial when such fields are present. AH may be used alone, or in combination with the ESP, or in a nested fashion with tunneling. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a host and a gateway. ESP can provide nearly the same security services as AH, and ESP can also provide data confidentiality service. The main difference between authentication services provided by ESP and AH is the extent of the coverage; ESP does not protect IP header fields unless they are encapsulated by AH.

Authentication information: Information used to verify an identity claimed by or for an entity. (See: authentication, credential, user. Compare: identification information.)

Tutorial: Authentication information may exist as, or be derived from, one of the following:

(a) Something the entity knows (see: password);

(b) Something the entity possesses (see: token);

(c) Something the entity is (see: biometric authentication).

Authentication service: A security service that verifies an identity claimed by or for an entity. (See: authentication.)

Tutorial: In a network, there are two general forms of authentication service: data origin authentication service and peer entity authentication service.

Authenticity: The property of being genuine and able to be verified and be trusted. (See: authenticate, authentication, validate vs. verify.)

Authority: "An entity responsible for the issuance of certificates." Deprecated Usage: DOCUMENTS SHOULD NOT use this term as a synonym for attribute authority, certification authority, registration authority, or similar terms; the shortened form may cause confusion. Instead, use the full term at the first instance of usage and then, if it is necessary to shorten text, use AA, CA, RA, and other abbreviations defined in this Glossary.

Authority certificate: "A certificate issued to an authority (e.g. either to a certification authority or to an attribute authority)." (See: authority.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term because it is ambiguous. Instead, use the full term "certification authority certificate", "attribute authority certificate", "registration authority certificate", etc. at the first instance of usage and then, if it is necessary to shorten text, use AA, CA, RA, and other abbreviations defined in this Glossary.

Authority Information Access extension: The private extension defined by PKIX for X.509 certificates to indicate "how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data." (See: private extension.)

Authorization:

A. An approval that is granted to a system entity to access a system resource. (Compare: permission, privilege.) Usage: Some synonyms are "permission" and "privilege". Specific terms are preferred in certain contexts:

- (PKI) "Authorization" SHOULD be used, to align with "certification authority" in the standard [X509].
- (role-based access control) "Permission" SHOULD be used, to align with the standard [ANSI].
- (computer operating systems) "Privilege" SHOULD be used, to align with the literature. (See: privileged process, privileged user.)

Tutorial: The semantics and granularity of authorizations depend on the application and implementation (see: "first law" under "Courtney's laws"). An authorization may specify a particular access mode -- such as read, write, or execute -- for one or more system resources.

B. A process for granting approval to a system entity to access a system resource.

C. The process by which a properly appointed person or persons grants permission to perform some action on behalf of an organization. This process assesses transaction risk, confirms that a given transaction does not raise the account holder's debt above the account's credit limit, and reserves the specified amount of credit. (When a merchant obtains authorization, payment for the authorized amount is guaranteed -- provided, of course, that the merchant followed the rules associated with the authorization process.)

Authorization credential: See: (access control) under "credential".

Authorize: Grant an authorization to a system entity.

Authorized user: (access control) A system entity that accesses a system resource for which the entity has received an authorization. (Compare: insider, outsider, unauthorized user.)

Deprecated Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term is used in many ways and could easily be misunderstood.

Automated information system: See: information system.

Availability:

1. The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them. (See: critical, denial of service. Compare: precedence, reliability, survivability.)
2. The property of being accessible and usable upon demand by an authorized entity.
3. Timely, reliable access to data and information services for authorized users.

   Deprecated Definition: DOCUMENTS SHOULD NOT use the term with definition 3; the definition mixes "availability" with "reliability", which is a different property. (See: reliability.)

Tutorial: Availability requirements can be specified by quantitative metrics, but sometimes are stated qualitatively, such as in the following:

- "Flexible tolerance for delay" may mean that brief system outages do not endanger mission accomplishment, but extended outages may endanger the mission.
- "Minimum tolerance for delay" may mean that mission accomplishment requires the system to provide requested services in a short time.

Availability service: A security service that protects a system to ensure its **availability.**

Tutorial: This service addresses the security concerns raised by denial-of-service attacks. It depends on proper management and control of system resources, and thus depends on access control service and other security services.

Avoidance: See: secondary definition under "security".

B1, B2, or B3 computer system: (TCSEC) See: Tutorial under "Trusted Computer System Evaluation Criteria".

Back door:

1. (COMPUSEC) A computer system feature -- which may be:

   (a) An unintentional flaw,

(b) A mechanism deliberately installed by the system's creator, or

(c) A mechanism surreptitiously installed by an intruder -- that provides access to a system resource by other than the usual procedure and usually is hidden or otherwise not well-known. (See: maintenance hook. Compare: Trojan Horse.)

Example: A way to access a computer other than through a normal login. Such an access path is not necessarily designed with malicious intent; operating systems sometimes are shipped by the manufacturer with hidden accounts intended for use by field service technicians or the vendor's maintenance programmers.

2. (cryptography) A feature of a cryptographic system that makes it easily possible to break or circumvent the protection that the system is designed to provide.

Example: A feature that makes it possible to decrypt cipher text much more quickly than by brute-force cryptanalysis, without having prior knowledge of the decryption key.

Back up: (verb) Create a reserve copy of data or, more generally, provide alternate means to perform system functions despite loss of system resources. (See: contingency plan. Compare: archive.)

Backup: (noun or adjective) Refers to alternate means of performing system functions despite loss of system resources. (See: contingency plan).

Example: A reserve copy of data, preferably one that is stored separately from the original, for use if the original becomes lost or damaged. (Compare: archive.)

Bagbiter: (slang) An entity, such as a program or a computer, that fails to work or that works in a remarkably clumsy manner. A person who has caused some trouble, inadvertently or otherwise, typically by failing to program the computer properly.

Deprecated Term: It is likely that other cultures use different metaphors for these concepts. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term.

Baggage: (SET) An opaque encrypted tuple, which is included in a SET message but appended as external data to the PKCS encapsulated data. This avoids super-encryption of the previously encrypted tuple, but guarantees linkage with the PKCS portion of the message.

Deprecated Usage: DOCUMENTS SHOULD NOT use this term to describe a data element, except in the form "SET (trademark) baggage" with the meaning given above.

Baked-in security: The inclusion of security mechanisms in an information system beginning at an early point in the system's lifecycle, i.e., during the design phase, or at least early in the implementation phase. (Compare: add-on security.)

Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term (unless they also provide a definition like this one).

Bandwidth: The total width of the frequency band that is available to or used by a communication channel; usually expressed in Hertz (Hz). (RFC 3753) (Compare: channel capacity.)

Bank identification number (BIN):

1. The digits of a credit card number that identify the issuing bank. (See: primary account number.)
2. (SET) The first six digits of a primary account number.

Basic Encoding Rules (BER): A standard for representing ASN.1 data types as strings of octets. (See: Distinguished Encoding Rules.)

Deprecated Usage: Sometimes incorrectly treated as part of ASN.1. However, ASN.1 properly refers only to a syntax description language, and not to the encoding rules for the language.

Basic Security Option: See: secondary definition under "IPSO".

Bastion host: A strongly protected computer that is in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few) in the network that can be directly accessed from networks on the other side of the firewall. (See: firewall.)

Tutorial: Filtering routers in a firewall typically restrict traffic from the outside network to reaching just one host, the bastion host, which usually is part of the firewall. Since only this one host can be directly attacked, only this one host needs to be very strongly protected, so security can be maintained more easily and less expensively. However, to allow legitimate internal and external users to access application resources through the firewall, higher-layer protocols and services need to be relayed and forwarded by the bastion host. Some services (e.g., DNS and SMTP) have forwarding built in; other services (e.g., TELNET and FTP) require a proxy server on the bastion host.

BBN Technologies Corp. (BBN): The research-and-development company (originally called Bolt Baranek and Newman, Inc.) that built the ARPANET.

BCA: See: brand certification authority.

BCR: See: BLACK(Crypto)RED.

BCI: See: brand CRL identifier.

Bell-LaPadula model: A formal, mathematical, state-transition model of confidentiality policy for multilevel-secure computer systems. (Compare: Biba model, Brewer-Nash model.)

Tutorial: The model, devised by David Bell and Leonard LaPadula at The MITRE Corporation in 1973, characterizes computer system elements as subjects and objects. To determine whether or not a subject is authorized for a particular access mode on an object, the clearance of the subject is compared to the classification of the object. The model defines the notion of a "secure state", in which the only permitted access modes of subjects to objects are in accordance with a specified security policy. It is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system is secure.

In this model, a multilevel-secure system satisfies several rules, including the "confinement property" (a.k.a. the "*-property"), the "simple security property", and the "tranquility property".

Benign:

1. (COMSEC) "Condition of cryptographic data [such] that [the data] cannot be compromised by human access [to the data]."
2. (COMPUSEC) See: secondary definition under "trust".

Benign fill: Process by which keying material is generated, distributed, and placed into an ECU without exposure to any human or other system entity, except the cryptographic module that consumes and uses the material. (See: benign.)

BER: See: Basic Encoding Rules.

Beyond A1:

1. (formal) A level of security assurance that is beyond the highest level (level A1) of criteria specified by the TCSEC. (See: Tutorial under "Trusted Computer System Evaluation Criteria".)
2. (informal) A level of trust so high that it is beyond state-of-the-art technology; i.e., it cannot be provided or verified by currently available assurance methods, and especially not by currently available formal methods.

Biba integrity: Synonym for "source integrity".

Biba model: A formal, mathematical, state-transition model of integrity policy for multilevel-secure computer systems. (See: source integrity. Compare: Bell-LaPadula model.)

Tutorial: This model for integrity control is analogous to the Bell-LaPadula model for confidentiality control. Each subject and object is assigned an integrity level and, to determine whether or not a subject is authorized for a particular access mode on an object, the integrity level of the subject is compared to that of the object. The model prohibits the changing of information in an object by a subject with a lesser or incomparable level. The rules of the Biba model are duals of the corresponding rules in the Bell-LaPadula model.

Billet: A personnel position or assignment that may be filled by one person. (Compare: principal, role, user.)

Tutorial: In an organization, a "billet" is a populational position, of which there is exactly one instance; but a "role" is functional position, of which there can be multiple instances. System entities are in one-to-one relationships with their billets, but may be in many-to-one and one-to-many relationships with their roles.

BIN: See: bank identification number.

Bind: To inseparably associate by applying some security mechanism. Example: A CA creates a public-key certificate by using a digital signature to bind together

(a) A subject name,

(b) A public key, and usually

(c) Some additional data items (e.g., "X.509 public-key certificate").

Biometric authentication: A method of generating authentication information for a person by digitizing measurements of a physical or behavioral characteristic, such as a fingerprint, hand shape, retina pattern, voiceprint, handwriting style, or face.

Birthday attack: A class of attacks against cryptographic functions, including both encryption functions and hash functions. The attacks take advantage of a statistical property: Given a cryptographic function having an N-bit output, the probability is greater than 1(2 that for 2**(N(2) randomly chosen inputs, the function will produce at least two outputs that are identical. (See: Tutorial under "hash function".)

Derivation: From the somewhat surprising fact (often called the "birthday paradox") that although there are 365 days in a year, the probability is greater than 1(2 that two of more people share the same birthday in any randomly chosen group of 23 people. Birthday attacks enable an adversary to find two inputs for which a cryptographic function produces the same cipher text (or find two inputs for which a hash functions produces the same hash result) much faster than a brute-force attack can; and a clever adversary can use such a capability to create considerable mischief. However, no birthday attack can enable an adversary to decrypt a given cipher text (or find a hash input that results in a given hash result) any faster than a brute-force attack can.

Bit: A contraction of the term "binary digit"; the smallest unit of information storage, which has two possible states or values. The values usually are represented by the symbols "0" (zero) and "1" (one). (See: block, byte, nibble, word.)

Bit string: A sequence of bits, each of which is either "0" or "1".

BLACK:

1. Designation for data that consists only of cipher text, and for information system equipment items or facilities that handle only cipher text. Example: "BLACK key". (See: BCR, color change, RED(BLACK separation. Compare: RED.)
2. (U.S. Government) Designation applied to information systems, and to associated areas, circuits, components, and equipment, in which national security information is encrypted or is not processed.
3. Any data that can be disclosed without harm.

Deprecated Definition: DOCUMENTS SHOULD NOT use the term with definition 3 because the definition is ambiguous with regard to whether or not the data is protected.

BLACK(Crypto)RED (BCR): An experimental, end-to-end, network packet encryption system developed in a working prototype form by BBN and the Collins Radio division of Rockwell Corporation in the 1975-1980 time frame for the U.S. DoD. BCR was the first network security system to support TCP(IP traffic, and it incorporated the first DES chips that were validated by the U.S. National Bureau of Standards (now called NIST). BCR also was the first to use a KDC and an ACC to manage connections.

BLACK key: A key that is protected with a key-encrypting key and that must be decrypted before use. (See: BLACK. Compare: RED key.)

BLACKER: An end-to-end encryption system for computer data networks that was developed by the U.S. DoD in the 1980s to provide host to-host data confidentiality service for datagrams at OSI-RM Layer 3.

Tutorial: Each user host connects to its own bump-in-the-wire encryption device called a BLACKER Front End (BFE, TSEC(KI-111), through which the host connects to the subnetwork. The system also includes two types of centralized devices: one or more KDCs connect to the subnetwork and communicate with assigned sets of BFEs, and one or more ACCs connect to the subnetwork and communicate with assigned KDCs. BLACKER uses only symmetric encryption. A KDC distributes session keys to BFE pairs as authorized by an ACC. Each ACC maintains a database for a set of BFEs, and the database determines which pairs from that set (i.e., which pairs of user hosts behind the BFEs) are authorized to communicate and at what security levels.

The BLACKER system is MLS in three ways:

(a) The BFEs form a security perimeter around a subnetwork, separating user hosts from the subnetwork, so that the subnetwork can operate at a different security level (possibly a lower, less expensive level) than the hosts.

(b) The BLACKER components are trusted to separate datagrams of different security levels, so that each datagram of a given security level can be received only by a host that is authorized for that security level; and thus BLACKER can separate host communities that operate at different security levels. (c) The host side of a BFE is itself MLS and can recognize a security label on each packet, so that an MLS user host can be authorized to successively transmit datagrams that are labeled with different security levels.

Blind attack: A type of network-based attack method that does not require the attacking entity to receive data traffic from the attacked entity; i.e., the attacker does not need to "see" data packets sent by the victim. Example: SYN flood.

Tutorial: If an attack method is blind, the attacker's packets can carry:

(a) A false IP source address (making it difficult for the victim to find the attacker) and

(b) A different address on every packet (making it difficult for the victim to block the attack). If the attacker needs to receive traffic from the victim, the attacker must either

(c) Reveal its own IP address to the victim (which enables the victim to find the attacker or block the attack by filtering) or

(d) Provide a false address and also subvert network routing mechanisms to divert the returning packets to the attacker (which makes the attack more complex, more difficult, or more expensive).

Block: A bit string or bit vector of finite length. (See: bit, block cipher. Compare: byte, word.) Usage: An "N-bit block" contains N bits, which usually are numbered from left to right as 1, 2, 3, ..., N.

Block cipher: An encryption algorithm that breaks plain text into fixed-size segments and uses the same key to transform each plaintext segment into a fixed-size segment of cipher text. Examples: AES, Blowfish, DEA, IDEA, RC2, and SKIPJACK. (See: block, mode. Compare: stream cipher.)

Tutorial: A block cipher can be adapted to have a different external interface, such as that of a stream cipher, by using a mode of cryptographic operation to package the basic algorithm. (See: CBC, CCM, CFB, CMAC, CTR, DEA, ECB, OFB.)

Blowfish: A symmetric block cipher with variable-length key (32 to 448 bits) designed in 1993 by Bruce Schneier as an unpatented, license-free, royalty-free replacement for DES or IDEA.

Brain-damaged: **(**slang) "Obviously wrong: extremely poorly designed. Calling something brain-damaged is very extreme. The word implies that the thing is completely unusable, and that its failure to work is due to poor design, not accident." (See: flaw.)

Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term.

Brand:

1. A distinctive mark or name that identifies a product or business entity.

2. (SET) The name of a payment card. (See: BCA.)

Tutorial: Financial institutions and other companies have founded payment card brands, protect and advertise the brands, establish and enforce rules for use and acceptance of their payment cards, and provide networks to interconnect the financial institutions. These brands combine the roles of issuer and acquirer in interactions with cardholders and merchants.

Brand certification authority (BCA): **(**SET) A CA owned by a payment card brand, such as MasterCard, Visa, or American Express. (See: certification hierarchy, SET.)

Brand CRL identifier (BCI): **(**SET) A digitally signed list, issued by a BCA, of the names of CAs for which CRLs need to be processed when verifying signatures in SET messages.

Break: **(**cryptography) To successfully perform cryptanalysis and thus succeed in decrypting data or performing some other cryptographic function, without initially having knowledge of the key that the function requires. (See: penetrate, strength, work factor.)

Usage: This term applies to encrypted data or, more generally, to a cryptographic algorithm or cryptographic system. Also, while the most common use is to refer to completely breaking an algorithm, the term is also used when a method is found that substantially reduces the work factor.

Brewer-Nash model: A security model to enforce the Chinese wall policy. (Compare: Bell-LaPadula model, Clark-Wilson model.)

Tutorial: All proprietary information in the set of commercial firms F(1), F(2), ..., F(N) is categorized into mutually exclusive conflict-of-interest classes I(1), I(2), ..., I(M) that apply across all firms. Each firm belongs to exactly one class. The Brewer-Nash model has the following mandatory rules:

- Brewer-Nash Read Rule: Subject S can read information object O from firm F(i) only if either (a) O is from the same firm as some object previously read by S *or* (b) O belongs to a class I(i) from which S has not previously read any object. (See: object, subject.)
- Brewer-Nash Write Rule: Subject S can write information object O to firm F(i) only if (a) S can read O by the Brewer-Nash Read Rule *and* (b) no object

can be read by S from a different firm F(j), no matter whether F(j) belongs to the same class as F(i) or to a different class.

Bridge: A gateway for traffic flowing at OSI-RM Layer 2 between two networks (usually two LANs). (Compare: bridge CA, router.)

Bridge CA: A PKI consisting of only a CA that cross-certifies with CAs of some other PKIs. (See: cross-certification. Compare: bridge.)

Tutorial: A bridge CA functions as a hub that enables a certificate user in any of the PKIs that attach to the bridge, to validate certificates issued in the other attached PKIs.

For example, a bridge CA (BCA) CA1could cross-certify with four ^ PKIs that have the roots CA1, | CA2, CA3, and CA4. The cross- v certificates that the roots CA2 <-> BCA <-> CA3 exchange with the BCA enable an ^ end entity EE1 certified under |under CA1 in PK1 to construct v a certification path needed to CA4 validate the certificate of end entity EE2 under CA2, CA1 -> BCA -> CA2 -> EE2 or vice versa. CA2 -> BCA -> CA1 -> EE1

British Standard 7799: Part 1 of the standard is a code of practice for how to secure an information system. Part 2 specifies the management framework, objectives, and control requirements for information security management systems.

Browser: client computer program that can retrieve and display information from servers on the World Wide Web. Examples: Netscape Navigator and Microsoft Internet Explorer.

Brute force: A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries a large number of possible solutions to the problem. (See: impossible, strength, work factor.)

Tutorial: In some cases, brute force involves trying all of the possibilities. For example, for cipher text where the analyst already knows the decryption algorithm, a brute-force technique for finding matching plain text is to decrypt the message with every possible key. In other cases, brute force involves trying a large number of possibilities but substantially fewer than all of them.

BS7799: See: British Standard 7799.

Buffer overflow: Any attack technique that exploits a vulnerability resulting from computer software or hardware that does not check for exceeding the bounds of a storage area when data is written into a sequence of storage locations beginning in that area.

Tutorial: By causing a normal system operation to write data beyond the bounds of a storage area, the attacker seeks to either disrupt system operation or cause the system to execute malicious software inserted by the attacker.

Buffer zone: A neutral internetwork segment used to connect other segments that each operate under a different security policy.

Tutorial: To connect a private network to the Internet or some other relatively public network, one could construct a small, separate, isolated LAN and connect it to both the private network and the public network; one or both of the connections would implement a firewall to limit the traffic that could pass through the buffer zone.

Bulk encryption:

1. Encryption of multiple channels by aggregating them into a single transfer path and then encrypting that path. (See: channel.)
2. Simultaneous encryption of all channels of a multichannel telecommunications link. (Compare: bulk keying material.)

Usage: The use of "simultaneous" in definition 2 could be interpreted to mean that multiple channels are encrypted separately but at the same time. However, the common meaning of the term is that multiple data flows are combined into a single stream and then that stream is encrypted as a whole.

Bulk key: In a few published descriptions of hybrid encryption for SSH, Windows 2000, and other applications, this term refers to a symmetric key that (a) is used to encrypt a relatively large amount of data and (b) is itself encrypted with a public key. (Compare: bulk keying material, session key.)

Example: To send a large file to Bob, Alice (a) generates a symmetric key and uses it to encrypt the file (i.e., encrypt the bulk of the information that is to be sent) and then (b) encrypts that symmetric key (the "bulk key") with Bob's public key.

Deprecated Term: DOCUMENTS SHOULD NOT use this term or definition; the term is not well-established and could be confused with the established term "bulk keying material". Instead, use "symmetric key" and carefully explain how the key is applied.

Bulk keying material: Refers to handling keying material in large quantities, e.g., as a dataset that contains many items of keying material. (See: type 0. Compare: bulk key, bulk encryption.)

Bump-in-the-stack: An implementation approach that places a network security mechanism inside the system that is to be protected. (Compare: bump-in-the-wire.)

Example: IPsec can be implemented inboard, in the protocol stack of an existing system or existing system design, by placing a new layer between the existing IP layer and the OSI-RM Layer 3 drivers. Source code access for the existing stack is not required, but the system that contains the stack does need to be modified.

Bump-in-the-wire: An implementation approach that places a network security mechanism outside of the system that is to be protected. (Compare: bump-in-the-stack.)

Example: IPsec can be implemented outboard, in a physically separate device, so that the system that receives the IPsec protection does not need to be modified at all. Military grade link encryption has mainly been implemented as bump-in-the wire devices.

Business-case analysis: An extended form of cost-benefit analysis that considers factors beyond financial metrics, including security factors such as the requirement for security services, their technical and programmatic feasibility, their qualitative benefits, and associated risks. (See: risk analysis.)

Byte: A fundamental unit of computer storage; the smallest addressable unit in a computer's architecture. Usually holds one character of information and, today, usually means eight bits. (Compare: octet.)

Usage: Understood to be larger than a "bit", but smaller than a "word". Although "byte" almost always means "octet" today, some computer architectures have had bytes in other sizes (e.g., six bits, nine bits). Therefore, an STD SHOULD state the number of bits in a byte where the term is first used in the STD.

C field: See: Compartments field.

C1 or C2 computer system: (TCSEC) See: Tutorial under "Trusted Computer System Evaluation Criteria".

CA: See: certification authority.

CA certificate: A certificate for one CA issued by another CA."

Deprecated Definition: DOCUMENTS SHOULD NOT use the term with this definition; the definition is ambiguous with regard to how the certificate is constructed and how it is intended to be used.

Tutorial: There is no single, obvious choice for a technical definition of this term. Different PKIs can use different certificate profiles, and X.509 provides several choices of how to issue certificates to CAs. For example, one possible definition is the following: A v3 X.509 public-key certificate that has a "basicConstraints" extension containing a "cA" value of "TRUE". That would specifically indicate that "the certified public key may be used to verify certificate signatures", i.e., that the private key may be used by a CA. However, there also are other ways to indicate such usage. The certificate may have a "key Usage" extension that indicates the purposes for which the public key may be used, and one of the values that X.509 defines for that extension is "keyCertSign", to indicate that the certificate may be used for verifying a CA's signature on certificates. If "keyCertSign" is present in a certificate that also has a "basicConstraints" extension, then "cA" is set to "TRUE"

in that extension. Alternatively, a CA could be issued a certificate in which "keyCertSign" is asserted without "basicConstraints" being present; and an entity that acts as a CA could be issued a certificate with "keyUsage" set to other values, either with or without "keyCertSign".

CA domain: (PK) A security policy domain that consists of a CA and its subjects [i.e., the entities named in the certificates issued by the CA]. Sometimes referred to as a PKI domain. (See: domain.)

Caesar cipher: A cipher that is defined for an alphabet of N characters, A(1), A(2), ..., A(N), and creates cipher text by replacing each plaintext character A(i) by A(i+K, mod N) for some 0<K<N+1.

Examples: (a) During the Gallic wars, Julius Caesar used a cipher with K=3. In a Caesar cipher with K=3 for the English alphabet, A is replaced by D, B by E, C by F, ..., W by Z, X by A, Y by B, Z by C. (b) UNIX systems sometimes include "ROT13" software that implements a Caesar cipher with K=13 (i.e., ROTate by 13).

Call back: An authentication technique for terminals that remotely access a computer via telephone lines; the host system disconnects the caller and then reconnects on a telephone number that was previously authorized for that terminal.

CAM: See: Certificate Arbitrator Module.

CANEWARE: An end-to-end encryption system for computer data networks that was developed by the U.S. DoD in the 1980s to provide host-to-host data confidentiality service for datagrams in OSI-RM Layer 3. (Compare: BLACKER, IPsec.)

Tutorial: Each user host connects to its own bump-in-the-wire encryption device called a CANEWARE Front End (CFE), through which the host connects to the subnetwork. CANEWARE uses symmetric encryption for CFE-to-CFE traffic, but also uses FIREFLY to establish those session keys. The public-key certificates issued by the FIREFLY system include credentials for mandatory access control. For discretionary access control, the system also includes one or more centralized CANEWARE Control Processors (CCPs) that connect to the subnetwork, maintain a database for discretionary access control authorizations, and communicate those authorizations to assigned sets of CFEs.

The CANEWARE system is MLS in only two of the three ways that BLACKER is MLS: (a) Like BLACKER BFEs, CFEs form a security perimeter around a subnetwork, separating user hosts from the subnetwork, so that the subnetwork can operate at a different security level than the hosts. (b) Like BLACKER, the CANEWARE components are trusted to separate datagrams of different security levels, so that each datagram of a given security level can be received only by a host that is authorized for that security level; and thus CANEWARE can separate

host communities that operate at different security levels. (c) Unlike a BFE, the host side of a CFE is not MLS, and treats all packets received from a user host as being at the same mandatory security level.

Capability list: (information system) A mechanism that implements access control for a system entity by enumerating the system resources that the entity is permitted to access and, either implicitly or explicitly, the access modes granted for each resource. (Compare: access control list, access control matrix, access profile, capability token.)

Capability token: A token (usually an unforgeable data object) that gives the bearer or holder the right to access a system resource. Possession of the token is accepted by a system as proof that the holder has been authorized to access the resource indicated by the token. (See: attribute certificate, capability list, credential, digital certificate, ticket, token.)

Capability Maturity Model (CMM): (N) Method for judging the maturity of software processes in an organization and for identifying crucial practices needed to increase process maturity. (Compare: Common Criteria.)

Tutorial: The CMM does not specify security evaluation criteria (see: assurance level), but its use may improve security assurance. The CMM describes principles and practices that can improve software processes in terms of evolving from ad hoc processes to disciplined processes. The CMM has five levels:

- **Initial:** Software processes are ad hoc or chaotic, and few are well-defined. Success depends on individual effort and heroics.
- **Repeatable:** Basic project management processes are established to track cost, schedule, and functionality. Necessary process discipline is in place to repeat earlier successes on projects with similar applications.
- **Defined**: Software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. Each project uses an approved, tailored version of the organization's standard process for developing and maintaining software.
- **Managed:** Detailed measures of software process and product quality are collected. Both software process and products are quantitatively understood and controlled.
- **Optimizing:** Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

CAPI: See: cryptographic application programming interface.

CAPSTONE: An integrated microcircuit (in MYK-8x series manufactured by Mykotronx, Inc.) that implements SKIPJACK, KEA, DSA, SHA, and basic mathematical

functions needed to support asymmetric cryptography; has a non-deterministic random number generator; and supports key escrow. (See: FORTEZZA. Compare: CLIPPER.)

Card: See: cryptographic card, FORTEZZA, payment card, PC card, smart card, token.

Card backup: See: token backup.

Card copy: See: token copy.

Card restore: See: token restore.

Cardholder:

1. An entity to whom or to which a card has been issued.

   Usage: Usually refers to a living human being, but might refer (a) to a position (see: billet, role) in an organization or (b) to an automated process. (Compare: user.)

2. (SET) The holder of a valid payment card account and user of software supporting electronic commerce. A cardholder is issued a payment card by an issuer. SET ensures that in the cardholder's interactions with merchants, the payment card account information remains confidential.

Cardholder certificate: **(**SET) A digital certificate that is issued to a cardholder upon approval of the cardholder's issuing financial institution and that is transmitted to merchants with purchase requests and encrypted payment instructions, carrying assurance that the account number has been validated by the issuing financial institution and cannot be altered by a third party.

Cardholder certification authority (CCA): **(**SET) A CA responsible for issuing digital certificates to cardholders and operated on behalf of a payment card brand, an issuer, or another party according to brand rules. A CCA maintains relationships with card issuers to allow for the verification of cardholder accounts. A CCA does not issue a CRL but does distribute CRLs issued by root CAs, brand CAs, geopolitical CAs, and payment gateway CAs.

CAST: A design procedure for symmetric encryption algorithms, and a resulting family of algorithms, invented by Carlisle Adams (C.A.) and Stafford Tavares (S.T.).

Category: A grouping of sensitive information items to which a nonhierarchical restrictive security label is applied to increase protection of the data. (See: formal access approval. Compare: compartment, classification.)

CAW: See: certification authority workstation.

CBC: See: cipher block chaining.

CCA: See: cardholder certification authority.

CCEP: See: Commercial COMSEC Endorsement Program.

CCI: See: Controlled Cryptographic Item.

CCITT: Acronym for French translation of International Telephone and Telegraph Consultative Committee. Now renamed ITU-T.

CCM: See: Counter with Cipher Block Chaining-Message Authentication Code.

CERIAS: Purdue University's Center for Education and Research in Information Assurance and Security, which includes faculty from multiple schools and departments and takes a multidisciplinary approach to security problems ranging from technical to ethical, legal, educational, communicational, linguistic, and economic.

CERT: See: computer emergency response team.

Certificate:

1. (general English) A document that attests to the truth of something or the ownership of something.
2. (general security) See: capability token, digital certificate.
3. (PKI(See: attribute certificate, public-key certificate.

Certificate Arbitrator Module (CAM): An open-source software module that is designed to be integrated with an application for routing, replying to, and otherwise managing and meditating certificate validation requests between that application and the CAs in the ACES PKI.

Certificate authority: Synonym for "certification authority".

Certificate chain: Synonym for "certification path". (See: trust chain.)

Deprecated Term: DOCUMENTs SHOULD NOT use this term; it duplicates the meaning of a standardized term. Instead, use "certification path".

Certificate chain validation: Synonym for "certificate validation" or "path validation".

Deprecated Term: DOCUMENTs SHOULD NOT use this term; it duplicates the meaning of standardized terms and mixes concepts in a potentially misleading way. Instead, use "certificate validation" or "path validation", depending on what is meant. (See: validate vs. verify.)

Certificate creation: The act or process by which a CA sets the values of a digital certificate's data fields and signs it. (See: issue.)

Certificate expiration: The event that occurs when a certificate ceases to be valid because its assigned lifetime has been exceeded. (See: certificate revocation, expire.)

Certificate extension: See: extension.

Certificate holder: Synonym for the "subject" of a digital certificate. (Compare: certificate owner, certificate user.)

Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for the subject of a digital certificate; the term is potentially ambiguous. For example, the term could be misunderstood as referring to a system entity or component, such as a repository, that simply has possession of a copy of the certificate.

Certificate management: The functions that a CA may perform during the lifecycle of a digital certificate, including the following:

- Acquire and verify data items to bind into the certificate.
- Encode and sign the certificate.
- Store the certificate in a directory or repository.
- Renew, rekey, and update the certificate.
- Revoke the certificate and issue a CRL. (See: archive management, certificate management, key management, security architecture, token management.)

Certificate management authority (CMA): (U.S. DoD) Used to mean either a CA or an RA.

Deprecated Term: DOCUMENTS SHOULD NOT use this term because it is potentially ambiguous, such as in a context involving ICRLs. Instead, use CA, RA, or both, depending on what is meant.

Certificate owner: Synonym for the "subject" of a digital certificate. (Compare: certificate holder, certificate user.)

Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for the subject of a digital certificate; the term is potentially ambiguous. For example, the term could refer to a system entity, such as a corporation, that has purchased a certificate to operate equipment, such as a Web server.

Certificate path: Synonym for "certification path".

Deprecated Term: DOCUMENTs SHOULD NOT use this term; it suggests careless use of "certification path", which is preferred in PKI standards.

Certificate policy: A named set of rules that indicates the applicability of a certificate to a particular community and(or class of application with common security requirements. (Compare: CPS, security policy.)

Example: U.S. DoD's certificate policy defined four classes (i.e., assurance levels) for X.509 public-key certificates and defines the applicability of those classes. (See: class 2.)

Tutorial: A certificate policy can help a certificate user to decide whether a certificate should be trusted in a particular application. "For example, a particular certificate policy might indicate applicability of a type of certificate for the authentication of electronic data interchange transactions for the trading of goods within a given price range." A v3 X.509 public-key certificate may have a "certificatePolicies" extension that lists certificate policies, recognized by the issuing CA, that apply to the certificate and govern its use. Each policy is denoted by an object identifier and may optionally have certificate policy qualifiers. (See: certificate profile.) Each SET certificate specifies at least one certificate policy, that of the SET root CA. SET uses certificate policy qualifiers to point to the actual policy statement and to add qualifying policies to the root policy. (See: SET qualifier.)

Certificate policy qualifier: Information that pertains to a certificate policy and is included in a "certificate Policies" extension in a v3 X.509 public-key certificate.

Certificate profile: A specification of the format and semantics of public-key certificates or attribute certificates, constructed for use in a specific application context by selecting from among options offered by a broader standard. (Compare: protection profile.)

Certificate reactivation: The act or process by which a digital certificate, that a CA has designated for revocation but not yet listed on a CRL, is returned to the valid state.

Certificate rekey:

1. The act or process by which an existing public-key certificate has its key value changed by issuing a new certificate with a different (usually new) public key. (See: certificate renewal, certificate update, rekey.)

   Tutorial: For an X.509 public-key certificate, the essence of rekey is that the subject stays the same and a new public key is bound to that subject. Other changes are made, and the old certificate is revoked, only as required by the PKI and CPS in support of the rekey. If changes go beyond that, the process is a "certificate update".

2. (MISSI) The act or process by which a MISSI CA creates a new X.509 public-key certificate that is identical to the old one, except the new one has (a) a new, different KEA key or (b) a new, different DSS key or (c) new, different KEA and DSS keys. The new certificate also has a different serial number and may have a different validity period. A new key creation date and maximum key lifetime period are assigned to each newly generated key. If a new KEA key is generated, that key is assigned a new KMID. The old certificate remains valid until it expires, but may not be further renewed, rekeyed, or updated.

Certificate renewal: The act or process by which the validity of the binding asserted by an existing public-key certificate is extended in time by issuing a new certificate. (See: certificate rekey, certificate update.)

Tutorial: For an X.509 public-key certificate, this term means that the validity period is extended (and, of course, a new serial number is assigned) but the binding of the public key to the subject and to other data items stays the same. The other data items are changed, and the old certificate is revoked, only as required by the PKI and CPS to support the renewal. If changes go beyond that, the process is a "certificate rekey" or "certificate update".

Certificate request: Synonym for "certification request".

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it suggests careless use of the term "certification request", which is preferred in PKI standards (e.g., see PKCS #10).

Certificate revocation: The event that occurs when a CA declares that a previously valid digital certificate issued by that CA has become invalid; usually stated with an effective date.

Tutorial: In X.509, a revocation is announced to potential certificate users by issuing a CRL that mentions the certificate. Revocation and listing on a CRL is only necessary prior to the certificate's scheduled expiration.

Certificate revocation list (CRL):

1. A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, delta CRL, X.509 certificate revocation list.)
2. A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes.

Certificate revocation tree: A mechanism for distributing notices of certificate revocations; uses a tree of hash results that is signed by the tree's issuer. Offers an alternative to issuing a CRL, but is not supported in X.509. (See: certificate status responder.)

Certificate serial number:

1. An integer value that (a) is associated with, and may be carried in, a digital certificate; (b) is assigned to the certificate by the certificate's issuer; and (c) is unique among all the certificates produced by that issuer.
2. An integer value, unique within the issuing CA, that is unambiguously associated with a certificate issued by that CA.

Certificate status authority: **(**U.S. DoD) A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness [should instead say 'validity'], and may also provide additional attribute information for the subject certificate.

Deprecated Term: DOCUMENTs SHOULD NOT use this term because it is not widely accepted; instead, use "certificate status responder" or "OCSP server", or otherwise explain what is meant.

Certificate status responder: (FPKI) A trusted online server that acts for a CA to provide authenticated certificate status information to certificate users. Offers an alternative to issuing a CR. (See: certificate revocation tree, OCSP.)

Certificate update: The act or process by which non-key data items bound in an existing public-key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate. (See: certificate rekey, certificate renewal.)

Usage: For an X.509 public-key certificate, the essence of this process is that fundamental changes are made in the data that is bound to the public key, such that it is necessary to revoke the old certificate. (Otherwise, the process is only a "certificate rekey" or "certificate renewal".)

Certificate user:

1. A system entity that depends on the validity of information (such as another entity's public key value) provided by a digital certificate.

   Usage: The depending entity may be a human being or an organization, or a device or process controlled by a human or organization. (See: user.)

2. An entity that needs to know, with certainty, the public key of another entity.

3. Synonym for "subject" of a digital certificate.

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term with definition 3; the term could be confused with one of the other two definitions given above.

Certificate validation:

1. An act or process by which a certificate user establishes that the assertions made by a digital certificate can be trusted. (See: valid certificate, validate vs. verify.)

2. The process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e. were not expired or revoked) at that given time.

   Tutorial: To validate a certificate, a certificate user checks that the certificate is properly formed and signed and is currently in force:

   - Checks the syntax and semantics: Parses the certificate's syntax and interprets its semantics, applying rules specified for and by its data fields, such as for critical extensions in an X.509 certificate.
   - Checks the signature: Uses the issuer's public key to verify the digital signature of the CA who issued the certificate in question. If the verifier obtains

the issuer's public key from the issuer's own public-key certificate, that certificate should be validated, too. That validation may lead to yet another certificate to be validated, and so on. Thus, in general, certificate validation involves discovering and validating a certification path.

- Checks currency and revocation: Verifies that the certificate is currently in force by checking that the current date and time are within the validity period (if that is specified in the certificate) and that the certificate is not listed on a CRL or otherwise announced as invalid. (The CRLs also must be checked by a similar validation process.)

Certification:

1. (information system) Comprehensive evaluation (usually made in support of an accreditation action) of an information system's technical security features and other safeguards to establish the extent to which the system's design and implementation meet a set of specified security requirements. (See: accreditation. Compare: evaluation.)
2. (digital certificate) The act or process of vouching for the truth and accuracy of the binding between data items in a certificate. (See: certify.)
3. (PKI) The act or process of vouching for the ownership of a public key by issuing a public-key certificate that binds the key to the name of the entity that possesses the matching private key. Besides binding a key with a name, a public-key certificate may bind those items with other restrictive or explanatory data items. (See: X.509 public-key certificate.)
4. (SET) The process of ascertaining that a set of requirements or criteria has been fulfilled and attesting to that fact to others, usually with some written instrument. A system that has been inspected and evaluated as fully compliant with the SET protocol by duly authorized parties and process would be said to have been certified compliant.

Certification authority (CA):

1. An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.
2. An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys.

   Tutorial: Certificate users depend on the validity of information provided by a certificate. Thus, a CA should be someone that certificate users trust and that usually holds an official position created and granted power by a government, a corporation, or some other organization. A CA is responsible for managing the life cycle of certificates (see: certificate management) and, depending on the type of

certificate and the CPS that applies, may be responsible for the lifecycle of key pairs associated with the certificates (see: key management).

Certification authority workstation (CAW): A computer system that enables a CA to issue digital certificates and supports other certificate management functions as required.

Certification hierarchy:

1. A tree-structured (loop-free) topology of relationships between CAs and the entities to whom the CAs issue public-key certificates. (See: hierarchical PKI, hierarchy management.)

   Tutorial: In this structure, one CA is the top CA, the highest level of the hierarchy. (See: root, top CA.) The top CA may issue public-key certificates to one or more additional CAs that form the second-highest level. Each of these CAs may issue certificates to more CAs at the third-highest level, and so on. The CAs at the second-lowest level issue certificates only to non-CA entities that form the lowest level (see: end entity). Thus, all certification paths begin at the top CA and descend through zero or more levels of other CAs. All certificate users base path validations on the top CA's public key.

2. (PEM) A certification hierarchy for PEM has three levels of CAs
   - The highest level is the "Internet Policy Registration Authority".
   - A CA at the second-highest level is a "policy certification authority".
   - A CA at the third-highest level is a "certification authority".
3. (MISSI) A certification hierarchy for MISSI has three or four levels of CAs:
   - A CA at the highest level, the top CA, is a "policy approving authority".
   - A CA at the second-highest level is a "policy creation authority".
   - A CA at the third-highest level is a local authority called a "certification authority".
   - A CA at the fourth-highest (optional) level is a "subordinate certification authority".
4. (SET) A certification hierarchy for SET has three or four levels of CAs:
   - The highest level is a "SET root CA".
   - A CA at the second-highest level is a "brand certification authority".
   - A CA at the third-highest (optional) level is a "geopolitical certification authority".
   - A CA at the fourth-highest level is a "cardholder CA", a "merchant CA", or a "payment gateway CA".

Certification path:

1. A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. (See: trust anchor, certificate validation, valid certificate.)

2. An ordered sequence of certificates of objects in the [X.500 Directory Information Tree] which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

   Tutorial: The list is "linked" in the sense that the digital signature of each certificate (except possibly the first) is verified by the public key contained in the preceding certificate; i.e., the private key used to sign a certificate and the public key contained in the preceding certificate form a key pair that has previously been bound to the authority that signed. The path is the "list of certificates needed to [enable] a particular user to obtain the public key [or attributes] of another [user]." [X509] Here, the word "particular" points out that a certification path that can be validated by one certificate user might not be able to be validated by another. That is because either the first certificate needs to be a trusted certificate or the signature on the first certificate needs to be verifiable by a trusted key (e.g., a root key), but such trust is established only relative to a "particular" (i.e., specific) user, not absolutely for all users.

Certification policy: Synonym for either "certificate policy" or "certification practice statement".

Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for either of those terms; that would be duplicative and would mix concepts in a potentially misleading way. Instead, use either "certificate policy" or "certification practice statement", depending on what is meant.

Certification practice statement (CPS): A statement of the practices which a certification authority employs in issuing certificates. (See: certificate policy.)

Tutorial: A CPS is a published security policy that can help a certificate user to decide whether a certificate issued by a particular CA can be trusted enough to use in a particular application. A CPS may be

(a) a declaration by a CA of the details of the system and practices it uses in its certificate management operations,

(b) part of a contract between the CA and an entity to whom a certificate is issued,

(c) a statute or regulation applicable to the CA, or

(d) a combination of these types involving multiple documents.

A CPS is usually more detailed and procedurally oriented than a certificate policy. A CPS applies to a particular CA or CA community, while a certificate policy applies across CAs or communities. A CA with its single CPS may support multiple certificate policies, which may be used for different application purposes or by different user communities. On the other hand, multiple CAs, each with a different CPS, may support the same certificate policy.

Certification request: An algorithm-independent transaction format (e.g., PKCS #10, RFC 4211) that contains a DN, and a public key or, optionally, a set of attributes, collectively signed by the entity requesting certification, and sent to a CA, which transforms the request to an X.509 public-key certificate or another type of certificate.

Certify:

1. Issue a digital certificate and thus vouch for the truth, accuracy, and binding between data items in the certificate (e.g., "X.509 public-key certificate"), such as the identity of the certificate's subject and the ownership of a public key. (See: certification.)

   Usage: To "certify a public key" means to issue a public-key certificate that vouches for the binding between the certificate's subject and the key.

2. The act by which a CA uses measures to verify the truth, accuracy, and binding between data items in a digital certificate.

   Tutorial: A description of the measures used for verification should be included in the CA's CPS.

Challenge Handshake Authentication Protocol (CHAP): A peer entity authentication method (employed by PPP and other protocols, e.g., RFC 3720) that uses a randomly generated challenge and requires a matching response that depends on a cryptographic hash of some combination of the challenge and a secret key. [R1994] (See: challenge-response, PAP.)

Challenge-response: An authentication process that verifies an identity by requiring correct authentication information to be provided in response to a challenge. In a computer system, the authentication information is usually a value that is required to be computed in response to an unpredictable challenge value, but it might be just a password.

Challenge-Response Authentication Mechanism (CRAM): (IMAP4) A mechanism [R2195], intended for use with IMAP4 AUTHENTICATE, by which an IMAP4 client uses a keyed hash [R2104] to authenticate itself to an IMAP4 server. (See: POP3 APOP.)

Tutorial: The server includes a unique time stamp in its ready response to the client. The client replies with the client's name and the hash result of applying

MD5 to a string formed from concatenating the time stamp with a shared secret that is known only to the client and the server.

Channel:

1. An information transfer path within a system. (See: covert channel.)
2. A subdivision of the physical medium allowing possibly shared independent uses of the medium."

Channel capacity: The total capacity of a link to carry information; usually expressed in bits per second. (RFC 3753) (Compare: bandwidth.)

Tutorial: Within a given bandwidth, the theoretical maximum channel capacity is given by Shannon's Law. The actual channel capacity is determined by the bandwidth, the coding system used, and the signal-to-noise ratio.

CHAP: See: Challenge Handshake Authentication Protocol.

Checksum: A value that

(a) is computed by a function that is dependent on the contents of a data object and

(b) is stored or transmitted together with the object, for detecting changes in the data. (See: cyclic redundancy check, data integrity service, error detection code, hash, keyed hash, parity bit, protected checksum.)

Tutorial: To gain confidence that a data object has not been changed, an entity that later uses the data can independently re-compute the checksum value and compare the result with the value that was stored or transmitted with the object.

Computer systems and networks use checksums (and other mechanisms) to detect accidental changes in data. However, active wiretapping that changes data could also change an accompanying checksum to match the changed data. Thus, some checksum functions by themselves are not good countermeasures for active attacks. To protect against active attacks, the checksum function needs to be well-chosen (see: cryptographic hash), and the checksum result needs to be cryptographically protected (see: digital signature, keyed hash).

Chinese wall policy: A security policy to prevent conflict of interest caused by an entity (e.g., a consultant) interacting with competing firms. (See: Brewer-Nash model.)

Tutorial: All information is categorized into mutually exclusive conflict-of-interest classes I(1), I(2), ..., I(M), and each firm F(1), F(2), ..., F(N) belongs to exactly one class. The policy states that if a consultant has access to class I(i) information from a firm in that class, then the consultant may not access information from another firm in that same class, but may access information from another firm that is in a different class. Thus, the policy creates a barrier to communication between firms that are in the same conflict-of-interest class. Brewer and Nash modeled

enforcement of this policy [BN89], including dealing with policy violations that could occur because two or more consultants work for the same firm.

Chosen-ciphertext attack: A cryptanalysis technique in which the analyst tries to determine the key from knowledge of plain text that corresponds to cipher text selected (i.e., dictated) by the analyst.

Chosen-plaintext attack: A cryptanalysis technique in which the analyst tries to determine the key from knowledge of cipher text that corresponds to plain text selected (i.e., dictated) by the analyst.

CIAC: See: Computer Incident Advisory Capability.

CIK: See: cryptographic ignition key.

Cipher: A cryptographic algorithm for encryption and decryption.

Cipher block chaining (CBC): A block cipher mode that enhances ECB mode by chaining together blocks of cipher text it produces.

Tutorial: This mode operates by combining (exclusive OR-ing) the algorithm's ciphertext output block with the next plaintext block to form the next input block for the algorithm.

Cipher feedback (CFB): A block cipher mode that enhances ECB mode by chaining together the blocks of cipher text it produces and operating on plaintext segments of variable length less than or equal to the block length.

Tutorial: This mode operates by using the previously generated ciphertext segment as the algorithm's input (i.e., by "feeding back" the cipher text) to generate an output block, and then combining (exclusive OR-ing) that output block with the next plaintext segment (block length or less) to form the next cipher-text segment.

Cipher text:

1. (Noun) Data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available. (See: ciphertext. Compare: clear text, plain text.)
2. Data produced through the use of encipherment. The semantic content of the resulting data is not available.

Ciphertext:

1. (noun) Synonym for "cipher text" .
2. (adjective) Referring to cipher text. Usage: Commonly used instead of "cipher-text". (Compare: cleartext, plaintext.)

Ciphertext auto-key: (CTAK) (D) "Cryptographic logic that uses previous cipher text to generate a key stream." [C4009, A1523] (See: KAK.) Deprecated Term:

DOCUMENTs SHOULD NOT use this term; it is neither well-known nor precisely defined. Instead, use terms associated with modes that are defined in standards, such as CBC, CFB, and OFB.

Ciphertext-only attack: A cryptanalysis technique in which the analyst tries to determine the key solely from knowledge of intercepted cipher text (although the analyst may also know other clues, such as the cryptographic algorithm, the language in which the plain text was written, the subject matter of the plain text, and some probable plaintext words.)

Ciphony: The process of encrypting audio information.

CIPSO: See: Common IP Security Option.

CKL: See: compromised key list.

Clark-Wilson model: A security model [Clark] to maintain data integrity in the commercial world. (Compare: Bell-LaPadula model.)

Class 2, 3, 4, 5: **(**U.S. DoD) Assurance levels for PKIs, and for X.509 public-key certificates issued by a PKI. [DoD7] (See: "first law" under "Courtney's laws".)

- "Class 2": Intended for applications handling unclassified, low-value data in minimally or moderately protected environments.
- "Class 3": Intended for applications handling unclassified, medium-value data in moderately protected environments, or handling unclassified or high-value data in highly protected environments, and for discretionary access control of classified data in highly protected environments.
- "Class 4": Intended for applications handling unclassified, high-value data in minimally protected environments.
- "Class 5": Intended for applications handling classified data in minimally protected environments, and for authentication of material that would affect the security of classified systems. The environments are defined as follows:
- "Highly protected environment": Networks that are protected either with encryption devices approved by NSA for protection of classified data or via physical isolation, and that are certified for processing system-high classified data, where exposure of unencrypted data is limited to U.S. citizens holding appropriate security clearances.
- "Moderately protected environment":
- Physically isolated unclassified, unencrypted networks in which access is restricted based on legitimate need.
- Networks protected by NSA-approved, type 1 encryption, accessible by U.S.-authorized foreign nationals.

- "Minimally protected environments": Unencrypted networks connected to either the Internet or NIPRNET, either directly or via a firewall.

Class A1, B3, B2, B1, C2, or C1 computer system: (TCSEC) See: Tutorial under "Trusted Computer System Evaluation Criteria".

Classification:

1. A grouping of classified information to which a hierarchical, restrictive security label is applied to increase protection of the data from unauthorized disclosure. (See: aggregation, classified, data confidentiality service. Compare: category, compartment.)

2. An authorized process by which information is determined to be classified and assigned to a security level. (Compare: declassification.)

   Usage: Usually understood to involve data confidentiality, but DOCUMENTs SHOULD make this clear when data also is sensitive in other ways and SHOULD use other terms for those other sensitivity concepts. (See: sensitive information, data integrity.)

Classification label: A security label that tells the degree of harm that will result from unauthorized disclosure of the labeled data, and may also tell what countermeasures are required to be applied to protect the data from unauthorized disclosure. Example: IPSO. (See: classified, data confidentiality service. Compare: integrity label.)

Usage: Usually understood to involve data confidentiality, but DOCUMENTS SHOULD make this clear when data also is sensitive in other ways and SHOULD use other terms for those other sensitivity concepts. (See: sensitive information, data integrity.)

Classification level: A hierarchical level of protection (against unauthorized disclosure) that is required to be applied to certain classified data. (See: classified. Compare: security level.)

Classified:

1. Refers to information (stored or conveyed, in any form) that is formally required by a security policy to receive data confidentiality service and to be marked with a security label (which, in some cases, might be implicit) to indicate its protected status. (See: classify, collateral information, SAP, security level. Compare: unclassified.)

   Usage: Usually understood to involve data confidentiality, but DOCUMENTS SHOULD make this clear when data also is sensitive in other ways and SHOULD use other terms for those other sensitivity concepts. (See: sensitive information, data integrity.) Mainly used by national governments, especially by the military, but the underlying concept also applies outside of governments.

2. (U.S. Government) "Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status."

Classify: To officially designate an information item or type of information as being classified and assigned to a specific security level. (See: classified, declassify, security level.)

Clean system: A computer system in which the operating system and application system software and files have been freshly installed from trusted software distribution media. (Compare: secure state.)

Clear: Synonym for "erase".

Deprecated Definition: DOCUMENTS SHOULD NOT use the term with this definition; that could be confused with "clear text" in which information is directly recoverable.

Clear text:

1. (noun) Data in which the semantic information content (i.e., the meaning) is intelligible or is directly available, i.e., not encrypted. (See: cleartext, in the clear. Compare: cipher text, plain text.)
2. (noun) "Intelligible data, the semantic content of which is available." [I7498-2]
3. (noun) Synonym for "plain text".

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "plain text", because the plain text that is input to an encryption operation may itself be cipher text that was output from a previous encryption operation. (See: super-encryption.)

Clearance: See: security clearance.

Clearance level: The security level of information to which a security clearance authorizes a person to have access.

Cleartext:

1. Synonym for "clear text".
2. (adjective) Referring to clear text. Usage: Commonly used instead of "clear-text". (Compare: ciphertext, plaintext.)
3. (adjective) Synonym for "plaintext".

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "plaintext", because the plaintext data that is input to an encryption operation may itself be ciphertext data that was output from a previous encryption operation. (See: super-encryption.)

CLEF: See: commercially licensed evaluation facility.

Client: A system entity that requests and uses a service provided by another system entity, called a "server". (See: server.)

Tutorial: Usually, it is understood that the client and server are automated components of the system, and the client makes the request on behalf of a human user. In some cases, the server may itself be a client of some other server.

Client-server system: A distributed system in which one or more entities, called clients, request a specific service from one or more other entities, called servers, that provide the service to the clients.

CLIPPER: An integrated microcircuit (in MYK-7x series manufactured by Mykotronx, Inc.) that implements SKIPJACK, has a non-deterministic random number generator, and supports key escrow. (See: Escrowed Encryption Standard. Compare: CLIPPER.)

Tutorial: The chip was mainly intended for protecting telecommunications over the public switched network. The key escrow scheme for the chip involves a SKIPJACK key that is common to all chips and that protects the unique serial number of the chip, and a second SKIPJACK key unique to the chip that protects all data encrypted by the chip. The second key is escrowed as split key components held by NIST and the U.S. Treasury Department.

Closed security environment: (U.S. DoD) A system environment that meets both of the following conditions: (a) Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic. (b) Configuration control provides sufficient assurance that system applications and the equipment they run on are protected against the introduction of malicious logic prior to and during the operation of applications. [NCS04] (See: "first law" under "Courtney's laws". Compare: open security environment.)

CMA: See: certificate management authority.

CMAC: A message authentication code [SP38B] that is based on a symmetric block cipher. (See: block cipher.)

Derivation: Cipher-based MAC. (Compare: HMAC.) Tutorial: Because CMAC is based on approved, symmetric-key block ciphers, such as AES, CMAC can be considered a mode of operation for those block ciphers. (See: mode of operation.)

CMCS: See: COMSEC Material Control System.

CMM: See: Capability Maturity Model.

CMS: See: Cryptographic Message Syntax.

Code:

1. A system of symbols used to represent information, which might originally have some other representation. Examples: ASCII, BER, country code, Morse code. (See: encode, object code, source code.)

Deprecated Abbreviation: To avoid confusion with definition 1, DOCUMENTS SHOULD NOT use "code" as an abbreviation of "country code", "cyclic redundancy code", "Data Authentication Code", "error detection code", or "Message Authentication Code". To avoid misunderstanding, use the fully qualified term in these other cases, at least at the point of first usage.

2. (cryptography) An encryption algorithm based on substitution; i.e., a system for providing data confidentiality by using arbitrary groups (called "code groups") of letters, numbers, or symbols to represent units of plain text of varying length. (See: codebook, cryptography.)

Deprecated Usage: To avoid confusion with definition 1, DOCUMENTS SHOULD NOT use "code" as a synonym for any of the following terms:

(a) "cipher", "hash", or other words that mean "a cryptographic algorithm";

(b) "cipher text"; or

(c) "encrypt", "hash", or other words that refer to applying a cryptographic algorithm.

3. An algorithm based on substitution, but used to shorten messages rather than to conceal their content.

4. (computer programming) To write computer software. (See: object code, source code.)

Deprecated Abbreviation: To avoid confusion with definition 1, DOCUMENTS SHOULD NOT use "code" as an abbreviation of "object code" or "source code". To avoid misunderstanding, use the fully qualified term in these other cases, at least at the point of first usage.

Code book:

1. Document containing a systematically arranged list of plaintext units and their cipher-text equivalents.

2. An encryption algorithm that uses a word substitution technique. (See: code, ECB.)

Code signing: A security mechanism that uses a digital signature to provide data integrity and data origin authentication for software that is being distributed for use. (See: mobile code, trusted distribution.)

Tutorial: In some cases, the signature on a software module may imply some assertion that the signer makes about the software.

Code word: (U.S. Government) A single word that is used as a security label (usually applied to classified information) but which itself has a classified meaning. (See: classified, (U.S. Government) security label.)

COI: See: community of interest.

Cold start: (cryptographic module) A procedure for initially keying cryptographic equipment.

Collateral information: (U.S. Government) Information that is classified but is not required to be protected by an SAP. (See: (U.S. Government) classified.)

Color change: In a system being operated in periods-processing mode, the act of purging all information from one processing period and then changing over to the next processing period. (See: BLACK, RED.)

Commercial COMSEC Evaluation Program (CCEP): "Relationship between NSA and industry in which NSA provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product."

Commercially licensed evaluation facility (CLEF): An organization that has official approval to evaluate the security of products and systems under the Common Criteria, ITSEC, or some other standard. (Compare: KLIF.)

Committee on National Security Systems (CNSS): (O) (U.S. Government) A Government, interagency, standing committee of the President's Critical Infrastructure Protection Board. The CNSS is chaired by the Secretary of Defense and provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems. The Secretary of Defense and the Director of Central Intelligence are responsible for developing and overseeing the implementation of Government-wide policies, principles, standards, and guidelines for the security of systems that handle national security information.

Common Criteria for Information Technology Security: A standard for evaluating information technology (IT) products and systems. It states requirements for security functions and for assurance measures. (See: CLEF, EAL, packages, protection profile, security target, TOE. Compare: CMM.) Tutorial: Canada, France, Germany, the Netherlands, the United Kingdom, and the United States (NIST and NSA) began developing this standard in 1993, based on the European ITSEC, the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), and the U.S. "Federal Criteria for Information Technology Security" and its precursor, the TCSEC. Work was done in cooperation with ISO(IEC Joint Technical Committee 1 (Information Technology), Subcommittee 27 (Security

Techniques), Working Group 3 (Security Criteria). Version 2.0 of the Criteria has been issued as ISO's International Standard 15408. The U.S. Government intends this standard to supersede both the TCSEC and FIPS PUB 140. (See: NIAP.)

The standard addresses data confidentiality, data integrity, and availability and may apply to other aspects of security. It focuses on threats to information arising from human activities, malicious or otherwise, but may apply to non-human threats. It applies to security measures implemented in hardware, firmware, or software. It does not apply to

(a) Administrative security not related directly to technical security,

(b) Technical physical aspects of security such as electromagnetic emanation control,

(c) Evaluation methodology or administrative and legal framework under which the criteria may be applied,

(d) Procedures for use of evaluation results, or

(e) Assessment of inherent qualities of cryptographic algorithms.

Part 1, Introduction and General Model, defines general concepts and principles of IT security evaluation; presents a general model of evaluation; and defines constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

Part 2, Security Functional Requirements, contains a catalog of well-defined and well-understood functional requirement statements that are intended to be used as a standard way of expressing the security requirements for IT products and systems.

Part 3, Security Assurance Requirements, contains a catalog of assurance components for use as a standard way of expressing such requirements for IT products and systems, and defines evaluation criteria for protection profiles and security targets.

Common IP Security Option (CIPSO): See: secondary definition under "IPSO".

Common name: A character string that

(a) May be a part of the X.500 DN of a Directory object ("commonName" attribute)

(b) Is a (possibly ambiguous) name by which the object is commonly known in some limited scope (such as an organization), and

(c) Conforms to the naming conventions of the country or culture with which it is associated. (See: "subject" and "issuer" under "X.509 public-key certificate".)

Communications cover: "Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary." (See: operations security, traffic-flow confidentiality, TRANSEC.)

Communication security (COMSEC): Measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities.

Usage: COMSEC is usually understood to include

(a) cryptography and its related algorithms and key management methods and processes, devices that implement those algorithms and processes, and the lifecycle management of the devices and keying material. Also, COMSEC is sometimes more broadly understood as further including

(b) traffic-flow confidentiality,

(c) TRANSEC, and

(d) Steganography. (See: cryptology, signal security.)

Community of interest (COI):

1. A set of entities that operate under a common security policy. (Compare: domain.)
2. A set of entities that exchange information collaboratively for some purpose.

Community risk: Probability that a particular vulnerability will be exploited within an interacting population and adversely affect some members of that population.

Community string: A community name in the form of an octet string that serves as a cleartext password in SNMP version 1 and version 2. (See: password, Simple Network Management Protocol.)

Tutorial: The SNMPv1 and SNMPv2 protocols have been declared "historic" and have been replaced by the more secure SNMPv3 standard (RFCs 3410-3418), which does not use cleartext passwords.

Compartment

1. A grouping of sensitive information items that require special access controls beyond those normally provided for the basic classification level of the information. (See: compartmented security mode. Compare: category, classification.)

   Usage: The term is usually understood to include the special handling procedures to be used for the information.

2. Synonym for "category".

   Deprecated Usage: This Glossary defines "category" with a slightly narrower meaning than "compartment". That is, a security label is assigned to a category because the data owner needs to handle the data as a compartment. However, a

compartment could receive special protection in a system without being assigned a category label.

Compartmented security mode: A mode of system operation wherein all users having access to the system have the necessary security clearance for the single, hierarchical classification level of all data handled by the system, but some users do not have the clearance for a nonhierarchical category of some data handled by the system. (See: category, (system operation) under "mode", protection level, security clearance.)

Usage: Usually abbreviated as "compartmented mode". This term was defined in U.S. Government policy on system accreditation. In this mode, a system may handle:

(a) A single hierarchical classification level and

(b) Multiple non-hierarchical categories within that level.

Compartments field: A 16-bit field (the "C field") that specifies compartment values in the security option (option type 130) of version 4 IP's datagram header format. The valid field values are assigned by the U.S. Government.

Deprecated Abbreviation: DOCUMENTS SHOULD NOT use the abbreviation "C field"; the abbreviation is potentially ambiguous. Instead, use "Compartments field".

Component: See: system component.

Compression: A process that encodes information in a way that minimizes the number of resulting code symbols and thus reduces storage space or transmission time.

Tutorial: A data compression algorithm may be "lossless", i.e. retain all information that was encoded in the data, so that decompression can recover all the information; or an algorithm may be "lossy". Text usually needs to be compressed losslessly, but images are often compressed with lossy schemes. Not all schemes that encode information losslessly for machine processing are efficient in terms of minimizing the number of output bits. For example, ASCII encoding is lossless, but ASCII data can often be losslessly reencoded in fewer bits with other schemes. These more efficient schemes take advantage of some sort of inherent imbalance, redundancy, or repetition in the data, such as by replacing a character string in which all characters are the same by a shorter string consisting of only the single character and a character count.

Lossless compression schemes cannot effectively reduce the number of bits in cipher text produced by a strong encryption algorithm, because the cipher text is essentially a pseudorandom bit string that does not contain patterns susceptible to re-encoding. Therefore, protocols that offer both encryption and compression

services (e.g., SSL) need to perform the compression operation before the encryption operation.

Compromise: See: data compromise, security compromise.

Compromise recovery: The process of regaining a secure state for a system after detecting that the system has experienced a security compromise.

Compromised key list (CKL): **(**MISSI) A list that identifies keys for which unauthorized disclosure or alteration may have occurred. (See: compromise.)

Tutorial: A CKL is issued by a CA, like a CRL is issued. But a CKL lists only KMIDs, not subjects that hold the keys, and not certificates in which the keys are bound.

COMPUSEC: See: computer security.

Computer emergency response team (CERT): An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security. (See: CSIRT, security incident.)

Computer Incident Advisory Capability (CIAC): The centralized CSIRT of the U.S. Department of Energy; a member of FIRST.

Computer network: A collection of host computers together with the subnetwork or internetwork through which they can exchange data. Usage: This definition is intended to cover systems of all sizes and types, ranging from the complex Internet to a simple system composed of a personal computer dialing in as a remote terminal of another computer.

Computer platform: A combination of computer hardware and an operating system (which may consist of software, firmware, or both) for that hardware. (Compare: computer system.)

Computer security (COMPUSEC):

1. Measures to implement and assure security services in a computer system, particularly those that assure access control service.

   Usage: Usually refers to internal controls (functions, features, and technical characteristics) that are implemented in software (especially in operating systems); sometimes refers to internal controls implemented in hardware; rarely used to refer to external controls.

2. "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information (data, and telecommunications)."

Computer security incident response team (CSIRT): An organization "that coordinates and supports the response to security incidents that involve sites within a defined constituency." (See: CERT, FIRST, security incident.)

Tutorial: To be considered a CSIRT, an organization must do as follows:

(a) Provide a (secure) channel for receiving reports about suspected security incidents.

(b) Provide assistance to members of its constituency in handling the incidents.

(c) Disseminate incident-related information to its constituency and other involved parties.

Computer security object: The definition or representation of a resource, tool, or mechanism used to maintain a condition of security in computerized environments. Includes many items referred to in standards that are either selected or defined by separate user communities. (See: object identifier, Computer Security Objects Register.)

Computer Security Objects Register (CSOR): A service operated by NIST is establishing a catalog for computer security objects to provide stable object definitions identified by unique names. The use of this register will enable the unambiguous specification of security parameters and algorithms to be used in secure data exchanges. (See: object identifier.)

Tutorial: The CSOR follows registration guidelines established by the international standards community and ANSI. Those guidelines establish minimum responsibilities for registration authorities and assign the top branches of an international registration hierarchy. Under that international registration hierarchy, the CSOR is responsible for the allocation of unique identifiers under the branch: {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3)}.

Computer system: Synonym for "information system", or a component thereof. (Compare: computer platform.)

Computers At Risk: The 1991 report of the System Security Study Committee, sponsored by the U.S. National Academy of Sciences and supported by the Defense Advanced Research Projects Agency of the U.S. DoD. It made many recommendations for industry and governments to improve computer security and trustworthiness. Some of the most important recommendations (e.g., establishing an Information Security Foundation chartered by the U.S. Government) have not been implemented at all, and others (e.g., codifying Generally Accepted System Security Principles similar to accounting principles) have been implemented but not widely adopted.

COMSEC: See: communication security.

COMSEC account: **(**U.S. Government) "Administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material." (See: COMSEC custodian.)

COMSEC accounting: **(**U.S. Government) The process of creating, collecting, and maintaining data records that describe the status and custody of designated items of COMSEC material. (See: accounting legend code.)

Tutorial: Almost any secure information system needs to record a security audit trail, but a system that manages COMSEC material needs to record additional data about the status and custody of COMSEC items.

COMSEC tracking: The process of automatically collecting, recording, and managing information that describes the status of designated items of COMSEC material at all times during each product's lifecycle.

COMSEC controlling: The process of supplementing tracking data with custody data, which consists of explicit acknowledgements of system entities that they:

(a) Have received specific COMSEC items and

(b) Are responsible for preventing exposure of those items.

For example, a key management system that serves a large customer base needs to record tracking data for the same reasons that a national parcel delivery system does, i.e., to answer the question "Where is that thing now?". If keys are encrypted immediately upon generation and handled only in BLACK form between the point of generation and the point of use, then tracking may be all that is needed. However, in cases where keys are handled at least partly in RED form and are potentially subject to exposure, then tracking needs to be supplemented by controlling. Data that is used purely for tracking need be retained only temporarily, until an item's status changes. Data that is used for controlling is retained indefinitely to ensure accountability and support compromise recovery.

COMSEC boundary: "Definable perimeter encompassing all hardware, firmware, and software components performing critical COMSEC functions, such as key generation and key handling and storage." (Compare: cryptographic boundary.)

COMSEC custodian: **(**U.S. Government) "Individual designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding, and destruction of COMSEC material assigned to a COMSEC account."

COMSEC material: **(**U.S. Government) Items designed to secure or authenticate communications or information in general; these items include (but are not limited to) keys; equipment, devices, documents, firmware, and software that embodies or describes cryptographic logic; and other items that perform COMSEC functions. (Compare: keying material.)

COMSEC Material Control System (CMCS): **(**U.S. Government) "Logistics and accounting system through which COMSEC material marked 'CRYPTO' is distributed, controlled, and safeguarded." (See: COMSEC account, COMSEC custodian.)

Confidentiality: See: data confidentiality.

Concealment system: "A method of achieving confidentiality in which sensitive information is hidden by embedding it in irrelevant data." (Compare: steganography.)

Configuration control: The process of regulating changes to hardware, firmware, software, and documentation throughout the development and operational life of a system. (See: administrative security, harden, trusted distribution.)

Tutorial: Configuration control helps protect against unauthorized or malicious alteration of a system and thus provides assurance of system integrity. (See: malicious logic.)

Confinement property: **(**formal model) Property of a system whereby a subject has write access to an object only if the classification of the object dominates the clearance of the subject. (See: *-property, Bell- LaPadula model.)

Constraint: **(**access control) A limitation on the function of an identity, role, or privilege. (See: rule-based access control.)

Tutorial: In effect, a constraint is a form of security policy and may be either static or dynamic:

"Static constraint": A constraint that must be satisfied at the time the policy is defined, and then continues to be satisfied until the constraint is removed.

"Dynamic constraint": A constraint that may be defined to apply at various times that the identity, role, or other object of the constraint is active in the system.

Content filter: **(**World Wide Web) Application software used to prevent access to certain Web servers, such as by parents who do not want their children to access pornography. (See: filter, guard.)

Tutorial: The filter is usually browser-based, but could be part of an intermediate cache server. The two basic content filtering techniques are (a) to block a specified list of URLs and (b) to block material that contains specified words and phrases.

Contingency plan: A plan for emergency response, backup operations, and post disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis. (See: availability.)

Control zone: "The space, expressed in feet of radius, surrounding equipment processing sensitive information that is under sufficient physical and technical control to preclude an unauthorized entry or compromise." (Compare: inspectable space, TEMPEST zone.)

Controlled access protection: (TCSEC) The level of evaluation criteria for a C2 computer system.

Tutorial: The major features of the C2 level are individual accountability, audit, access control, and object reuse.

Controlled cryptographic item (CCI): (U.S. Government) "Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements." (Compare: EUCI.)

Tutorial: This category of equipment was established in 1985 to promote broad use of secure equipment for protecting both classified and unclassified information in the national interest. CCI equipment uses a classified cryptographic logic, but the hardware or firmware embodiment of that logic is unclassified. Drawings, software implementations, and other descriptions of that logic remain classified.

Controlled interface: A mechanism that facilitates the adjudication of the different security policies of interconnected systems. (See: domain, guard.)

Controlled security mode: A mode of system operation wherein

(a) Two or more security levels of information are allowed to be handled concurrently within the same system when some users having access to the system have neither a security clearance nor need-to-know for some of the data handled by the system,

(b) Separation of the users and the classified material on the basis, respectively, of clearance and classification level are not dependent only on operating system control (like they are in multilevel security mode). (See: (system operation (under "mode", protection level.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term. It was defined in a U.S. Government policy regarding system accreditation and was subsumed by "partitioned security mode" in a later policy. Both terms were dropped in still later policies.

Tutorial: Controlled mode was intended to encourage ingenuity in meeting data confidentiality requirements in ways less restrictive than "dedicated security mode" and "system-high security mode", but at a level of risk lower than that generally associated with true "multilevel security mode". This was intended to be accomplished by implementation of explicit augmenting measures to reduce or

remove a substantial measure of system software vulnerability together with specific limitation of the security clearance levels of users having concurrent access to the system.

Controlling authority: (U.S. Government) "Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet."

Cookie:

1. (HTTP) Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.

   Tutorial: An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections. A cookie may include a description of the range of URLs for which the state is valid. Future requests made by the client in that range will also send the current value of the cookie to the server. Cookies can be used to generate profiles of web usage habits, and thus may infringe on personal privacy.

2. (IPsec) Data objects exchanged by ISAKMP to prevent certain denial-of-service attacks during the establishment of a security association.

3. (access control) Synonym for "capability token" or "ticket".

Coordinated Universal Time (UTC): UTC is derived from International Atomic Time (TAI) by adding a number of leap seconds. The International Bureau of Weights and Measures computes TAI once each month by averaging data from many laboratories. (See: Generalized Time, UTC Time.)

Correction: (security) A system change made to eliminate or reduce the risk of reoccurrence of a security violation or threat consequence. (See: secondary definition under "security".)

Correctness: "The property of a system that is guaranteed as the result of formal verification activities." (See: correctness proof, verification.)

Correctness integrity: The property that the information represented by data is accurate and consistent. (Compare: data integrity, source integrity.)

Tutorial: DOCUMENTS SHOULD NOT use this term without providing a definition; the term is neither well-known nor precisely defined. Data integrity refers to the constancy of data values, and source integrity refers to confidence in data values. However, correctness integrity refers to confidence in the underlying information that data values represent, and this property is closely related to issues of accountability and error handling.

Correctness proof: A mathematical proof of consistency between a specification for system security and the implementation of that specification. (See: correctness, formal specification.)

Corruption: A type of threat action that undesirably alters system operation by adversely modifying system functions or data. (See: disruption.)

Usage: This type of threat action includes the following subtypes:

"Tampering": (corruption) Deliberately altering a system's logic, data, or control information to interrupt or prevent correct operation of system functions. (See: misuse, main entry for "tampering".)

"Malicious logic": (corruption) Any hardware, firmware, or software (e.g., a computer virus) intentionally introduced into a system to modify system functions or data. (See: incapacitation, main entry for "malicious logic", masquerade, misuse.)

"Human error": (corruption) Human action or inaction that unintentionally results in the alteration of system functions or data.

"Hardware or software error": (corruption) Error that results in the alteration of system functions or data.

"Natural disaster": (corruption) Any "act of God" (e.g., power surge caused by lightning) that alters system functions or data.

Counter:

1. (noun) See: counter mode.
2. (verb) See: countermeasure.

Counter-countermeasure: An action, device, procedure, or technique used by an attacker to offset a defensive countermeasure.

Tutorial: For every countermeasure devised to protect computers and networks, some cracker probably will be able to devise a counter-countermeasure. Thus, systems must use "defense in depth".

Counter mode (CTR): A block cipher mode that enhances ECB mode by ensuring that each encrypted block is different from every other block encrypted under the same key. (See: block cipher.)

Tutorial: This mode operates by first encrypting a generated sequence of blocks, called "counters", that are separate from the input sequence of plaintext blocks which the mode is intended to protect. The resulting sequence of encrypted counters is exclusive-ORed with the sequence of plaintext blocks to produce the final ciphertext output blocks. The sequence of counters must have the property that each counter is different from every other counter for all of the plain text that is encrypted under the same key.

Counter with Cipher Block Chaining-Message Authentication Code (CCM): A block cipher mode that provides both data confidentiality and data origin authentication, by combining the techniques of CTR and a CBC-based message authentication code. (See: block cipher.)

Countermeasure: An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Tutorial: In an Internet protocol, a countermeasure may take the form of a protocol feature, a component function, or a usage constraint.

Country code: An identifier that is defined for a nation by ISO

Tutorial: For each nation, ISO Standard 3166 defines a unique two character alphabetic code, a unique three-character alphabetic code, and a three-digit code. Among many uses of these codes, the two-character codes are used as top-level domain names.

Courtney's laws: Principles for managing system security that were stated by Robert H. Courtney, Jr.

Tutorial: Bill Murray codified Courtney's laws as follows:

Courtney's first law: You cannot say anything interesting (i.e., significant) about the security of a system except in the context of a particular application and environment.

Courtney's second law: Never spend more money eliminating a security exposure than tolerating it will cost you. (See: acceptable risk, risk analysis.)

Courtney's third law: There are no technical solutions to management problems, but there are management solutions to technical problems.

Covert action: An operation that is planned and executed in a way that conceals the identity of the operator.

Covert channel:

1. An unintended or unauthorized intra-system channel that enables two cooperating entities to transfer information in a way that violates the system's security policy but does not exceed the entities' access authorizations. (See: covert storage channel, covert timing channel, out-of-band, tunnel.)
2. "A communications channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy."

Tutorial: The cooperating entities can be either two insiders or an insider and an outsider. Of course, an outsider has no access authorization at all. A covert

channel is a system feature that the system architects neither designed nor intended for information transfer.

Covert storage channel: A system feature that enables one system entity to signal information to another entity by directly or indirectly writing a storage location that is later directly or indirectly read by the second entity. (See: covert channel.)

Covert timing channel: A system feature that enables one system entity to signal information to another by modulating its own use of a system resource in such a way as to affect system response time observed by the second entity. (See: covert channel.)

CPS: See: certification practice statement.

Cracker: Someone who tries to break the security of, and gain unauthorized access to, someone else's system, often with malicious intent. (See: adversary, intruder, packet monkey, script kiddy. Compare: hacker.)

Usage: Was sometimes spelled "kracker".

CRAM: See: Challenge-Response Authentication Mechanism.

CRC: See: cyclic redundancy check.

Credential:

1. (authentication) "identifier credential": A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in verifying an identity claimed by an entity that attempts to access a system. Example: X.509 public-key certificate. (See: anonymous credential.)
2. (access control) "authorization credential": A data object that is a portable representation of the association between an identifier and one or more access authorizations, and that can be presented for use in verifying those authorizations for an entity that attempts such access. Example: X.509 attribute certificate. (See: capability token, ticket.)
3. (OSI-RM) "Data that is transferred to establish the claimed identity of an entity."

   Deprecated Definition: DOCUMENTS SHOULD NOT use the term with definition 3. As explained in the tutorial below, an authentication process can involve the transfer of multiple data objects, and not all of those are credentials.

4. (U.S. Government) "An object that is verified when presented to the verifier in an authentication transaction."

   Deprecated Definition: DOCUMENTS SHOULD NOT use the term with definition 4; it mixes concepts in a potentially misleading way. For example, in an authentication process, it is the identity that is "verified", not the credential; the credential is "validated". (See: validate vs. verify.)

Tutorial: In general English, "credentials" are evidence or testimonials that (a) support a claim of identity or authorization and (b) usually are intended to be used more than once (i.e., a credential's life is long compared to the time needed for one use). Some examples are a policeman's badge, an automobile driver's license, and a national passport. An authentication or access control process that uses a badge, license, or passport is outwardly simple: the holder just shows the thing.

The problem with adopting this term in Internet security is that an automated process for authentication or access control usually requires multiple steps using multiple data objects, and it might not be immediately obvious which of those objects should get the name "credential".

For example, if the verification step in a user authentication process employs public-key technology, then the process involves at least three data items: (a) the user's private key, (b) a signed value -- signed with that private key and passed to the system, perhaps in response to a challenge from the system – and (c) the user's public-key certificate, which is validated by the system and provides the public key needed to verify the signature. - Private key: The private key is *not* a credential, because it is never transferred or presented. Instead, the private key is "authentication information", which is associated with the user's identifier for a specified period of time and can be used in multiple authentications during that time.

Signed value: The signed value is *not* a credential; the signed value is only ephemeral, not long lasting. The OSI-RM definition could be interpreted to call the signed value a credential, but that would conflict with general English.

Certificate: The user's certificate *is* a credential. It can be "transferred" or "presented" to any person or process that needs it at any time. A public-key certificate may be used as an "identity credential", and an attribute certificate may be used as an "authorization credential".

Critical:

1. (system resource) A condition of a system resource such that denial of access to, or lack of availability of, that resource would jeopardize a system user's ability to perform a primary function or would result in other serious consequences, such as human injury or loss of life. (See: availability, precedence. Compare: sensitive.)

2. (extension) An indication that an application is not permitted to ignore an extension.

   Tutorial: Each extension of an X.509 certificate or CRL is flagged as either "critical" or "non-critical". In a certificate, if a computer program does not recognize an extension's type (i.e., does not implement its semantics), then if the extension

is critical, the program is required to treat the certificate as invalid; but if the extension is non-critical, the program is permitted to ignore the extension.

In a CRL, if a program does not recognize a critical extension that is associated with a specific certificate, the program is required to assume that the listed certificate has been revoked and is no longer valid, and then take whatever action is required by local policy.

When a program does not recognize a critical extension that is associated with the CRL as a whole, the program is required to assume that all listed certificates have been revoked and are no longer valid. However, since failing to process the extension may mean that the list has not been completed, the program cannot assume that other certificates are valid, and the program needs to take whatever action is therefore required by local policy.

Critical information infrastructure: Those systems that are so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety.

CRL: See: certificate revocation list.

CRL distribution point: See: distribution point.

CRL extension: See: extension.

Cross-certificate: A public-key certificate issued by a CA in one PKI to a CA in another PKI. (See: cross-certification.)

Cross-certification: The act or process by which a CA in one PKI issues a public key certificate to a CA in another PKI. (See: bridge CA.)

Tutorial: X.509 says that a CA (say, CA1) may issue a "cross-certificate" in which the subject is another CA (say, CA2). X.509 calls CA2 the "subject CA" and calls CA1 an "intermediate CA", but this Glossary deprecates those terms. (See: intermediate CA, subject CA). Cross-certification of CA2 by CA1 appears similar to certification of a subordinate CA by a superior CA, but cross-certification involves a different concept. The "subordinate CA" concept applies when both CAs are in the same PKI, i.e., when either (a) CA1 and CA2 are under the same root or (b) CA1 is itself a root. The "cross-certification" concept applies in other cases:

First, cross-certification applies when two CAs are in different PKIs, i.e., when CA1 and CA2 are under different roots, or perhaps are both roots themselves. Issuing the cross-certificate enables end entities certified under CA1 in PK1 to construct the certification paths needed to validate the certificates of end entities certified under CA2 in PKI2. Sometimes, a pair of cross-certificates is issued -- by CA1 to CA2, and by CA2 to CA1 – so that an end entity in either PKI can validate certificates issued in the other PKI.

Second, X.509 says that two CAs in some complex, multi-CA PKI can cross-certify one another to shorten the certification paths constructed by end entities. Whether or not a CA may perform this or any other form of cross-certification, and how such certificates may be used by end entities, should be addressed by the local certificate policy and CPS.

Cross-domain solution:

1. Synonym for "guard".

   Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for "guard"; this term unnecessarily (and verbosely) duplicates the meaning of the long-established "guard".

2. (U.S. Government) A process or subsystem that provides a capability (which could be either manual or automated) to access two or more differing security domains in a system, or to transfer information between such domains. (See: domain, guard.)

Cryptanalysis:

1. The mathematical science that deals with analysis of a cryptographic system to gain knowledge needed to break or circumvent the protection that the system is designed to provide. (See: cryptology, secondary definition under "intrusion".)

2. "The analysis of a cryptographic system and (or its inputs and outputs to derive confidential variables and-or sensitive data including cleartext."

   Tutorial: Definition 2 states the traditional goal of cryptanalysis, i.e., convert cipher text to plain text (which usually is clear text) without knowing the key; but that definition applies only to encryption systems. Today, the term is used with reference to all kinds of cryptographic algorithms and key management, and definition 1 reflects that. In all cases, however, a cryptanalyst tries to uncover or reproduce someone else's sensitive data, such as clear text, a key, or an algorithm.

   The basic cryptanalytic attacks on encryption systems are ciphertext-only, known-plaintext, chosen-plaintext, and chosen cipher text; and these generalize to the other kinds of cryptography.

Crypto, CRYPTO:

1. A prefix ("crypto-") that means "cryptographic".

   Usage: DOCUMENTS MAY use this prefix when it is part of a term listed in this Glossary. Otherwise, DOCUMENTS SHOULD NOT use this prefix; instead, use the unabbreviated adjective, "cryptographic".

2. In lower case, "crypto" is an abbreviation for the adjective "cryptographic", or for the nouns "cryptography" or "cryptographic component".

Deprecated Abbreviation: DOCUMENTS SHOULD NOT use this abbreviation because it could easily be misunderstood in some technical sense.

3. (U.S. Government) In upper case, "CRYPTO" is a marking or designator that identifies "COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information." (See: security label, security marking.)

Cryptographic: An adjective that refers to cryptography.

Cryptographic algorithm: An algorithm that uses the science of cryptography, including

(a) encryption algorithms,

(b) cryptographic hash algorithms,

(c) digital signature algorithms, and

(d) key-agreement algorithms.

Cryptographic application programming interface (CAPI): The source code formats and procedures through which an application program accesses cryptographic services, which are defined abstractly compared to their actual implementation. Example, see: PKCS #11

Cryptographic association: A security association that involves the use of cryptography to provide security services for data exchanged by the associated entities. (See: ISAKMP.)

Cryptographic boundary: See: secondary definition under "cryptographic module".

Cryptographic card: A cryptographic token in the form of a smart card or a PC card.

Cryptographic component: A generic term for any system component that involves cryptography. (See: cryptographic module.)

Cryptographic hash: See: secondary definition under "hash function".

Cryptographic ignition key (CIK)

1. A physical (usually electronic) token used to store, transport, and protect cryptographic keys and activation data. (Compare: dongle, fill device.)

   Tutorial: A key-encrypting key could be divided (see: split key) between a CIK and a cryptographic module, so that it would be necessary to combine the two to regenerate the key, use it to decrypt other keys and data contained in the module, and thus activate the module.

2. "Device or electronic key used to unlock the secure mode of cryptographic equipment." Usage: Abbreviated as "crypto-ignition key".

Cryptographic key: See: key. Usage: Usually shortened to just "key".

Cryptographic Message Syntax (CMS): An encapsulation syntax for digital signatures, hashes, and encryption of arbitrary messages.

Tutorial: CMS derives from PKCS #7. CMS values are specified with ASN.1 and use BER encoding. The syntax permits multiple encapsulation with nesting, permits arbitrary attributes to be signed along with message content, and supports a variety of architectures for digital certificate-based key management.

Cryptographic module: A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the module's "cryptographic boundary", which is an explicitly defined contiguous perimeter that establishes the physical bounds of the module.

Cryptographic system:

1. A set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context.

   Usage: DOCUMENTS SHOULD use definition 1 because it covers a wider range of algorithms than definition 2.

2. "A collection of transformations from plain text into cipher text and vice versa [which would exclude digital signature, cryptographic hash, and key-agreement algorithms], the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm."

Cryptographic token: A portable, user-controlled, physical device (e.g., smart card or PCMCIA card) used to store cryptographic information and possibly also perform cryptographic functions. See: cryptographic card, token.)

Tutorial: A smart token might implement some set of cryptographic algorithms and might incorporate related key management functions, such as a random number generator. A smart cryptographic token may contain a cryptographic module or may not be explicitly designed that way.

Cryptography:

1. The mathematical science that deals with transforming data to render its meaning unintelligible (i.e., to hide its semantic content), prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form. (See: cryptology, steganography.)

2. "The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and or prevent its unauthorized use.... Cryptography determines the methods used in encipherment and decipherment."

Tutorial: Comprehensive coverage of applied cryptographic protocols and algorithms is provided by Schneier. Businesses and governments use cryptography to make data incomprehensible to outsiders; to make data incomprehensible to both outsiders and insiders, the data is sent to lawyers for a rewrite.

Cryptoki: A CAPI defined in PKCS #11. Pronunciation: "CRYPTO-key". Derivation: Abbreviation of "cryptographic token interface".

Cryptology: The science of secret communication, which includes both cryptography and cryptanalysis. Sometimes the term is used more broadly to denote activity that includes both rendering signals secure (see: signal security) and extracting information from signals (see: signal intelligence).

Cryptonet: A network (i.e., a communicating set) of system entities that share a secret cryptographic key for a symmetric algorithm. (See: controlling authority.) "Stations holding a common key."

Cryptoperiod: The time span during which a particular key value is authorized to be used in a cryptographic system. (See: key management.)

Usage: This term is long-established in COMPUSEC usage. In the context of certificates and public keys, "key lifetime" and "validity period" are often used instead.

Tutorial: A crypto-period is usually stated in terms of calendar or clock time, but sometimes is stated in terms of the maximum amount of data permitted to be processed by a cryptographic algorithm using the key. Specifying a crypto-period involves a tradeoff between the cost of rekeying and the risk of successful cryptoanalysis.

Cryptosystem: Contraction of "cryptographic system".

Cryptovariable: Synonym for "key".

Deprecated Usage: In contemporary COMSEC usage, the term "key" has replaced the term "crypto-variable".

CSIRT: See: computer security incident response team.

CTAK: See: cipher-text auto-key.

CTR: See: counter mode.

Cut-and-paste attack: An active attack on the data integrity of cipher text, effected by replacing sections of cipher text with other cipher text, such that the result appears to decrypt correctly but actually decrypts to plain text that is forged to the satisfaction of the attacker.

Cyclic redundancy check (CRC): A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where

accidental changes to data are expected. Sometimes called "cyclic redundancy code".

Daemon: A computer program that is not invoked explicitly but waits until a specified condition occurs, and then runs with no associated user (principal), usually for an administrative purpose. (See: zombie.)

Dangling threat: A threat to a system for which there is no corresponding vulnerability and, therefore, no implied risk.

Dangling vulnerability: A vulnerability of a system for which there is no corresponding threat and, therefore, no implied risk.

DASS: See: Distributed Authentication Security Service.

Data: Information in a specific representation, usually as a sequence of symbols that have meaning. Usage: Refers to both

(a) Representations that can be recognized, processed, or produced by a computer or other type of machine, and

(b) Representations that can be handled by a human.

Data Authentication Algorithm, data authentication algorithm

1. (capitalized) The ANSI standard for a keyed hash function that is equivalent to DES cipher block chaining with IV = 0.

2. (not capitalized) Synonym for some kind of "checksum". Please do not use the uncapitalized form "data authentication algorithm" as a synonym for any kind of checksum, Instead, use "checksum", "Data Authentication Code", "error detection code", "hash", "keyed hash", "Message Authentication Code", "protected checksum", or some other specific term, depending on what is meant.

   The uncapitalized term can be confused with the Data Authentication Code and also mixes concepts in a potentially misleading way. The word "authentication" is misleading because the checksum may be used to perform a data integrity function rather than a data origin authentication function.

Data Authentication Code, data authentication code:

1. (capitalized) A specific U.S. Government standard for a checksum that is computed by the Data Authentication Algorithm. Usage: a.k.a. Message Authentication Code.) (See: DAC.)

2. (not capitalized) Synonym for some kind of "checksum".

   Deprecated Term: DOCUMENTS SHOULD NOT use the uncapitalized form "data authentication code" as a synonym for any kind of checksum, regardless of whether or not the checksum is based on the Data

Authentication Algorithm. The uncapitalized term can be confused with the Data Authentication Code and also mixes concepts in a potentially misleading way (see: authentication code).

Data compromise:

1. A security incident in which information is exposed to potential unauthorized access, such that unauthorized disclosure, alteration, or use of the information might have occurred. (Compare: security compromise, security incident.)
2. (U.S. DoD) A "compromise" is a "communication or physical transfer of information to an unauthorized recipient."
3. (U.S. Government) "Type of [security] incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred."

Data confidentiality:

1. The property that data is not disclosed to system entities unless they have been authorized to know the data. (See: Bell-LaPadula model, classification, data confidentiality service, secret. Compare: privacy.)
2. "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]."

   Deprecated Definition: The phrase "made available" might be interpreted to mean that the data could be altered, and that would confuse this term with the concept of "data integrity".

Data confidentiality service: A security service that protects data against unauthorized disclosure. (See: access control, data confidentiality, datagram confidentiality service, flow control, inference control.)

Data Encryption Algorithm (DEA): A symmetric block cipher, defined in the U.S. Government's DES. DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block. (See: AES, symmetric cryptography.)

Usage: This algorithm is usually referred to as "DES". The algorithm has also been adopted in standards outside the Government.

Data encryption key (DEK): A cryptographic key that is used to encipher application data. (Compare: key-encrypting key.)

Data Encryption Standard (DES): A U.S. Government standard that specifies the DEA and states policy for using the algorithm to protect unclassified, sensitive data. (See: AES.)

Data integrity:

1. The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (See: data integrity service. Compare: correctness integrity, source integrity.)
2. "The property that information has not been modified or destroyed in an unauthorized manner."

   Usage: Deals with

   (a) Constancy of and confidence in data values, and not with either

   (b) Information that the values represent (see: correctness integrity) or

   (c) The trustworthiness of the source of the values (see: source integrity).

Data integrity service: A security service that protects against unauthorized changes to data, including both intentional change or destruction and accidental change or loss, by ensuring that changes to data are detectable. (See: data integrity, checksum, datagram integrity service.)

Tutorial: A data integrity service can only detect a change and report it to an appropriate system entity; changes cannot be prevented unless the system is perfect (error-free) and no malicious user has access. However, a system that offers data integrity service might also attempt to correct and recover from changes.

The ability of this service to detect changes is limited by the technology of the mechanisms used to implement the service. For example, if the mechanism were a one-bit parity check across each entire SDU, then changes to an odd number of bits in an SDU would be detected, but changes to an even number of bits would not.

Relationship between data integrity service and authentication services: Although data integrity service is defined separately from data origin authentication service and peer entity authentication service, it is closely related to them.

Authentication services depend, by definition, on companion data integrity services. Data origin authentication service provides verification that the identity of the original source of received data unit is as claimed; there can be no such verification if the data unit has been altered. Peer entity authentication service provides verification that the identity of a peer entity in a current association is as claimed; there can be no such verification if the claimed identity has been altered.

Data origin authentication: "The corroboration that the source of data received is as claimed." (See: authentication.)

Data origin authentication service: A security service that verifies the identity of a system entity that is claimed to be the original source of received data. (See: authentication, authentication service.)

Tutorial: This service is provided to any system entity that receives or holds the data. Unlike peer entity authentication service, this service is independent of any association between the originator and the recipient, and the data in question may have originated at any time in the past.

A digital signature mechanism can be used to provide this service, because someone who does not know the private key cannot forge the correct signature. However, by using the signer's public key, anyone can verify the origin of correctly signed data.

This service is usually bundled with connectionless data integrity service. (See: "relationship between data integrity service and authentication services" under "data integrity service".

Data owner: The organization that has the final statutory and operational authority for specified information.

Data privacy: Synonym for "data confidentiality".

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it mixes concepts in a potentially misleading way. Instead, use either "data confidentiality" or "privacy" or both, depending on what is meant.

Data recovery:

1. (cryptanalysis) A process for learning, from some cipher text, the plain text that was previously encrypted to produce the cipher text. (See: recovery.)
2. **(**System integrity) The process of restoring information following damage or destruction.

Data security: The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorized.

Tutorial: Both data confidentiality service and data integrity service are needed to achieve data security.

Datagram: "A self-contained, independent entity of data [i.e., a packet] carrying sufficient information to be routed from the source [computer] to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." Example: A PDU of IP.

Datagram confidentiality service: A data confidentiality service that preserves the confidentiality of data in a single, independent, packet; i.e., the service applies to datagrams one-at-a-time. Example: ESP. (See: data confidentiality.)

Usage: When a protocol is said to provide data confidentiality service, this is usually understood to mean that only the SDU is protected in each packet. DOCUMENTs that use the term to mean that the entire PDU is protected should include a highlighted definition.

Tutorial: This basic form of network confidentiality service suffices for protecting the data in a stream of packets in both connectionless and connection-oriented protocols. Except perhaps for traffic flow confidentiality, nothing further is needed to protect the confidentiality of data carried by a packet stream. The OSI-RM distinguishes between connection confidentiality and connectionless confidentiality. The IPS need not make that distinction, because those services are just instances of the same service (i.e., datagram confidentiality) being offered in two different protocol contexts. (For data integrity service, however, additional effort is needed to protect a stream, and the IPS does need to distinguish between "datagram integrity service" and "stream integrity service".)

Datagram integrity service: A data integrity service that preserves the integrity of data in a single, independent, packet; i.e., the service applies to datagrams one-at-a-time. (See: data integrity. Compare: stream integrity service.)

Tutorial: The ability to provide appropriate data integrity is important in many Internet security situations, and so there are different kinds of data integrity services suited to different applications. This service is the simplest kind; it is suitable for connectionless data transfers.

Datagram integrity service usually is designed only to attempt to detect changes to the SDU in each packet, but it might also attempt to detect changes to some or all of the PCI in each packet (see: selective field integrity). In contrast to this simple, one-at-a-time service, some security situations demand a more complex service that also attempts to detect deleted, inserted, or reordered datagrams within a stream of datagrams (see: stream integrity service).

DEA: See: Data Encryption Algorithm.

Deception: A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. (See: authentication.)

Tutorial: This is a type of threat consequence, and it can be caused by the following types of threat actions: masquerade, falsification, and repudiation.

Decipher: Synonym for "decrypt".

Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "decrypt". However, see usage note under "encryption".

Decipherment: Synonym for "decryption".

Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "decryption". However, see the Usage note under "encryption".

Declassification: An authorized process by which information is declassified. (Compare: classification.)

Declassify: To officially remove the security level designation of a classified information item or information type, such that the information is no longer classified (i.e., becomes unclassified). (See: classified, classify, security level. Compare: downgrade.)

Decode:

1. Convert encoded data back to its original form of representation. (Compare: decrypt.)
2. Synonym for "decrypt".

   Deprecated Definition: Encoding is not usually meant to conceal meaning. Therefore, DOCUMENTs SHOULD NOT use this term as a synonym for "decrypt", because that would mix concepts in a potentially misleading way.

Decrypt: Cryptographically restore cipher text to the plaintext form it had before encryption.

Decryption: See: secondary definition under "encryption".

Dedicated security mode: A mode of system operation wherein all users having access to the system possess, for all data handled by the system, both

(a) All necessary authorizations (i.e., security clearance and formal access approval) and

(b) A need-to-know. (See: (system operation) under "mode", formal access approval, need to know, protection level, security clearance.)

Usage: Usually abbreviated as "dedicated mode". This mode was defined in U.S. Government policy on system accreditation, but the term is also used outside the Government. In this mode, the system may handle either (a) a single classification level or category of information or (b) a range of levels and categories.

Default account: A system login account (usually accessed with a user identifier and password) that has been predefined in a manufactured system to permit initial access when the system is first put into service. (See: harden.)

Tutorial: A default account becomes a serious vulnerability if not properly administered. Sometimes, the default identifier and password are well-known because they are the same in each copy of the system. In any case, when a system is put into service, any default password should immediately be changed or the default account should be disabled.

Defense in depth: "The siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and [enable] the commander to maneuver the reserve."

Tutorial: In information systems, defense in depth means constructing a system's security architecture with layered and complementary security mechanisms and countermeasures, so that if one security mechanism is defeated, one or more other mechanisms (which are "behind" or "beneath" the first mechanism) still provide protection.

This architectural concept is appealing because it aligns with traditional warfare doctrine, which applies defense in depth to physical, geospatial structures; but applying the concept to logical, cyberspace structures of computer networks is more difficult. The concept assumes that networks have a spatial or topological representation. It also assumes that there can be implemented

- From the "outer perimeter" of a network, through its various "layers" of components, to its "center" (i.e., to the subscriber application systems supported by the network)
- A varied series of countermeasures that together provide adequate protection. However, it is more difficult to map the topology of networks and make certain that no path exists by which an attacker could bypass all defensive layers.

Defense Information Infrastructure (DII): **(**U.S. DoD) The U.S. DoD's shared, interconnected system of computers, communications, data, applications, security, people, training, and support structures, serving information needs worldwide. (See: DISN.) Usage: Has evolved to be called the GIG.

Tutorial: The DII connects mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and provides information processing and value-added services to subscribers over the DISN. Users' own data and application software are not considered part of the DII.

Defense Information Systems Network (DISN): (U.S. DoD) The U.S. DoD's consolidated, worldwide, enterprise level telecommunications infrastructure that provides end-to-end information transfer for supporting military operations; a part of the DII. (Compare: GIG.)

Degauss:

1a. Apply a magnetic field to permanently remove data from a magnetic storage medium, such as a tape or disk [NCS25]. (Compare: erase, purge, sanitize.)

1b. Reduce magnetic flux density to zero by applying a reversing magnetic field. (See: magnetic remanence.)

Degausser: An electrical device that can degauss magnetic storage media.

DEK: See: data encryption key.

Delay: (packet) See: secondary definition under "stream integrity service".

Deletion: (packet) See: secondary definition under "stream integrity service".

Deliberate exposure: (threat action) See: secondary definition under "exposure".

Delta CRL: A partial CRL that only contains entries for certificates that have been revoked since the issuance of a prior, base CRL [X509].

This method can be used to partition CRLs that become too large and unwieldy. (Compare: CRL distribution point.)

Demilitarized zone (DMZ): Synonym for "buffer zone".

Denial of service: The prevention of authorized access to a system resource or the delaying of system operations and functions. (See: availability, critical, flooding.)

Tutorial: A denial-of-service attack can prevent the normal conduct of business on the Internet. There are four types of solutions to this security problem:

Awareness: Maintaining cognizance of security threats and vulnerabilities.

Detection: Finding attacks on end systems and subnetworks.

Prevention: Following defensive practices on network-connected systems.

Response: Reacting effectively when attacks occur.

DES: See: Data Encryption Standard.

Designated approving authority (DAA): (U.S. Government) Synonym for "accreditor".

Detection: See: secondary definition under "security".

Deterrence: See: secondary definition under "security".

Dictionary attack: An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.

Diffie-Hellman-Merkle: A key-agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman.

Usage: The algorithm is most often called "Diffie-Hellman". However, in the November 1978 issue of "IEEE Communications Magazine", Hellman wrote that the algorithm "is a public key distribution system, a concept developed by [Ralph C.] Merkle, and hence should be called 'Diffie-Hellman-Merkle' ... to recognize Merkle's equal contribution to the invention of public key cryptography."

Tutorial: Diffie-Hellman-Merkle does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

The algorithm is described in. In brief, Alice and Bob together pick large integers that satisfy certain mathematical conditions, and then use the integers to each separately compute a public-private key pair. They send each other their public key. Each person uses their own private key and the other person's public key to compute a key,that, because of the mathematics of the algorithm, is the same for

each of them. Passive wiretapping cannot learn the shared k, because k is not transmitted, and neither are the private keys needed to compute k.

The difficulty of breaking Diffie-Hellman-Merkle is considered to be equal to the difficulty of computing discrete logarithms modulo a large prime. However, without additional mechanisms to authenticate each party to the other, a protocol based on the algorithm may be vulnerable to a man-in-the-middle attack.

Digest: See: message digest.

Digital certificate: A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object.

Deprecated Usage: DOCUMENTS SHOULD NOT use this term to refer to a signed CRL or CKL. Although the recommended definition can be interpreted to include other signed items, the security community does not use the term with those meanings.

Digital certification: Synonym for "certification".

Deprecated Definition: DOCUMENTS SHOULD NOT use this definition unless the context is not sufficient to distinguish between digital certification and another kind of certification, in which case it would be better to use "public-key certification" or another phrase that indicates what is being certified.

Digital document: An electronic data object that represents information originally written in a non-electronic, non-magnetic medium (usually ink on paper) or is an analogue of a document of that type.

Digital envelope: A combination of

(a) Encrypted content data (of any kind) intended for a recipient and

(b) The content encryption key in an encrypted form that has been prepared for the use of the recipient.

Usage: In DOCUMENTS, the term SHOULD be defined at the point of first use because, although the term is defined in PKCS #7 and used in S/MIME, it is not widely known.

Tutorial: Digital enveloping is not simply a synonym for implementing data confidentiality with encryption; digital enveloping is a hybrid encryption scheme to "seal" a message or other data, by encrypting the data and sending both it and a protected form of the key to the intended recipient, so that no one other than the intended recipient can "open" the message. In PKCS #7, it means first encrypting the data using a symmetric encryption algorithm and a secret key, and then encrypting the secret key using an asymmetric encryption algorithm.

Digital ID (service mark): Synonym for "digital certificate".

Deprecated Term: DOCUMENTS SHOULD NOT use this term. It is a service mark of a commercial firm, and it unnecessarily duplicates the meaning of a better-established term. (See: credential.)

Digital key: Synonym for an input parameter of a cryptographic algorithm or other process. (See: key.)

Deprecated Usage: The adjective "digital" need not be used with "key" or "cryptographic key", unless the context is insufficient to distinguish the digital key from another kind of key, such as a metal key for a door lock.

Digital notary: An electronic functionary analogous to a notary public. Provides a trusted timestamp for a digital document, so that someone can later prove that the document existed at that point in time; verifies the signature(s) on a signed document before applying the stamp. (See: notarization.)

Digital signature:

1. A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. (See: data origin authentication service, data integrity service, signer. Compare: digitized signature, electronic signature.)

2. "Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient."

   Tutorial: A digital signature should have these properties:

   - Be capable of being verified. (See: validate vs. verify.)
   - Be bound to the signed data object in such a way that if the data is changed, then when an attempt is made to verify the signature, it will be seen as not authentic. (In some schemes, the signature is appended to the signed object as stated by definition 2, but in other it, schemes is not.)
   - Uniquely identify a system entity as being the signer.
   - Be under the signer's sole control, so that it cannot be created by any other entity. To achieve these properties, the data object is first input to a hash function, and then the hash result is cryptographically transformed using a private key of the signer. The final resulting value is called the digital signature of the data object. The signature value is a protected checksum, because the properties of a cryptographic hash ensure that if the data object is changed, the digital signature will no longer match it. The digital signature is unforgeable because one cannot be certain of correctly creating or changing the signature without knowing the private key of the supposed signer.

Some digital signature schemes use an asymmetric encryption algorithm (e.g., "RSA") to transform the hash result. Thus, when Alice needs to sign a message to send to Bob, she can use her private key to encrypt the hash result. Bob receives both the message and the digital signature. Bob can use Alice's public key to decrypt the signature, and then compare the plaintext result to the hash result that he computes by hashing the message himself. If the values are equal, Bob accepts the message because he is certain that it is from Alice and has arrived unchanged. If the values are not equal, Bob rejects the message because either the message or the signature was altered in transit.

Other digital signature schemes (e.g., "DSS") transform the hash result with an algorithm (e.g., "DSA", "El Gamal") that cannot be directly used to encrypt data. Such a scheme creates a signature value from the hash and provides a way to verify the signature value, but does not provide a way to recover the hash result from the signature value. In some countries, such a scheme may improve exportability and avoid other legal constraints on usage. Alice sends the signature value to Bob along with both the message and its hash result. The algorithm enables Bob to use Alice's public signature key and the signature value to verify the hash result he receives. Then, as before, he compares that hash result she sent to the one that he computes by hashing the message himself.

Digital Signature Algorithm (DSA): An asymmetric cryptographic algorithm for a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified. (See: DSS.)

Digital Signature Standard (DSS): The U.S. Government standard that specifies the DSA.

Digital watermarking: Computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data -- text, graphics, images, video, or audio -- and for detecting or extracting the marks later.

Tutorial: A "digital watermark", i.e., the set of embedded bits, is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. Depending on the particular technique that is used, digital watermarking can assist in proving ownership, controlling duplication, tracing distribution, ensuring data integrity, and performing other functions to protect intellectual property rights.

Digitized signature: Denotes various forms of digitized images of handwritten signatures. (Compare: digital signature).

Deprecated Term: DOCUMENTS SHOULD NOT use this term without including this definition. This term suggests careless use of "digital signature", which is the term standardized by. (See: electronic signature.)

DII: See: Defense Information Infrastructure.

Direct attack: See: secondary definition under "attack". (Compare: indirect attack.)

Directory:

1. (Not capitalized) Refers generically to a database server or other system that stores and provides access to values of descriptive or operational data items that are associated with the components of a system. (Compare: repository.)

2. (Capitalized) Refers specifically to the X.500 Directory. (See: DN, X.500.)

Directory Access Protocol (DAP): An OSI protocol [X519] for communication between a Directory User Agent (a type of X.500 client) and a Directory System Agent (a type of X.500 server). (See: LDAP.)

Disaster plan: Synonym for "contingency plan".

Deprecated Term: DOCUMENTS SHOULD NOT use this term; instead, for consistency and neutrality of language, DOCUMENTS SHOULD use "contingency plan".

Disclosure: See: unauthorized disclosure. Compare: exposure.

Discretionary access control:

A. An access control service that:

(a) Enforces a security policy based on the identity of system entities and the authorizations associated with the identities and

(b) Incorporates a concept of ownership in which access rights for a system resource may be granted and revoked by the entity that owns the resource. (See: access control list, DAC, identity-based security policy, mandatory access control.)

Derivation: This service is termed "discretionary" because an entity can be granted access rights to a resource such that the entity can by its own volition enable other entities to access the resource.

B. (formal model) "A means of restricting access to objects based on the identity of subjects and-or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject."

DISN: See: Defense Information Systems Network (DISN).

Disruption: A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Tutorial: Disruption is a type of threat consequence; it can be caused by the following types of threat actions: incapacitation, corruption, and obstruction.

Distinguished Encoding Rules (DER): A subset of the Basic Encoding Rules that always provides only one way to encode any data structure defined by ASN.1. [X690].

Tutorial: For a data structure defined abstractly in ASN.1, BER often provides for encoding the structure into an octet string in more than one way, so that two separate BER implementations can legitimately produce different octet strings for the same ASN.1 definition. However, some applications require all encodings of a structure to be the same, so that encodings can be compared for equality. Therefore, DER is used in applications in which unique encoding is needed, such as when a digital signature is computed on a structure defined by ASN.1.

Distinguished name (DN): An identifier that uniquely represents an object in the X.500 Directory Information Tree. (Compare: domain name, identity, naming authority.)

Tutorial: A DN is a set of attribute values that identify the path leading from the base of the DIT to the object that is named. An X.509 public-key certificate or CRL contains a DN that identifies its issuer, and an X.509 attribute certificate contains a DN or other form of name that identifies its subject.

Distributed attack:

A. An attack that is implemented with distributed computing. (See: zombie.)

B. An attack that deploys multiple threat agents.

Distributed Authentication Security Service (DASS): An experimental Internet protocol that uses cryptographic mechanisms to provide strong, mutual authentication services in a distributed environment.

Distributed computing: A technique that disperses a single, logically related set of tasks among a group of geographically separate yet cooperating computers. (See: distributed attack.)

Distribution point: An X.500 Directory entry or other information source that is named in a v3 X.509 public-key certificate extension as a location from which to obtain a CRL that may list the certificate.

Tutorial: A v3 X.509 public-key certificate may have a "Crl Distribution Points" extension that names places to get CRLs on which the certificate might be listed. (See: certificate profile.)

A CRL obtained from a distribution point may

(a) Cover either all reasons for which a certificate might be revoked or only some of the reasons,

(b) Be issued by either the authority that signed the certificate or some other authority, and

(c) Contain revocation entries for only a subset of the full set of certificates issued by one CA or (d) contain revocation entries for multiple CAs.

DKIM: See: Domain Keys Identified Mail.

DMZ: See: demilitarized zone.

DN: See: distinguished name.

DNS: See: Domain Name System.

Doctrine: See: security doctrine.

DoD: Department of Defense.

Usage: To avoid international misunderstanding, DOCUMENTS SHOULD use this abbreviation only with a national qualifier (e.g., U.S. DoD).

DOI: See: Domain of Interpretation.

Domain:

1a. (general security) An environment or context that (a) includes a set of system resources and a set of system entities that have the right to access the resources and (b) usually is defined by a security policy, security model, or security architecture. Compare: COI, enclave.

Tutorial: A "controlled interface" or "guard" is required to transfer information between network domains that operate under different security policies.

1b. (Security policy) A set of users, their information objects, and a common security policy.

1c. (security policy) A system or collection of systems that (a) belongs to a community of interest that implements a consistent security policy and (b) is administered by a single authority.

2. (COMPUSEC) An operating state or mode of a set of computer hardware.

Tutorial: Most computers have at least two hardware operating modes:

- "Privileged" mode: a.k.a. "executive", "master", "system", "kernel", or "supervisor" mode. In this mode, software can execute all machine instructions and access all storage locations.
- "Unprivileged" mode: a.k.a. "user", "application", or "problem" mode. In this mode, software is restricted to a subset of the instructions and a subset of the storage locations.

3. "A distinct scope within which certain common characteristics are exhibited and common rules are observed."

4. (MISSI) The domain of a MISSI CA is the set of MISSI users whose cetificates are signed by the CA.

5. (Internet) That part of the tree-structured name space of the DNS that is at or below the name that specifies the domain. A domain is a subdomain of another domain if it is contained within that domain. For example, D.C.B.A is a subdomain of C.B.A

6. (OSI) An administrative partition of a complex distributed OSI system.

Domain Keys Identified Mail (DKIM): A protocol, which is being specified by the IETF working group of the same name, to provide data integrity and domain-level (see: DNS, domain name) data origin authentication for Internet mail messages. (Compare: PEM.)

Tutorial: DKIM employs asymmetric cryptography to create a digital signature for an Internet email message's body and selected headers (see RFC 1822), and the signature is then carried in a header of the message. A recipient of the message can verify the signature and, thereby, authenticate the identity of the originating domain and the integrity of the signed content, by using a public key belonging to the domain. The key can be obtained from the DNS.

Domain name: The style of identifier that is defined for subtrees in the Internet DNS -- i.e., a sequence of case-insensitive ASCII labels separated by dots (e.g., "bbn.com") -- and also is used in other types of Internet identifiers, such as host names (e.g., "rosslyn.bbn.com"), mailbox names (e.g., "rshirey@bbn.com") and URLs (e.g., "http:((www.rosslyn.bbn.com(foo"). (See: domain. Compare: DN.)

Tutorial: The name space of the DNS is a tree structure in which each node and leaf holds records describing a resource. Each node has a label. The domain name of a node is the list of labels on the path from the node to the root of the tree. The labels in a domain name are printed or read left to right, from the most specific (lowest, farthest from the root) to the least specific (highest, closest to the root), but the root's label is the null string. (See: country code.)

Domain Name System (DNS): The main Internet operations database, which is distributed over a collection of servers and used by client software for purposes such as

(a) Translating a domain name-style host name into an IP address (e.g., "rosslyn.bbn.com" translates to "192.1.7.10") and

(b) Locating a host that accepts mail for a given mailbox address. (RFC 1034) (See: domain name.)

Tutorial: The DNS has three major components:

- **Domain name space and resource records**: Specifications for the tree-structured domain name space, and data associated with the names.

- **Name servers**: Programs that hold information about a subset of the tree's structure and data holdings, and also hold pointers to other name servers that can provide information from any part of the tree.
- **Resolvers**: Programs that extract information from name servers in response to client requests; typically, system routines directly accessible to user programs.

Extensions to the DNS support:

(a) Key distribution for public keys needed for the DNS and for other protocols,

(b) Data origin authentication service and data integrity service for resource records,

(c) Data origin authentication service for transactions between resolvers and servers, and

(d) Access control of records.

Domain of interpretation (DOI): A DOI for ISAKMP or IKE defines payload formats, exchange types, and conventions for naming security-relevant information such as security policies or cryptographic algorithms and modes.

Derivation: The DOI concept is based on work by the TSIG's CIPSO Working Group.

Dominate: Security level A is said to "dominate" security level B if the (hierarchical) classification level of A is greater (higher) than or equal to that of B, and A's (nonhierarchical) categories include (as a subset) all of B's categories. (See: lattice, lattice model.)

Dongle: A portable, physical, usually electronic device that is required to be attached to a computer to enable a particular software program to run. (See: token.)

Tutorial: A dongle is essentially a physical key used for copy protection of software; that is, the program will not run unless the matching dongle is attached. When the software runs, it periodically queries the dongle and quits if the dongle does not reply with the proper authentication information. Dongles were originally constructed as an EPROM (erasable programmable read-only memory) to be connected to a serial input-output port of a personal computer.

Downgrade: **(**data security) Reduce the security level of data (especially the classification level) without changing the information content of the data. (Compare: downgrade.)

Downgrade attack: A type of man-in-the-middle attack in which the attacker can cause two parties, at the time they negotiate a security association, to agree on a lower level of protection than the highest level that could have been supported by both of them. (Compare: downgrade.)

Draft RFC: A preliminary, temporary version of a document that is intended to become an RFC. (Compare: Internet-Draft.)

Draft Standard: See: secondary definition under "Internet Standard".

DSA: See: Digital Signature Algorithm.

DSS: See: Digital Signature Standard.

Dual control: A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource. (See: no-lone zone, separation of duties, split knowledge.)

Dual signature: (SET) A single digital signature that protects two separate messages by including the hash results for both sets in a single encrypted value.

Deprecated Usage: DOCUMENTS SHOULD NOT use this term except when qualified as "SET (trademark) dual signature" with this definition.

Tutorial: Generated by hashing each message separately, concatenating the two hash results, and then hashing that value and encrypting the result with the signer's private key. Done to reduce the number of encryption operations and to enable verification of data integrity without complete disclosure of the data.

Dual-use certificate: A certificate that is intended for use with both digital signature and data encryption services.

Usage: DOCUMENTS that use this term SHOULD state a definition for it by identifying the intended uses of the certificate, because there are more than just these two uses mentioned in the NIST publication. A v3 X.509 public-key certificate may have a "key Usage" extension, which indicates the purposes for which the public key may be used. (See: certificate profile.)

Duty: An attribute of a role that obligates an entity playing the role to perform one or more tasks, which usually are essential for the functioning of the system. [Sand] (Compare authorization, privilege. See: role, billet.)

E-cash: Electronic cash; money that is in the form of data and can be used as a payment mechanism on the Internet. (See: IOTP.)

Usage: DOCUMENTS that use this term SHOULD state a definition for it because many different types of electronic cash have been devised with a variety of security mechanisms.

EAP: See: Extensible Authentication Protocol.

EAL: See: evaluation assurance level.

Easter egg: "Hidden functionality within an application program, which becomes activated when an undocumented, and often convoluted, set of commands and keystrokes is entered. Easter eggs are typically used to display the credits for the

development team and [are] intended to be non-threatening", but Easter eggs have the potential to contain malicious code.

Deprecated Usage: Since other cultures use different metaphors for this concept, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term.

Eavesdropping: Passive wiretapping done secretly, i.e., without the knowledge of the originator or the intended recipients of the communication.

ECB: See: electronic codebook.

ECDSA: See: Elliptic Curve Digital Signature Algorithm.

Economy of alternatives: The principle that a security mechanism should be designed to minimize the number of alternative ways of achieving a service. (Compare: economy of mechanism.)

Economy of mechanism: The principle that a security mechanism should be designed to be as simple as possible, so that

(a) The mechanism can be correctly implemented and

(b) It can be verified that the operation of the mechanism enforces the system's security policy. (Compare: economy of alternatives, least privilege.)

ECU: See: end cryptographic unit.

EDI: See: electronic data interchange.

EDIFACT: See: secondary definition under "electronic data interchange".

EE: Abbreviation of "end entity" and other terms.

Deprecated Abbreviation: DOCUMENTS SHOULD NOT use this abbreviation; there could be confusion among "end entity", "end-to-end encryption", "escrowed encryption standard", and other terms.

EES: See: Escrowed Encryption Standard.

Effective key length: "A measure of strength of a cryptographic algorithm, regardless of actual key length." (See: work factor.)

Effectiveness: (ITSEC) A property of a TOE representing how well it provides security in the context of its actual or proposed operational use.

El Gamal algorithm: An algorithm for asymmetric cryptography, invented in 1985 by Taher El Gamal, that is based on the difficulty of calculating discrete logarithms and can be used for both encryption and digital signatures.

Electronic codebook (ECB): A block cipher mode in which a plaintext block is used directly as input to the encryption algorithm and the resultant output block is used directly as cipher text. (See: block cipher)

Electronic commerce:

1. Business conducted through paperless exchanges of information, using electronic data interchange, electronic funds transfer (EFT), electronic mail, computer bulletin boards, facsimile, and other paperless technologies.
2. (SET) "The exchange of goods and services for payment between the cardholder and merchant when some or all of the transaction is performed via electronic communication."

Electronic data interchange (EDI): Computer-to-computer exchange, between trading partners, of business data in standardized document formats.

Tutorial: EDI formats have been standardized primarily by ANSI X12 and by EDIFACT (EDI for Administration, Commerce, and Transportation), which is an international, UN-sponsored standard primarily used in Europe and Asia. X12 and EDIFACT are aligning to create a single, global EDI standard.

Electronic Key Management System (EKMS): "Interoperable collection of systems developed by ... the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic keying material and the management of other types of COMSEC material."

Electronic signature: Synonym for "digital signature" or "digitized signature".

Deprecated Term: DOCUMENTS SHOULD NOT use this term; there is no current consensus on its definition. Instead, use "digital signature", if that is what was intended

Electronic wallet: A secure container to hold, in digitized form, some sensitive data objects that belong to the owner, such as electronic money, authentication material, and various types of personal information.

Deprecated Term: DOCUMENTS SHOULD NOT use this term. There is no current consensus on its definition; and some uses and definitions may be proprietary. Meanings range from virtual wallets implemented by data structures to physical wallets implemented by cryptographic tokens.

Elliptic curve cryptography (ECC): A type of asymmetric cryptography based on mathematics of groups that are defined by the points on a curve, where the curve is defined by a quadratic equation in a finite field.

Tutorial: ECC is based on mathematics different than that originally used to define the Diffie-Hellman-Merkle algorithm and the DSA, but ECC can be used to define an algorithm for key agreement that is an analog of Diffie-Hellman-Merkle and an algorithm for digital signature that is an analog of DSA. The mathematical problem upon which ECC is based is believed to be more difficult than the problem upon which Diffie-Hellman-Merkle is based and, therefore, that keys for ECC can be shorter for a comparable level of security. (See: ECDSA.)

Elliptic Curve Digital Signature Algorithm (ECDSA): A standard that is the analog, in elliptic curve cryptography, of the Digital Signature Algorithm.

Emanation: A signal (e.g., electromagnetic or acoustic) that is emitted by a system (e.g., through radiation or conductance) as a consequence (i.e., byproduct) of the system's operation, and that may contain information. (See: emanations security.)

Emanations analysis: **(**threat action) See: secondary definition under "interception".

Emanations security (EMSEC): Physical security measures to protect against data compromise that could occur because of emanations that might be received and read by an unauthorized party. (See: emanation, TEMPEST.)

Usage: Refers either to preventing or limiting emanations from a system and to preventing or limiting the ability of unauthorized parties to receive the emissions.

Embedded cryptography: "Cryptography engineered into an equipment or system whose basic function is not cryptographic."

Emergency plan: Synonym for "contingency plan".

Deprecated Term: DOCUMENTS SHOULD NOT use this term. Instead, for neutrality and consistency of language, use "contingency plan".

Emergency response: An urgent response to a fire, flood, civil commotion, natural disaster, bomb threat, or other serious situation, with the intent of protecting lives, limiting damage to property, and minimizing disruption of system operations.

EMSEC: See: emanations security.

EMV: Abbreviation of "Europay, MasterCard, Visa". Refers to a specification for smart cards that are used as payment cards, and for related terminals and applications.

Encapsulating Security Payload (ESP): An Internet protocol designed to provide data confidentiality service and other security services for IP datagrams. (See: IPsec. Compare: AH.)

Tutorial: ESP may be used alone, or in combination with AH, or in a nested fashion with tunneling. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a host and a gateway. The ESP header is encapsulated by the IP header, and the ESP header encapsulates either the upper-layer protocol header (transport mode) or an IP header (tunnel mode). ESP can provide data confidentiality service, data origin authentication service, connectionless data integrity service, an anti-replay service, and limited traffic-flow confidentiality. The set of services depends on the placement of the implementation and on options selected when the security association is established.

Encipher: Synonym for "encrypt".

Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "encrypt". However, see Usage note under "encryption".

Encipherment: Synonym for "encryption".

Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "encryption". However, see Usage note under "encryption".

Enclave:

1. A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (Compare: domain.)
2. (U.S. Government) "Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security."

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term with definition 2 because the definition applies to what is usually called a "security domain". That is, a security domain is a set of one or more security enclaves.

Encode:

1. Use a system of symbols to represent information, which might originally have some other representation. Example: Morse code. (See: ASCII, BER.) (See: code, decode.)
2. Synonym for "encrypt". Deprecated Definition: DOCUMENTs SHOULD NOT use this term as a synonym for "encrypt"; encoding is not always meant to conceal meaning.

Encrypt: Cryptographically transform data to produce cipher text. (See: encryption. Compare: seal.)

Encryption:

1. Cryptographic transformation of data (called "plain text") into a different form (called "cipher text") that conceals the data's original meaning and prevents the original form from being used. The corresponding reverse process is "decryption", a transformation that restores encrypted data to its original form. (See: cryptography.)
2. "The cryptographic transformation of data to produce cipher-text."

   Usage: For this concept, DOCUMENTS SHOULD use the verb "to encrypt" (and related variations: encryption, decrypt, and decryption). However, because of cultural biases involving human burial, some international documents (particularly ISO and CCITT standards) avoid "to encrypt" and instead use the verb "to encipher" (and related variations: encipherment, decipher, decipherment).

Tutorial: Usually, the plaintext input to an encryption operation is clear text. But in some cases, the plain text may be cipher text that was output from another encryption operation. See: super encryption.)

Encryption and decryption involve a mathematical algorithm for transforming data. Besides the data to be transformed, the algorithm has one or more inputs that are control parameters: (a) a key that varies the transformation and, in some cases, (b) an IV that establishes the starting state of the algorithm.

Encryption certificate: A public-key certificate that contains a public key that is intended to be used for encrypting data, rather than for verifying digital signatures or performing other cryptographic functions. Tutorial: A v3 X.509 public-key certificate may have a "keyUsage" extension that indicates the purpose for which the certified public key is intended. (See: certificate profile.)

End cryptographic unit (ECU):

1. Final destination device into which a key is loaded for operational use.
2. A device that (a) performs cryptographic functions, (b) typically is part of a larger system for which the device provides security services, and (c), from the viewpoint of a supporting security infrastructure such as a key management system, is the lowest level of identifiable component with which a management transaction can be conducted

End entity:

1. A system entity that is the subject of a public-key certificate and that is using, or is permitted and able to use, the matching private key only for purposes other than signing a digital certificate; i.e., an entity that is not a CA.
2. "A certificate subject [that] uses its public key for purposes other than signing certificates."

   Deprecated Definition: DOCUMENTS SHOULD NOT use definition 2, which is misleading and incomplete. First, that definition should have said "private key" rather than "public key" because certificates are not usefully signed with a public key. Second, the X.509 definition is ambiguous regarding whether an end entity may or may not use the private key to sign a certificate, i.e., whether the subject may be a CA. The intent of X.509's authors was that an end entity certificate is not valid for use in verifying a signature on an X.509 certificate or X.509 CRL.

   Usage: Despite the problems in the X.509 definition, the term itself is useful in describing applications of asymmetric cryptography. The way the term is used in X.509 implies that it was meant to be defined, as we have done here, relative to roles that an entity (which is associated with an OSI end system) is playing or is permitted to play in applications of asymmetric cryptography other than the PKI that supports applications.

Tutorial: Whether a subject can play both CA and non-CA roles, with either the same or different certificates, is a matter of policy. (See: CPS.) A v3 X.509 public-key certificate may have a "basic Constraints" extension containing a "cA" value that specifically "indicates whether or not the public key may be used to verify certificate signatures". (See: certificate profile.)

End system: (OSI-RM) A computer that implements all seven layers of the OSI-RM and may attach to a subnetwork. Usage: In the IPS context, an end system is called a "host".

End-to-end encryption: Continuous protection of data that flows between two points in a network, effected by encrypting data when it leaves its source, keeping it encrypted while it passes through any intermediate computers (such as routers), and decrypting it only when it arrives at the intended final destination. (See: wiretapping. Compare: link encryption.) Examples: A few are BLACKER, CANEWARE, IPLI, IPsec, PLI, SDNS, SILS, SSH, SSL, TLS.

Tutorial: When two points are separated by multiple communication links that are connected by one or more intermediate relays, end-to-end encryption enables the source and destination systems to protect their communications without depending on the intermediate systems to provide the protection.

End user:

1. (information system) A system entity, usually a human individual, that makes use of system resources, primarily for application purposes as opposed to system management purposes.
2. (PKI) Synonym for "end entity".

Deprecated Definition: DOCUMENTS SHOULD NOT use "end user" as a synonym for "end entity", because that would mix concepts in a potentially misleading way.

Endorsed-for-unclassified cryptographic item (EUCI): (U.S. Government) "Unclassified cryptographic equipment that embodies a U.S. Government classified cryptographic logic and is endorsed by NSA for the protection of national security information."

Entity: See: system entity.

Entrapment: "The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit."

Entropy:

1. An information-theoretic measure (usually stated as a number of bits) of the amount of uncertainty that an attacker faces to determine the value of a secret. (See: strength.) Example: If a password is said to contain at least 20 bits of

entropy that means that it must be as hard to find the password as to guess a 20-bit random number.

2. An information-theoretic measure (usually stated as a number of bits) of the amount of information in a message; i.e., the minimum number of bits needed to encode all possible meanings of that message.

Ephemeral: (adjective) Refers to a cryptographic key or other cryptographic parameter or data object that is short-lived, temporary, or used one time.

Erase:

1. Delete stored data. (See: sanitize)

2. (U.S. Government) Delete magnetically stored data in such a way that the data cannot be recovered by ordinary means, but might be recoverable by laboratory methods.

Error detection code: A checksum designed to detect, but not correct, accidental (i.e., unintentional) changes in data.

Escrowed Encryption Standard (EES): A U.S. Government standard that specifies how to use a symmetric encryption algorithm (SKIPJACK) and create a Law Enforcement Access Field (LEAF) for implementing part of a key escrow system that enables decryption of telecommunications when interception is lawfully authorized.

Tutorial: Both SKIPJACK and the LEAF are intended for use in equipment used to encrypt and decrypt sensitive, unclassified, telecommunications data.

ESP: See: Encapsulating Security Payload.

Estelle: A language (ISO 9074-1989) for formal specification of computer network protocols.

ETSI: See: European Telecommunication Standards Institute.

EUCI: See: endorsed-for-unclassified cryptographic item.

European Telecommunication Standards Institute (ETSI): An independent, non-profit organization, based in France that is officially recognized by the European Commission and responsible for standardization of information and communication technologies within Europe.

Tutorial: ETSI maintains the standards for a number of security algorithms, including encryption algorithms for mobile telephone systems in Europe.

Evaluated system: A system that has been evaluated against security criteria (for example, against the TCSEC or against a profile based on the Common Criteria).

Evaluation: Assessment of an information system against defined security criteria (for example, against the TCSEC or against a profile based on the Common Criteria). (Compare: certification.)

Evaluation assurance level (EAL): A predefined package of assurance components that represents a point on the Common Criteria's scale for rating confidence in the security of information technology products and systems.

Tutorial: The Common Criteria defines a scale of seven, hierarchically ordered EALs for rating a TOE. From highest to lowest, they are as follows:

- EAL7. Formally verified design and tested.
- EAL6. Semiformally verified design and tested.
- EAL5. Semiformally designed and tested.
- EAL4. Methodically designed, tested, and reviewed.
- EAL3. Methodically tested and checked.
- EAL2. Structurally tested.
- EAL1. Functionally tested.

An EAL is a consistent, baseline set of requirements. The increase in assurance from EAL to EAL is accomplished by substituting higher assurance components (i.e., criteria of increasing rigor, scope, or depth) from seven assurance classes:

(a) Configuration management,

(b) Delivery and operation,

(c) Development,

(d) Guidance documents,

(e) Lifecycle support,

(f) Tests, and

(g) Vulnerability assessment.

The EALs were developed with the goal of preserving concepts of assurance that were adopted from earlier criteria, so that results of previous evaluations would remain relevant. For example, EALs levels 2-7 are generally equivalent to the assurance portions of the TCSEC C2-A1 scale. However, this equivalency should be used with caution. The levels do not derive assurance in the same manner, and exact mappings do not exist.

Expire: (credential) Cease to be valid (i.e., change from being valid to being invalid) because its assigned lifetime has been exceeded. (See: certificate expiration.)

Exposure: A type of threat action whereby sensitive data is directly released to an unauthorized entity. (See: unauthorized disclosure.)

Usage: This type of threat action includes the following subtypes:

- "Deliberate Exposure": Intentional release of sensitive data to an unauthorized entity.
- "Scavenging": Searching through data residue in a system to gain unauthorized knowledge of sensitive data.
- "Human error": (exposure(Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data. (Compare: corruption, incapacitation.)
- "Hardware or software error": (exposure(System failure that unintentionally results in an entity gaining unauthorized knowledge of sensitive data. (Compare: corruption, incapacitation.)

Extended Security Option: See: secondary definition under "IPSO".

Extensible Authentication Protocol (EAP): An extension framework for PPP that supports multiple, optional authentication mechanisms, including clear-text passwords, challenge-response, and arbitrary dialog sequences. (Compare: GSS-API, SASL.)

Tutorial: EAP typically runs directly over IPS data link protocols or OSI-RM Layer 2 protocols, i.e., without requiring IP. Originally, EAP was developed for use in PPP, by a host or router that connects to a network server via switched circuits or dial-up lines. Today, EAP's domain of applicability includes other areas of network access control; it is used in wired and wireless LANs with IEEE 802.1X, and in IPsec with IKEv2. EAP is conceptually related to other authentication mechanism frameworks, such as SASL and GSS-API.

Extensible Markup Language (XML): A version of Standard Generalized Markup Language (ISO 8879) that separately represents a document's content and its structure. XML was designed by W3C for use on the World Wide Web.

Extension: (protocol) A data item or a mechanism that is defined in a protocol to extend the protocol's basic or original functionality.

Tutorial: Many protocols have extension mechanisms, and the use of these extension is usually optional. IP and X.509 are two examples of protocols that have optional extensions. In IP version 4, extensions are called "options", and some of the options have security purposes (see: IPSO). In X.509, certificate and CRL formats can be extended to provide methods for associating additional attributes with subjects and public keys and for managing a certification hierarchy:

- A "certificate extension": X.509 defines standard extensions that may be included in v3 certificates to provide additional key and security policy information, subject and issuer attributes, and certification path constraints.

- A "CRL extension": X.509 defines extensions that may be included in v2 CRLs to provide additional issuer key and name information, revocation reasons and constraints, and information about distribution points and delta CRLs.
- A "private extension": Additional extensions, each named by an OID, can be locally defined as needed by applications or communities. (See: Authority Information Access extension, SET private extensions.)

External controls: (COMPUSEC) Refers to administrative security, personnel security, and physical security. (Compare: internal controls.)

Extranet: A computer network that an organization uses for application data traffic between the organization and its business partners.

Tutorial: An extranet can be implemented securely, either on the Internet or using Internet technology, by constructing the extranet as a VPN.

Extraction resistance: Ability of cryptographic equipment to resist efforts to extract keying material directly from the equipment (as opposed to gaining knowledge of keying material by cryptanalysis).

Extrusion detection: Monitoring for unauthorized transfers of sensitive information and other communications that originate inside a system's security perimeter and are directed toward the outside; i.e., roughly the opposite of "intrusion detection".

Fail-safe

1. Synonym for "fail-secure".
2. A mode of termination of system functions that prevents damage to specified system resources and system entities when a failure occurs or is detected in the system (but the failure still might cause a security compromise).

Tutorial: Definitions 1 and 2 are opposing design alternatives. Therefore, DOCUMENTS SHOULD NOT use this term without providing a definition for it.

Fail-secure: A mode of termination of system functions that prevents loss of secure state when a failure occurs or is detected in the system (but the failure still might cause damage to some system resource or system entity) (Compare: fail-safe.)

Fail-soft: Selective termination of affected, non-essential system functions when a failure occurs or is detected in the system. (See: failure control.)

Failure control: A methodology used to provide fail-safe, fail-secure or fail-soft termination and recovery of system functions.

Fairness: A property of an access protocol for a system resource whereby the resource is made equitably or impartially available to all eligible users.

Tutorial: Fairness can be used to defend against some types of denial-of-service attacks on a system connected to a network.

Falsification: A type of threat action whereby false data deceives an authorized entity. (See: active wiretapping, deception.)

Usage: This type of threat action includes the following subtypes:

- **"Substitution**": Altering or replacing valid data with false data that serves to deceive an authorized entity.
- **"Insertion":** Introducing false data that serves to deceive an authorized entity.

Fault tree: A branching, hierarchical data structure that is used to represent events and to determine the various combinations of component failures and human acts that could result in a specified undesirable system event. (See: attack tree, flaw hypothesis methodology.)

Tutorial: "Fault-tree analysis" is a technique in which an undesired state of a system is specified and the system is studied in the context of its environment and operation to find all credible ways in which the event could occur. The specified fault event is represented as the root of the tree. The remainder of the tree represents AND or OR combinations of subevents, and sequential combinations of subevents, that could cause the root event to occur. The main purpose of a fault-tree analysis is to calculate the probability of the root event, using statistics or other analytical methods and incorporating actual or predicted quantitative reliability and maintainability data. When the root event is a security violation, and some of the subevents are deliberate acts intended to achieve the root event, then the fault-tree is an attack tree.

FEAL: A family of symmetric block ciphers that was developed in Japan; uses a 64-bit block, keys of either 64 or 128 bits, and a variable number of rounds; and has been successfully attacked by cryptanalysts.

Federal Information Processing Standards (FIPS): The Federal Information Processing Standards Publication (FIPS PUB) series issued by NIST under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987 (Public Law 100-235) as technical guidelines for U.S. Government procurements of information processing system equipment and services.

Federal Public-key Infrastructure (FPKI): A PKI being planned to establish facilities, specifications, and policies needed by the U.S. Government to use public-key certificates in systems involving unclassified but sensitive applications and interactions between Federal agencies as well as with entities of state and local governments, the business community, and the public.

Federal Standard 1027: An U.S. Government document defining emanation, anti-tamper, security fault analysis, and manual key management criteria for DES encryption devices, primary for OSI-RM Layer 2. Was renamed "FIPS PUB 140" when responsibility for protecting unclassified, sensitive information was

transferred from NSA to NIST, and has since been superseded by newer versions of that standard.

File Transfer Protocol (FTP): A TCP-based, Application-Layer, Internet Standard protocol (RFC 959) for moving data files from one computer to another.

Fill device: (COMSEC) A device used to transfer or store keying material in electronic form or to insert keying material into cryptographic equipment.

Filter:

1. (noun) Synonym for "guard". (Compare: content filter, filtering router.)
2. (verb) To process a flow of data and selectively block passage or permit passage of individual data items according to a security policy.

Filtering router: An internetwork router that selectively prevents the passage of data packets according to a security policy.

Tutorial: A router usually has two or more physical connections to networks or other systems; and when the router receives a packet on one of those connections, it forwards the packet on a second connection. A filtering router does the same; but it first decides, according to some security policy, whether the packet should be forwarded at all. The policy is implemented by rules (packet filters) loaded into the router. The rules mostly involve values of data packet control fields (especially IP source and destination addresses and TCP port numbers). A filtering router may be used alone as a simple firewall or be used as a Component of a more complex firewall.

Financial institution: An establishment responsible for facilitating customer-initiated transactions or transmission of funds for the extension of credit or the custody, loan, exchange, or issuance of money."

Fingerprint:

1. A pattern of curves formed by the ridges on a fingertip. (See: biometric authentication. Compare: thumbprint.)
2. (PGP) A hash result ("key fingerprint") used to authenticate a public key or other data.

Deprecated Definition: DOCUMENTS SHOULD NOT use this term with definition 2, and SHOULD NOT use this term as a synonym for "hash result" of *any* kind. Either use would mix concepts in a potentially misleading way.

FIPS: See: Federal Information Processing Standards.

FIPS PUB 140: The U.S. Government standard for security requirements to be met by a cryptographic module when the module is used to protect unclassified information in computer and communication systems. (See: Common Criteria, FIPS, Federal Standard 1027.)

Tutorial: The standard specifies four increasing levels (from "Level 1" to "Level 4") of requirements to cover a wide range of potential applications and environments. The requirements address basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference and electromagnetic compatibility (EMI(EMC), and self-testing. NIST and the Canadian Communication Security Establishment jointly certify modules.

FIREFLY: (U.S. Government) "Key management protocol based on public-key cryptography."

Firewall:

1. An internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). (See: guard, security gateway.)

2. A device or system that controls the flow of traffic between networks using differing security postures

Tutorial: A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies policy rules to control traffic that flows in and out of the protected network.

A firewall is not always a single computer. For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN (see: buffer zone) between the two routers. The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher-layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers. The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep unauthorized traffic (i.e.,intruders) out, but usually also needs to let authorized traffic pass both in and out.

Firmware: Computer programs and data stored in hardware -- typically in read-only memory (ROM) or programmable read-only memory (PROM) --such that the programs and data cannot be dynamically written or modified during execution of the programs. (See: hardware, software.)

FIRST: See: Forum of Incident Response and Security Teams.

Flaw:

1. An error in the design, implementation, or operation of an information system. A flaw may result in a vulnerability. (Compare: vulnerability.)
2. "An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed." (Compare: vulnerability. See: brain-damaged.)

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term with definition 2; not every flaw is a vulnerability.

Flaw hypothesis methodology: An evaluation or attack technique in which specifications and documentation for a system are analyzed to hypothesize flaws in the system. The list of hypothetical flaws is prioritized on the basis of the estimated probability that a flaw exists and, assuming it does, on the ease of exploiting it and the extent of control or compromise it would provide. The prioritized list is used to direct a penetration test or attack against the system.

Flooding:

1. An attack that attempts to cause a failure in a system by providing more input than the system can process properly.
2. The process of delivering data or control messages to every node of a network.

Flow analysis: An analysis performed on a nonprocedural, formal, system specification that locates potential flows of information between system variables. By assigning security levels to the variables, the analysis can find some types of covert channels.

Flow control:

1. (data security) A procedure or technique to ensure that information transfers within a system are not made from one security level to another security level, and especially not from a higher level to a lower level. (See: covert channel, confinement property, information flow policy, simple security property.)
2. (data security) "A concept requiring that information transfers within a system be controlled so that information in certain types of objects cannot, via any channel within the system, flow to certain other types of objects."

For Official Use Only (FOUO): A U.S. Government designation for information that has not been given a security classification pursuant to the criteria of an Executive Order dealing with national security, but which may be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one of the exemptions stated in the Freedom of Information Act (Section 552 of title 5, United States Code). (See: security label, security marking.)

Formal: Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Formal access approval: (U.S. Government) Documented approval by a data owner to allow access to a particular category of information in a system. (See: category.)

Formal Development Methodology: See: Ina Jo.

Formal model: A security model that is formal. Example: Bell-LaPadula model. (See: formal, security model.)

Formal proof: "A complete and convincing mathematical argument, presenting the full logical justification for each step in the proof, for the truth of a theorem or set of theorems."

Formal specification: A precise description of the (intended) behavior of a system, usually written in a mathematical language, sometimes for the purpose of supporting formal verification through a correctness proof.

Tutorial: A formal specification can be written at any level of detail but is usually a top-level specification.

Formal top-level specification: "A top-level specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven."

Formulary: A technique for enabling a decision to grant or deny access to be made dynamically at the time the access is attempted, rather than earlier when an access control list or ticket is created.

FORTEZZA (trademark): A registered trademark of NSA, used for a family of interoperable security products that implement a NIST/NSA-approved suite of cryptographic algorithms for digital signature, hash, encryption, and key exchange. The products include a PC card (which contains a CAPSTONE chip), and compatible serial port modems, server boards, and software implementations.

Forum of Incident Response and Security Teams (FIRST): An international consortium of CSIRTs (e.g., CIAC) that work together to handle computer security incidents and promote preventive activities. (See: CSIRT, security incident.) Tutorial: FIRST was founded in 1990 and, as of July 2004, had more than 100 members spanning the globe. Its mission includes:

- Provide members with technical information, tools, methods, assistance, and guidance.
- Coordinate proactive liaison activities and analytical support.
- Encourage development of quality products and services.
- Improve national and international information security for governments, private industry, academia, and the individual.

Forward secrecy: See: perfect forward secrecy.

FOUO: See: For Official Use Only.

FPKI: See: Federal Public-Key Infrastructure.

Fraggle attack: (slang) A synonym for "smurf attack". Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTs SHOULD NOT use this term. Derivation: The Fraggles are a fictional race of small humanoids (represented as hand puppets in a children's television series, "Fraggle Rock") that live underground.

Frequency hopping: Repeated switching of frequencies during radio transmission according to a specified algorithm. (See: spread Spectrum.)

Tutorial: Frequency hopping is a TRANSEC technique to minimize the potential for unauthorized interception or jamming.

Fresh: Recently generated; not replayed from some earlier interaction of the protocol.

FTP: See: File Transfer Protocol.

Gateway: An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks. (See: bridge, firewall, guard, internetwork, proxy server, router, and subnetwork.)

Tutorial: The networks may differ in any of several aspects, including protocols and security mechanisms. When two computer networks differ in the protocol by which they offer service to hosts, a gateway may translate one protocol into the other or otherwise facilitate interoperation of hosts (see: Internet Protocol). In theory, gateways between computer networks are conceivable at any OSI-RM layer. In practice, they usually operate at OSI-RM Layer 2 (see: bridge), 3 (see: router), or 7 (see: proxy server).

GCA: See: geopolitical certificate authority.

GDOI: See: Group Domain of Interpretation.

GeldKarte: A smartcard-based, electronic money system that is maintained by the German banking industry, incorporates cryptography, and can be used to make payments via the Internet.

GeneralizedTime: The ASN.1 data type "GeneralizedTime" (ISO 8601) contains a calendar date (YYYYMMDD) and a time of day, which is either (a) the local time, (b) the Coordinated Universal Time, or (c) both the local time and an offset that enables Coordinated Universal Time to be calculated. (See: Coordinated Universal Time. Compare: UTCTime.)

Generic Security Service Application Program Interface (GSS-API): An Internet Standard protocol [R2743] that specifies calling conventions by which an application (typically another communication protocol) can obtain authentication, integrity, and confidentiality security services independently of the underlying security mechanisms and technologies, thus enabling the Application source code to be ported to different environments. (Compare: EAP, SASL.)

Tutorial: "A GSS-API caller accepts tokens provided to it by its local GSS-API implementation and transfers the tokens to a peer on a remote system; that peer passes the received tokens to its local GSS-API implementation for processing. The security services available through GSS-API in this fashion are implementable (and have been implemented) over a range of underlying mechanisms based on [symmetric] and [asymmetric cryptography]."

Geopolitical certificate authority (GCA): **(**SET) In a SET certification hierarchy, an optional level that is certified by a BCA and that may certify cardholder CAs, merchant CAs, and payment gateway CAs. Using GCAs enables a brand to distribute responsibility for managing certificates to geographic or political regions, so that brand policies can vary between regions as needed.

GIG: See: Global Information Grid.

Global Information Grid (GIG): **(**U.S. DoD) The GIG is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel."

Good engineering practice(s): A term used to specify or characterize design, implementation, installation, or operating practices for an information system, when a more explicit specification is not possible. Generally understood to refer to the state of the engineering art for commercial systems that have problems and solutions equivalent to the system in question.

Granularity:

1. (access control) Relative fineness to which an access control mechanism can be adjusted.
2. (data security) "The size of the smallest protectable unit of information" in a trusted system.

Green Book: **(**slang) Synonym for "Defense Password Management Guideline"

Deprecated Term: Except as an explanatory appositive, DOCUMENTS SHOULD NOT use this term, regardless of the associated definition. Instead, use the full proper name of the document or, in subsequent references, a conventional abbreviation. (See: Rainbow Series.)

Deprecated Usage: To improve international comprehensibility of Internet Standards and the Internet Standards Process, DOCUMENTS SHOULD NOT use "cute" synonyms. No matter how clearly understood or popular a nickname may be in one community, it is likely to cause confusion or offense in others. For example, several other information system standards also are called "the Green Book".

Group Domain of Interpretation (GDOI): An ISAKMP/IKE domain of interpretation for group key management; i.e., a phase 2 protocol in ISAKMP. (See: secure multicast.)

Tutorial: In this group key management model that extends the ISAKMP standard, the protocol is run between a group member and a "group controller (key server", which establishes security associations among authorized group members. The GDOI protocol is itself protected by an ISAKMP phase 1 association. For example, multicast applications may use ESP to protect their data traffic. GDOI carries the needed security association parameters for ESP. In this way, GDOI supports multicast ESP with group authentication of ESP packets using a shared, group key.

Group identity: See: secondary definition under "identity".

Group security association: "A bundling of [security associations] (SAs) that together define how a group communicates securely. The [group SA] may include a registration protocol SA, a rekey protocol SA, and one or more data security protocol SAs."

GSS-API: See: Generic Security Service Application Program Interface.

Guard: A computer system that

(a) Acts as gateway between two information systems operating under different security policies and

(b) Is trusted to mediate information data transfers between the two. (See: controlled interface, cross-domain solution, domain, filter. Compare: firewall.)

Usage: Frequently understood to mean that one system is operating at a higher security level than the other, and that the gateway's purpose is to prevent unauthorized disclosure of data from the higher system to the lower. However, the purpose might also be to protect the data integrity, availability, or general system integrity of one system from threats posed by connecting to the other system. The mediation may be entirely automated or may involve "reliable human review".

Guest login: See: anonymous login.

GULS: Generic Upper Layer Security service element (ISO 11586), a five-part standard for the exchange of security information and security-transformation functions that protect confidentiality and integrity of application data.

Gypsy verification environment: A methodology, language, and integrated set of software tools developed at the University of Texas for specifying, coding, and verifying software to produce correct and reliable programs.

H field: See: Deprecated Usage under "Handling Restrictions field".

Hack:

1a. (verb) To work on something, especially to program a computer. (See: hacker.)

1b. (verb) To do some kind of mischief, especially to play a prank on, or penetrate, a system. (See: hacker, cracker.)

2. (noun) An item of completed work, or a solution for a problem, that is non-generalizable, i.e., is very specific to the application area or problem being solved.

Tutorial: Often, the application area or problem involves computer programming or other use of a computer. Characterizing something as a hack can be a compliment, such as when the solution is minimal and elegant; or it can be derogatory, such as when the solution fixes the problem but leaves the system in an unmaintainable state.

Hacker:

1. Someone with a strong interest in computers, who enjoys learning about them, programming them, and experimenting and otherwise working with them. (See: hack. Compare: adversary, cracker, intruder.)

Usage: This first definition is the original meaning of the term (circa 1960); it then had a neutral or positive connotation of "someone who figures things out and makes something cool happen".

2. "An individual who spends an inordinate amount of time working on computer systems for other than professional purposes."

3. Synonym for "cracker".

Handle:

1. (verb) Perform processing operations on data, such as receive and transmit, collect and disseminate, create and delete, store and retrieve, read and write, and compare. (See: access.)

2. (noun) An online pseudonym, particularly one used by a cracker; derived from citizens' band radio culture.

Handling restriction: A type of access control other than (a) the rule-based protections of mandatory access control and (b) the identity-based protections of discretionary access control; usually involves administrative security.

Handling Restrictions field: A 16-bit field that specifies a control and release marking in the security option (option type 130) of IP's datagram header format. The valid field values are alphanumeric digraphs assigned by the U.S. Government, as specified in RFC 791.

Handshake: Protocol dialogue between two systems for identifying and authenticating themselves to each other, or for synchronizing their operations with each other.

Handshake Protocol: The TLS Handshake Protocol consists of three parts (i.e., sub-protocols) that enable peer entities to agree upon security parameters for the record layer, authenticate themselves to each other, instantiate negotiated security parameters, and report error conditions to each other.

Harden: To protect a system by configuring it to operate in a way that eliminates or mitigates known vulnerabilities.

Hardware: The material physical components of an information system.

Hardware error: See: secondary definitions under "corruption", "exposure", and "incapacitation".

Hardware token: See: token.

Hash code: Synonym for "hash result" or "hash function".

Hash function:

1. A function H that maps an arbitrary, variable-length bit string, s, into a fixed-length string, h = H(s) (called the "hash result"). For most computing applications, it is desirable that given a string s with H(s) = h, any change to s that creates a different string s' will result in an unpredictable hash result H(s') that is, with high probability, not equal to H(s).

2. "A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A 'good' hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range."

   Tutorial: A hash function operates on variable-length input (e.g., a message or a file) and outputs a fixed-length output, which typically is much shorter than most input values. If the algorithm is "good" as described in the "O" definition, then the hash function may be a candidate for use in a security mechanism to detect accidental changes in data, but not necessarily for a mechanism to detect changes made by active wiretapping. (See: Tutorial under "checksum".) Security mechanisms require a "cryptographic hash function" (e.g., MD2, MD4, MD5, SHA-

1, Snefru), i.e., a good hash function that also has the one-way property and one of the two collision-free properties:

- "One-way property": Given H and a hash result h = H(s), it is hard (i.e., computationally infeasible, "impossible") to find s. (Of course, given H and an input s, it must be relatively easy to compute the hash result H(s).)
- "Weakly collision-free property": Given H and an input s, it is hard (i.e., computationally infeasible, "impossible") to find a different input, s', such that H(s) = H(s').
- "Strongly collision-free property": Given H, it is hard to find any pair of inputs s and s' such that H(s) = H(s').

If H produces a hash result N bits long, then to find an s' where H(s') = H(s) for a specific given s, the amount of computation required is O(2**n); i.e., it is necessary to try on the order of 2 to the power n values of s' before finding a collision. However, to simply find any pair of values s and s' that collide, the amount of computation required is only O(2**(n(2)); i.e., after computing H(s) for 2 to the power n(2 randomly chosen values of s, the probability is greater than 1(2 that two of those values have the same hash result. (See: birthday attack.)

Hash result:

1. The output of a hash function. (See: hash code, hash value. Compare: hash value.)
2. "The output produced by a hash function upon processing a message" (where "message" is broadly defined as "a digital representation of data").

   Usage: DOCUMENTS SHOULD avoid the unusual usage of "message" that is seen in the "O" definition.

Hash value: Synonym for "hash result".

HDM: See: Hierarchical Development Methodology.

Hierarchical Development Methodology (HDM): A methodology, language, and integrated set of software tools developed at SRI International for specifying, coding, and verifying software to produce correct and reliable programs.

Hierarchical PKI: A PKI architecture based on a certification hierarchy. (Compare: mesh PKI, trust-file PKI.)

Hierarchy management: The process of generating configuration data and issuing public-key certificates to build and operate a certification hierarchy. (See: certificate management.)

Hierarchy of trust: Synonym for "certification hierarchy".

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it mixes concepts in a potentially misleading way. (See: certification hierarchy, trust, web of trust.)

High-assurance guard: "An oxymoron," said Lt. Gen. William H. Campbell, former U.S. Army chief information officer, speaking at an Armed Forces Communications and Electronics Association conference.

Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term mixes concepts and could easily be misunderstood.

Hijack attack: A form of active wiretapping in which the attacker seizes control of a previously established communication association. (See: man-in-the-middle attack, pagejacking, piggyback attack.)

HIPAA: Health Information Portability and Accountability Act of 1996, a U.S. law (Public Law 104-191) that is intended to protect the privacy of patients' medical records and other health information in all forms, and mandates security for that information, including for its electronic storage and transmission.

HMAC: A keyed hash that can be based on any iterated cryptographic hash (e.g., MD5 or SHA-1), so that the cryptographic strength of HMAC depends on the properties of the selected cryptographic hash.

Derivation: Hash-based MAC. (Compare: CMAC.)

Tutorial: Assume that H is a generic cryptographic hash in which a function is iterated on data blocks of length B bytes. L is the length of hash result of H. K is a secret key of length L <= K <= B. The values IPAD and OPAD are fixed strings used as inner and outer padding and defined as follows: IPAD = the byte 0x36 repeated B times, and OPAD = the byte 0x5C repeated B times. HMAC is computed by H(K XOR OPAD, H(K XOR IPAD, inputdata)). HMAC has the following goals:

- To use available cryptographic hash functions without modification, particularly functions that perform well in software and for which software is freely and widely available.
- To preserve the original performance of the selected hash without significant degradation.
- To use and handle keys in a simple way.
- To have a well-understood cryptographic analysis of the strength of the mechanism based on reasonable assumptions about the underlying hash function.
- To enable easy replacement of the hash function in case a faster or stronger hash is found or required.

Honey pot: A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. (See: entrapment.)

Usage: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term without providing a definition for it. (See: Deprecated Usage under "Green Book".)

Host:

1. (general) A computer that is attached to a communication subnetwork or internetwork and can use services provided by the network to exchange data with other attached systems. (See: end system. Compare: server.)
2. (IPS) A networked computer that does not forward IP packets that are not addressed to the computer itself.

   Derivation: As viewed by its users, a host "entertains" them, providing Application-Layer services or access to other computers attached to the network. However, even though some traditional peripheral service devices, such as printers, can now be independently connected to networks, they are not usually called hosts.

HTML: See: Hypertext Markup Language.

HTTP: See: Hypertext Transfer Protocol.

Https: When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL. (Compare: S-HTTP.)

Human error: (threat action) See: secondary definitions under "corruption","exposure", and "incapacitation".

Hybrid encryption: An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption. Examples: digital envelope, MSP, PEM, PGP. (Compare: super-encryption.)

Tutorial: Asymmetric algorithms require more computation than equivalently strong symmetric ones. Thus, asymmetric encryption is not normally used for data confidentiality except to distribute a symmetric key in a hybrid encryption scheme, where the symmetric key is usually very short (in terms of bits) compared to the data file it protects. (See: bulk key.)

Hyperlink: In hypertext or hypermedia, an information object (such as a word, a phrase, or an image, which usually is highlighted by color or underscoring) that points (i.e., indicates how to connect) to related information that is located elsewhere and can be retrieved by activating the link (e.g., by selecting the object with a mouse pointer and then clicking).

Hypermedia: A generalization of hypertext; any media that contain hyperlinks that point to material in the same or another data object.

Hypertext: A computer document, or part of a document, that contains hyperlinks to other documents; i.e., text that contains active pointers to other text. Usually written in HTML and accessed using a web browser. (See: hypermedia.)

Hypertext Markup Language (HTML): A platform-independent system of syntax and semantics (RFC 1866) for adding characters to data files (particularly text files) to represent the data's structure and to point to related data, thus creating hypertext for use in the World Wide Web and other applications. (Compare: XML.)

Hypertext Transfer Protocol (HTTP): A TCP-based, Application-Layer, client-server, Internet protocol (RFC 2616) that is used to carry data requests and responses in the World Wide Web. (See: hypertext.)

IAB: See: Internet Architecture Board.

IANA: See: Internet Assigned Numbers Authority.

IATF: See: Information Assurance Technical Framework.

ICANN: See: Internet Corporation for Assigned Names and Numbers.

ICMP: See: Internet Control Message Protocol.

ICMP flood: A denial-of-service attack that sends a host more ICMP echo request ("ping") packets than the protocol implementation can handle. (See: flooding, smurf.)

ICRL: See: indirect certificate revocation list.

IDEA: See: International Data Encryption Algorithm.

Identification: An act or process that presents an identifier to a system so that the system can recognize a system entity and distinguish it from other entities. (See: authentication.)

Identification information: Synonym for "identifier"; synonym for "authentication information". (See: authentication, identifying information.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for either of those terms; this term (a) is not as precise as they are and (b) mixes concepts in a potentially misleading way. Instead, use "identifier" or "authentication information", depending on what is meant.

Identification Protocol: A client-server Internet protocol for learning the identity of a user of a particular TCP connection.

Tutorial: Given a TCP port number pair, the server returns a character string that identifies the owner of that connection on the server's system. The protocol does not provide an authentication service and is not intended for authorization or access control. At best, it provides additional auditing information with respect to TCP.

Identifier: A data object -- often, a printable, non-blank character string -- that definitively represents a specific identity of a system entity, distinguishing that identity from all others. (Compare: identity.)

Tutorial: Identifiers for system entities must be assigned very carefully, because authenticated identities are the basis for other security services, such as access control service.

Identifier credential:

1. See: (authentication) under "credential".

2. Synonym for "signature certificate".

Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term is used in many ways and could easily be misunderstood.

identifying information: Synonym for "identifier"; synonym for "authentication information". (See: authentication, identification information.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for either of those terms; this term (a) is not as precise as they are and (b) mixes concepts in a potentially misleading way. Instead, use "identifier" or "authentication information", depending on what is meant.

Identity: The collective aspect of a set of attribute values (i.e., a set of characteristics) by which a system user or other system entity is recognizable or known. (See: authenticate, registration. Compare: identifier.)

Usage: A DOCUMENT MAY apply this term to either a single entity or a set of entities. If the DOCUMENT involves both meanings, the DOCUMENT SHOULD use the following terms and definitions to avoid ambiguity:

- "Singular identity": An identity that is registered for an entity that is one person or one process.

"Shared identity": An identity that is registered for an entity that is a set of singular entities

(1) in which each member is authorized to assume the identity individually and

(2) for which the registering system maintains a record of the singular entities that comprise the set.

In this case, we would expect each member entity to be registered with a singular identity before becoming associated with the shared identity. - "Group identity": An identity that is registered for an entity (1) that is a set of entities (2) for which the registering system does not maintain a record of singular entities that comprise the set.

Tutorial: When security services are based on identities, two properties are desirable for the set of attributes used to define identities:

- The set should be sufficient to distinguish each entity from all other entities, i.e., to represent each entity uniquely.
- The set should be sufficient to distinguish each identity from any other identities of the same entity.

The second property is needed if a system permits an entity to register two or more concurrent identities. Having two or more identities for the same entity implies that the entity has two separate justifications for registration. In that case, the set of attributes used for identities must be sufficient to represent multiple identities for a single entity. Having two or more identities registered for the same entity is different from concurrently associating two different identifiers with the same identity, and also is different from a single identity concurrently accessing the system in two different roles. (See: principal, role-based access control.) When an identity of a user is being registered in a system, the system may require presentation of evidence that proves the identity's authenticity (i.e., that the user has the right to claim or use the identity) and its eligibility (i.e., that the identity is qualified to be registered and needs to be registered). The following diagram illustrates how this term relates to some other terms in a PKI system: authentication information, identifier, identifier credential, registration, registered user, subscriber, and user.

Identity-based security policy: "A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources (objects being accessed)."

Identity proofing: A process that vets and verifies the information that is used to establish the identity of a system entity.

IDS: See: intrusion detection system.

IEEE: See: Institute of Electrical and Electronics Engineers, Inc.

IEEE 802.10: An IEEE committee developing security standards for LANs. (See: SILS.)

IEEE P1363: An IEEE working group, Standard for Public-Key Cryptography, engaged in developing a comprehensive reference standard for asymmetric cryptography. Covers discrete logarithm (e.g., DSA), elliptic curve, and integer factorization (e.g., RSA); and covers key agreement, digital signature, and encryption.

IESG: See: Internet Engineering Steering Group.

IETF: See: Internet Engineering Task Force.

IKE: See: IPsec Key Exchange.

IMAP4: See: Internet Message Access Protocol, version 4.

IMAP4 AUTHENTICATE: An IMAP4 command (better described as a transaction type, or sub-protocol) by which an IMAP4 client optionally proposes a mechanism to an IMAP4 server to authenticate the client to the server and provide other security services. (See: POP3.)

Tutorial: If the server accepts the proposal, the command is followed by performing a challenge-response authentication protocol and, optionally, negotiating a protection mechanism for subsequent POP3 interactions. The security mechanisms that are used by IMAP4 AUTHENTICATE -- including Kerberos, GSS-API, and S-Key.

Impossible: Cannot be done in any reasonable amount of time. (See: break, brute force, strength, work factor.)

In the clear: Not encrypted. (See: clear text.)

Ina Jo: A methodology, language, and integrated set of software tools developed at the System Development Corporation for specifying, coding, and verifying software to produce correct and reliable programs. Usage: a.k.a. the Formal Development Methodology.

Incapacitation: A type of threat action that prevents or interrupts system operation by disabling a system component. (See: disruption.)

Usage: This type of threat action includes the following subtypes: - "Malicious logic": In context of incapacitation, any hardware, firmware, or software (e.g., logic bomb) intentionally introduced into a system to destroy system functions or resources. (See: corruption, main entry for "malicious logic", masquerade, misuse.)

- "Physical destruction": Deliberate destruction of a system component to interrupt or prevent system operation.
- "Human error": (incapacitation) Action or inaction that unintentionally disables a system component. (See: corruption, exposure.)
- "Hardware or software error": (incapacitation) Error that unintentionally causes failure of a system component and leads to disruption of system operation. (See: corruption, exposure.)
- "Natural disaster": (incapacitation) Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

Incident: See: security incident.

INCITS: See: "International Committee for Information Technology Standardization" under "ANSI".

Indicator: An action -- either specific, generalized, or theoretical -- that an adversary might be expected to take in preparation for an attack. (See: "attack sensing, warning, and response". Compare: message indicator.)

Indirect attack: See: secondary definition under "attack". Compare: direct attack.

Indirect certificate revocation list (ICRL): In X.509, a CRL that may contain certificate revocation notifications for certificates issued by CAs other than the issuer (i.e., signer) of the ICRL.

Indistinguishability: An attribute of an encryption algorithm that is a formalization of the notion that the encryption of some string is indistinguishable from the encryption of an equal-length string of nonsense.

Inference:

1. A type of threat action that reasons from characteristics or byproducts of communication and thereby indirectly accesses sensitive data, but not necessarily the data contained in the communication. (See: traffic analysis, signal analysis.)
2. A type of threat action that indirectly gains unauthorized access to sensitive information in a database management system by correlating query responses with information that is already known.

Inference control: Protection of data confidentiality against inference attack. (See: traffic-flow confidentiality.)

Tutorial: A database management system containing N records about individuals may be required to provide statistical summaries about subsets of the population, while not revealing sensitive information about a single individual. An attacker may try to obtain sensitive information about an individual by isolating a desired record at the intersection of a set of overlapping queries. A system can attempt to prevent this by restricting the size and overlap of query sets, distorting responses by rounding or otherwise perturbing database values, and limiting queries to random samples. However, these techniques may be impractical to implement or use, and no technique is totally effective. For example, restricting the minimum size of a query set -- that is, not responding to queries for which there are fewer than K or more than N-K records that satisfy the query -- usually cannot prevent unauthorized disclosure. An attacker can pad small query sets with extra records, and then remove the effect of the extra records. The formula for identifying the extra records is called the "tracker".

INFOCON: See: information operations condition

Informal: Expressed in natural language. [CCIB] (Compare: formal, semiformal.)

Information:

1. Facts and ideas, which can be represented (encoded) as various forms of data.

2. Knowledge -- e.g., data, instructions -- in any medium or form that can be communicated between system entities.

Tutorial: Internet security could be defined simply as protecting information in the Internet. However, the perceived need to use different protective measures for different types of information (e.g., authentication information, classified information, collateral information, national security information, personal information, protocol control information, sensitive compartmented information, sensitive information) has led to the diversity of terminology listed in this Glossary.

Information assurance: (U.S. Government) "Measures that protect and defend information and information systems by ensuring their availability integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

Information Assurance Technical Framework (IATF): A publicly available document [IATF], developed through a collaborative effort by organizations in the U.S. Government and industry, and issued by NSA. Intended for security managers and system security engineers as a tutorial and reference document about security problems in information systems and networks, to improve awareness of tradeoffs among available technology solutions and of desired characteristics of security approaches for particular problems.

Information domain: See: secondary definition under "domain".

Information domain security policy: See: secondary definition under "domain".

Information flow policy: (formal model) A triple consisting of a set of security levels (or their equivalent security labels), a binary operator that maps each pair of security levels into a security level, and a binary relation on the set that selects a set of pairs of levels such that information is permitted to flow from an object of the first level to an object of the second level. (See: flow control, lattice model.)

Information operations condition (INFOCON): A comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. (See: threat)

Derivation: From DEFCON, i.e., defense condition.

Tutorial: The U.S. DoD defines five INFOCON levels: NORMAL (normal activity), ALPHA (increased risk of attack), BRAVO (specific risk of attack), CHARLIE (limited attack), and DELTA (general attack).

Information security (INFOSEC): Measures that implement and assure security services in information systems, including in computer systems (see: COMPUSEC) and in communication systems (see: COMSEC).

Information system: An organized assembly of computing and communication resources and procedures -- i.e., equipment and services, together with their supporting infrastructure, facilities, and personnel – that create, collect, record, process, store, transport, retrieve, display, disseminate, control, or dispose of information to accomplish a specified set of functions. (See: system entity, system resource. Compare: computer platform.)

Information Technology Security Evaluation Criteria (ITSEC): A Standard [ITSEC] jointly developed by France, Germany, the Netherlands, and the United Kingdom for use in the European Union; accommodates a wider range of security assurance and functionality combinations than the TCSEC. Superseded by the Common Criteria.

INFOSEC: See: information security.

Ingress filtering: A method for countering attacks that use packets with false IP source addresses, by blocking such packets at the boundary between connected networks.

Tutorial: Suppose network A of an internet service provider (ISP) includes a filtering router that is connected to customer network B, and an attacker in B at IP source address "foo" attempts to send packets with false source address "bar" into A. The false address may be either fixed or randomly changing, and it may either be unreachable or be a forged address that legitimately exists within either B or some other network C. In ingress filtering, the ISP's router blocks all inbound packet that arrive from B with a source address that is not within the range of legitimately advertised addresses for B. This method does not prevent all attacks that can originate from B, but the actual source of such attacks can be more easily traced because the originating network is known.

Initialization value (IV): (cryptography) An input parameter that sets the starting state of a cryptographic algorithm or mode. (Compare: activation data.)

Tutorial: An IV can be used to synchronize one cryptographic process with another; e.g., CBC, CFB, and OFB use IVs. An IV also can be used to introduce cryptographic variance (see: salt) besides that provided by a key.

Initialization vector: (cryptography) Synonym for "initialization value".

Deprecated Term: To avoid international misunderstanding, DOCUMENTs SHOULD NOT use this term in the context of cryptography because most dictionary definitions of "vector" includes a concept of direction or magnitude, which are irrelevant to cryptographic use.

Insertion:

1. See: secondary definition under "stream integrity service".

2. (threat action) See: secondary definition under "falsification".

Inside attack: See: secondary definition under "attack". Compare: insider.

Insider:

1. A user (usually a person) that accesses a system from a position that is inside the system's security perimeter. (Compare: authorized user, outsider, unauthorized user.)

   Tutorial: An insider has been assigned a role that has more privileges to access system resources than do some other types of users, or can access those resources without being constrained by some access controls that are applied to outside users.

2. A person with authorized physical access to the system.

   Example: In this sense, an office janitor is an insider, but a burglar or casual visitor is not.

3. (O) A person with an organizational status that causes the system or members of the organization to view access requests as being authorized. Example: In this sense, a purchasing agent is an insider but a vendor is not.

Inspectable space: (EMSEC) "Three-dimensional space surrounding equipment that process classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists." (Compare: control zone, TEMPEST zone.)

Institute of Electrical and Electronics Engineers, Inc. (IEEE): The IEEE is a not-for-profit association of approximately 300,000 individual members in 150 countries. The IEEE produces nearly one third of the world's published literature in electrical engineering, computers, and control technology; holds hundreds of major, annual conferences; and maintains more than 800 active standards, with many more under development. (See: SILS.)

Integrity: See: data integrity, datagram integrity service, correctness integrity, source integrity, stream integrity service, system integrity.

integrity check: A computation that is part of a mechanism to provide data integrity service or data origin authentication service. (Compare: checksum.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for "cryptographic hash" or "protected checksum". This term unnecessarily duplicates the meaning of other, well-established terms;

Integrity label: A security label that tells the degree of confidence that may be placed in the data, and may also tell what countermeasures are required to be applied to protect the data from alteration and destruction. (See: integrity. Compare: classification label.)

Intelligent threat: A circumstance in which an adversary has the technical and operational ability to detect and exploit a vulnerability and also has the demonstrated, presumed, or inferred intent to do so.

Interception: A type of threat action whereby an unauthorized entity directly accesses sensitive data while the data is traveling between authorized sources and destinations.

Usage: This type of threat action includes the following subtypes:

- "Theft": Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.
- "Wiretapping (passive)": Monitoring and recording data that is flowing between two points in a communication system. (See: wiretapping.)
- "Emanations analysis": Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but was not intended to communicate the data. (See: emanation.)

I**nterference:** (threat action(See: secondary definition under "obstruction".

I**ntermediate CA:** The CA that issues a cross-certificate to another CA. [X509] (See: cross-certification.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term because it is not widely known and mixes concepts in a potentially misleading way. For example, suppose that end entity 1 ("EE1) is in one PKI ("PKI1"), end entity 2 ("EE2) is in another PKI ("PKI2"), and the root in PKI1 ("CA1") cross-certifies the root CA in PKI2 ("CA2"). Then, if EE1 constructs the certification path CA1-to-CA2-to-EE2 to validate a certificate of EE2, conventional English usage would describe CA2 as being in the "intermediate" position in that path, not CA1.

I**nternal controls:** (COMPUSEC) Functions, features, and technical characteristics of computer hardware and software, especially of operating systems. Includes mechanisms to regulate the operation of a computer system with regard to access control, flow control, and inference control. (Compare: external controls.)

International Data Encryption Algorithm (IDEA): A patented, symmetric block cipher that uses a 128-bit key and operates on 64-bit blocks. (See: symmetric cryptography.) International Standard (N) See: secondary definition under "ISO".

International Traffic in Arms Regulations (ITAR): Rules issued by the U.S. State Department, by authority of the Arms Export Control Act (22 U.S.C. 2778), to control export and import of defense articles and defense services, including information security systems, such as cryptographic systems, and TEMPEST suppression technology. (See: type 1 product, Wassenaar Arrangement.)

Internet: The internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share

(a) the protocol suite specified by the IAB (RFC 2026) and

(b) the name and address spaces managed by the ICANN. (See: Internet Layer, Internet Protocol Suite.)

Internet Architecture Board (IAB): A technical advisory group of the ISOC, chartered by the ISOC Trustees to provide oversight of Internet architecture and protocols and, in the context of Internet Standards, a body to which decisions of the IESG may be appealed. Responsible for approving appointments to the IESG from among nominees submitted by the IETF nominating committee. (RFC 2026)

Internet Assigned Numbers Authority (IANA): From the early days of the Internet, the IANA was chartered by the ISOC and the U.S. Government's Federal Network Council to be the central coordination, allocation, and registration body for parameters for Internet protocols. Superseded by ICANN.

Internet Control Message Protocol (ICMP): An Internet Standard protocol (RFC 792) that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

Internet Corporation for Assigned Names and Numbers (ICANN): The non-profit, private corporation that has assumed responsibility for the IP address space allocation, protocol parameter assignment, DNS management, and root server system management functions formerly performed under U.S. Government contract by IANA and other entities.

Tutorial: The IPS, as defined by the IETF and the IESG, contains numerous parameters, such as Internet addresses, domain names, autonomous system numbers, protocol numbers, port numbers, management information base OIDs, including private enterprise numbers, and many others. The Internet community requires that the values used in these parameter fields be assigned uniquely. ICANN makes those assignments as requested and maintains a registry of the current values. ICANN was formed in October 1998, by a coalition of the Internet's business, technical, and academic communities. The U.S. Government designated ICANN to serve as the global consensus entity with responsibility for coordinating four key functions for the Internet: allocation of IP address space, assignment of protocol parameters, management of the DNS, and management of the DNS root server system.

I**nternet-Draft:** A working document of the IETF, its areas, and its working groups. (RFC 2026) (Compare: RFC.)

Usage: The term is customarily hyphenated when used either as a adjective or a noun, even though the latter is not standard English punctuation.

Tutorial: An Internet-Draft is not an archival document like an RFC is. Instead, an Internet-Draft is a preliminary or working document that is valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time. It is inappropriate to use an Internet-Draft as reference material or to cite it other than as a "work in progress". Although most of the Internet-Drafts are produced by the IETF, any interested organization may request to have its working documents published as Internet-Drafts.

Internet Engineering Steering Group (IESG): The part of the ISOC responsible for technical management of IETF activities and administration of the Internet Standards Process according to procedures approved by the ISOC Trustees. Directly responsible for actions along the "standards track", including final approval of specifications as Internet Standards. Composed of IETF Area Directors and the IETF chairperson, who also chairs the IESG. (RFC 2026)

Internet Engineering Task Force (IETF): A self-organized group of people who make contributions to the development of Internet technology. The principal body engaged in developing Internet Standards, although not itself a part of the ISOC. Composed of Working Groups, which are arranged into Areas (such as the Security Area), each coordinated by one or more Area Directors. Nominations to the IAB and the IESG are made by a committee selected at random from regular IETF meeting attendees who have volunteered.

Internet Key Exchange (IKE): An Internet, IPsec, key-establishment protocol for putting in place authenticated keying material

(a) for use with ISAKMP and

(b) for other security associations, such as in AH and ESP.

Tutorial: IKE is based on three earlier protocol designs: ISAKMP, OAKLEY, and SKEME.

Internet Layer: See: Internet Protocol Suite.

Internet Message Access Protocol, version 4 (IMAP4): An Internet protocol (RFC 2060) by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client. (See: POP3.)

Internet Open Trading Protocol (IOTP): An Internet protocol proposed as a general framework for Internet commerce, able to encapsulate transactions of various proprietary payment systems (e.g., GeldKarte, Mondex, SET, Visa Cash). Provides optional security services by incorporating various Internet security mechanisms (e.g., MD5) and protocols (e.g., TLS).

Internet Policy Registration Authority (IPRA): An X.509-compliant CA that is the top CA of the Internet certification hierarchy operated under the auspices of the ISOC (See: (PEM) under "certification hierarchy".)

Internet Private Line Interface (IPLI): A successor to the PLI, updated to use TCP/IP and newer military-grade COMSEC equipment (TSEC(KG-84). The IPLI was a portable, modular system that was developed for use in tactical, packet-radio networks. (See: end-to-end encryption.)

Internet Protocol (IP): An Internet Standard, Internet-Layer protocol that moves datagrams (discrete sets of bits) from one computer to another across an internetwork but does not provide reliable delivery, flow control, sequencing, or other end-to-end services that TCP provides. IP version 4 (IPv4) is specified in RFC 791, and IP version 6 (IPv6) is specified in RFC 2460. (See: IP address, TCP(IP.)

Tutorial: If IP were used in an OSI-RM stack, IP would be placed at the top of Layer 3, above other Layer 3 protocols in the stack. In any IPS stack, IP is always present in the Internet Layer and is always placed at the top of that layer, on top of any other protocols that are used in that layer. In some sense, IP is the only protocol specified for the IPS Internet Layer; other protocols used there, such as AH and ESP, are just IP variations.

Internet Protocol security: See: IP Security Protocol.

Internet Protocol Security Option (IPSO) Refers to one of three types of IP security options, which are fields that may be added to an IP datagram for carrying security information about the datagram. (Compare: IPsec.)

Deprecated Usage: DOCUMENTS SHOULD NOT use this term without a modifier to indicate which of the following three types is meant:

- "DoD Basic Security Option" (IP option type 130): Defined for use on U.S. DoD common-use data networks. Identifies the DoD classification level at which the datagram is to be protected and the protection authorities whose rules apply to the datagram. (A "protection authority" is a National Access Program (e.g., GENSER, SIOP-ESI, SCI, NSA, Department of Energy)
- "DoD Extended Security Option" (IP option type 133): Permits additional security labeling information, beyond that present in the Basic Security Option, to be supplied in the datagram to meet the needs of registered authorities. [R1108]
- "Common IP Security Option" (CIPSO) (IP option type 134): Designed by TSIG to carry hierarchic and non-hierarchic security labels. (Formerly called "Commercial IP Security Option"; a version 2.3 draft was published 9 March 1993 as an Internet-Draft but did not advance to RFC form.)

Internet Protocol Suite (IPS): The set of network communication protocols that are specified by the IETF, and approved as Internet Standards by the IESG, within the oversight of the IAB. (See: OSI-RM Security Architecture. Compare: OSI-RM.)

Usage: This set of protocols is popularly known as "TCP-IP" because TCP and IP are its most basic and important components. For clarity, this Glossary refers to IPS protocol layers by name and capitalizes those names, and refers to OSI-RM protocol layers by number.

Tutorial: The IPS does have architectural principles, but there is no Internet Standard that defines a layered IPS reference model like the OSI-RM. Still, Internet community literature has referred (inconsistently) to IPS layers since early in the Internet's development.

- **IPS Application Layer:** The user runs an application program. The program selects the data transport service it needs --either a sequence of data messages or a continuous stream of data -- and hands application data to the Transport Layer for delivery. - IPS Transport Layer: This layer divides application data into packets, adds a destination address to each, and communicates them end-to-end -- from one application program to another -- optionally regulating the flow and ensuring reliable (errorfree and sequenced) delivery.
- **IPS Internet Layer:** This layer carries transport packets in IP datagrams. It moves each datagram independently, from its source computer to its addressed destination computer, routing the datagram through a sequence of networks and relays and selecting appropriate network interfaces en route.
- **IPS Network Interface Layer**: This layer accepts datagrams for transmission over a specific network. This layer specifies interface conventions for carrying IP over OSI-RM Layer 3 protocols and over Media Access Control sublayer protocols of OSI-RM Layer 2. An example is IP over IEEE 802 (RFD 1042).
- **IPS Network Hardware Layer**: This layer consists of specific, physical communication media. However, the IPS does not specify its own peer-to-peer protocols in this layer. Instead, the layering conventions specified by the Network Interface Layer use Layer 2 and Layer 3 protocols that are specified by bodies other than the IETF. That is, the IPS addresses *inter*-network functions and does not address *intra*-network functions. The two models are most dissimilar in the upper layers, where the IPS model does not include Session and Presentation layers. However, this omission causes fewer functional differences between the models than might be imagined, and the differences have relatively few security implications: - Formal separation of OSI-RM Layers 5, 6, and 7 is not needed in implementations; the functions of these layers sometimes are mixed in a single software unit, even in protocols in the OSI suite.

- Some OSI-RM Layer 5 services -- for example, connection termination -- are built into TCP, and the remaining Layer 5 and 6 functions are built into IPS Application-Layer protocols where needed.
- The OSI-RM does not place any security services in Layer 5 (see: OSI-RM Security Architecture).
- The lack of an explicit Presentation Layer in the IPS sometimes makes it simpler to implement security in IPS applications. For example, a primary function of Layer 6 is to convert data between internal and external forms, using a transfer syntax to unambiguously encode data for transmission. If an OSI-RM application encrypts data to protect against disclosure during transmission, the transfer encoding must be done before the encryption. If an application does encryption, as is done in OSI message handling and directory service protocols, then Layer 6 functions must be replicated in Layer 7.

The two models are most alike at the top of OSI-RM Layer 3, where the OSI Connectionless Network Layer Protocol (CLNP) and the IPS IP are quite similar. Connection-oriented security services offered in OSI-RM Layer 3 are inapplicable in the IPS, because the IPS Internet Layer lacks the explicit, connection-oriented service offered in the OSI-RM.

Internet Security Association and Key Management Protocol (ISAKMP): An Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

Tutorial: ISAKMP supports negotiation of security associations for protocols at all IPS layers. By centralizing management of security associations, ISAKMP reduces duplicated functionality within each protocol. ISAKMP can also reduce connection setup time, by negotiating a whole stack of services at once. Strong authentication is required on ISAKMP exchanges, and a digital signature algorithm based on asymmetric cryptography is used within ISAKMP's authentication component. ISAKMP negotiations are conducted in two "phases":

- "Phase 1 negotiation". A phase 1 negotiation establishes a security association to be used by ISAKMP to protect its own protocol operations.
- "Phase 2 negotiation". A phase 2 negotiation (which is protected by a security association that was established by a phase 1 negotiation) establishes a security association to be used to protect the operations of a protocol other than ISAKMP, such as ESP.

Internet Society (ISOC): A professional society concerned with Internet development (including technical Internet Standards); with how the Internet is and can be used; and with social, political, and technical issues that result. The ISOC Board of Trustees approves appointments to the IAB from among nominees submitted by the IETF nominating committee

Internet Standard: A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

Tutorial: The "Internet Standards Process" is an activity of the ISOC and is organized and managed by the IAB and the IESG. The process is concerned with all protocols, procedures, and conventions used in or by the Internet, whether or not they are part of the IPS.

Internetwork: A system of interconnected networks; a network of networks. Usually shortened to "internet". (See: internet, Internet.) Tutorial: An internet can be built using OSI-RM Layer 3 gateways to implement connections between a set of similar subnetworks. With dissimilar subnetworks, i.e., subnetworks that differ in the Layer 3 protocol service they offer, an internet can be built by implementing a uniform internetwork protocol (e.g., IP) that operates at the top of Layer 3 and hides the underlying subnetworks' heterogeneity from hosts that use communication services provided by the internet. (See: router.)

Intranet: A computer network, especially one based on Internet technology, that an organization uses for its own internal (and usually private) purposes and that is closed to outsiders. (See: extranet, VPN.)

Intruder: An entity that gains or attempts to gain access to a system or system resource without having authorization to do so. (See: intrusion. Compare: adversary, cracker, hacker.)

Intrusion:

1. A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so. (See: IDS.)
2. A type of threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. (See: unauthorized disclosure.)

Usage: This type of threat action includes the following subtypes: - "Trespass": Gaining physical access to sensitive data by circumventing a system's protections.

- "Penetration": Gaining logical access to sensitive data by circumventing a system's protections.
- "Reverse engineering": Acquiring sensitive data by disassembling and analyzing the design of a system component.
- "Cryptanalysis": Transforming encrypted data into plain text without having prior knowledge of encryption parameters or processes. (See: main entry for "cryptanalysis".)

I**ntrusion detection:** Sensing and analyzing system events for the purpose of noticing (i.e., becoming aware of) attempts to access system resources in an unauthorized manner. (See: anomaly detection, IDS, misuse detection. Compare: extrusion detection.) [IDSAN, IDSSC, IDSSE, IDSSY]

Usage: This includes the following subtypes:

- "Active detection": Real-time or near-real-time analysis of system event data to detect current intrusions, which result in an immediate protective response.
- "Passive detection": Off-line analysis of audit data to detect past intrusions, which are reported to the system security officer for corrective action. (Compare: security audit.) intrusion detection system (IDS)

1. A process or subsystem, implemented in software or hardware, that automates the tasks of

(a) monitoring events that occur in a computer network and

(b) analyzing them for signs of security problems. (See: intrusion detection.)

2. A security alarm system to detect unauthorized entry.

Tutorial: Active intrusion detection processes can be either hostbased or network-based:- "Host-based": Intrusion detection components -- traffic sensors and analyzers -- run directly on the hosts that they are **intended to protect.**

- "Network-based": Sensors are placed on subnetwork components, and analysis components run either on subnetwork components or hosts.

I**nvalidity date:** An X.509 CRL entry extension that "indicates the date at which it is known or suspected that the [revoked certificate's private key] was compromised or that the certificate should otherwise be considered invalid."

Tutorial: This date may be earlier than the revocation date in the CRL entry, and may even be earlier than the date of issue of earlier CRLs. However, the invalidity date is not, by itself, sufficient for purposes of non-repudiation service. For example, to fraudulently repudiate a validly generated signature, a private key holder may falsely claim that the key was compromised at some time in the past.

IOTP: See: Internet Open Trading Protocol.

IP: See: Internet Protocol.

IP address: A computer's internetwork address that is assigned for use by IP and other protocols. Tutorial: An IP version 4 address has four 8-bit parts and is written as a series of four decimal numbers separated by periods. Example: The address of the host named "rosslyn.bbn.com" is 192.1.7.10. An IP version 6 address has eight 16-bit parts and is written as eight hexadecimal numbers separated by colons.

IP Security Option: See: Internet Protocol Security Option.

IP Security Protocol (IPsec):

1a. The name of the IETF working group that is specifying an architecture and set of protocols to provide security services for IP traffic. (See: AH, ESP, IKE, SAD, SPD. Compare: IPSO.)

1b. A collective name for the IP security architecture and associated set of protocols (primarily AH, ESP, and IKE).

Usage: In DOCUMENTS that use the abbreviation "IPsec", the letters "IP" SHOULD be in uppercase, and the letters "sec" SHOULD NOT. Tutorial: The security services provided by IPsec include access control service, connectionless data integrity service, data origin authentication service, protection against replays (detection of the arrival of duplicate datagrams, within a constrained window), data confidentiality service, and limited traffic-flow confidentiality. IPsec specifies

(a) security protocols (AH and ESP),

(b) security associations (what they are, how they work, how they are managed, and associated processing),

(c) key management (IKE), and

(d) algorithms for authentication and encryption. Implementation of IPsec is optional for IP version 4, but mandatory for IP version 6. (See: transport mode, tunnel mode.)

IPLI: See: Internet Private Line Interface.

IPRA: See: Internet Policy Registration Authority.

IPS: See: Internet Protocol Suite.

IPsec: See: IP Security Protocol.

IPSO: See: Internet Protocol Security Option.

ISAKMP: See: Internet Security Association and Key Management Protocol.

ISO: International Organization for Standardization, a voluntary, non-treaty, non-governmental organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations. (Compare: ANSI, IETF, ITU-T, W3C.) Tutorial: Legally, ISO is a Swiss, non-profit, private organization. ISO and the IEC (the International Electro-technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in developing international standards through ISO and IEC technical committees that deal with particular fields of activity. Other international governmental and non-governmental organizations, in liaison with ISO and IEC, also take part. (ANSI is the U.S. voting member of ISO. ISO is a class D member of ITUT.) The ISO standards development process has four levels of increasing maturity: Working Draft (WD), Committee Draft (CD), Draft International Standard (DIS), and International Standard (IS). (Compare: "Internet Standards Track" under "Internet Standard".) In information technology, ISO and IEC have a joint technical committee, ISO/ IEC JTC 1. DISs adopted by JTC 1 are circulated to national bodies for voting, and publication as an IS requires approval by at least 75% of the national bodies casting a vote.

ISO 17799: An International Standard that is a code of practice, derived from Part 1 of British Standard 7799, for managing the security of information systems in an organization. This standard does not provide definitive or specific material on any security topic. It provides general guidance on a wide variety of topics, but typically does not go into depth.

ISOC: See: Internet Society.

Issue: (PKI) Generate and sign a digital certificate (or a CRL) and, usually, distribute it and make it available to potential certificate users (or CRL users). (See: certificate creation.) Usage: The term "issuing" is usually understood to refer not only to creating a digital certificate (or a CRL) but also to making it available to potential users, such as by storing it in a repository or other directory or otherwise publishing it. However, the ABA explicitly limits this term to the creation process and excludes any related publishing or distribution process.

Issuer:

1. (certificate, CRL) The CA that signs a digital certificate or CRL.

Tutorial: An X.509 certificate always includes the issuer's name. The name may include a common name value.

2. (payment card,) "The financial institution or its agent that issues the unique primary account number to the cardholder for the payment card brand."

Tutorial: The institution that establishes the account for a cardholder and issues the payment card also guarantees payment for authorized transactions that use the card in accordance with card brand regulations and local legislation.

ITAR: See: International Traffic in Arms Regulations.

ITSEC: See: Information Technology System Evaluation Criteria.

ITU-T: International Telecommunications Union, Telecommunication Standardization Sector (formerly "CCITT"), a United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations". (See: X.400, X.500.)

Tutorial: The Department of State represents the United States. ITU-T works on many kinds of communication systems. ITU-T cooperates with ISO on communication protocol standards, and many Recommendations in that area are also published as an ISO standard with an ISO name and number.

IV: See: initialization value.

Jamming: An attack that attempts to interfere with the reception of broadcast communications. (See: anti-jam, denial of service. Compare: flooding.) Tutorial: Jamming uses "interference" as a type of "obstruction" intended to cause "disruption". Jamming a broadcast signal is typically done by broadcasting a second signal that receivers cannot separate from the first one. Jamming is mainly thought of in the context of wireless communication, but also can be done in some wired technologies, such as LANs that use contention techniques to share a broadcast medium.

KAK: See: key-auto-key. (Compare: KEK.)

KDC: See: Key Distribution Center.

KEA: See: Key Exchange Algorithm.

KEK: See: key-encrypting key. (Compare: KAK.)

Kerberos: A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment. (See: realm.)

Tutorial: Kerberos was originally developed by Project Athena and is named for the mythical three-headed dog that guards Hades. The system architecture includes authentication servers and ticket-granting servers that function as an ACC and a KDC. describes extensions to the Kerberos specification that modify the initial authentication exchange between a client and the KDC. The extensions employ public-key cryptography to enable the client and KDC to mutually authenticate and establish shared, symmetric keys that are used to complete the exchange.

Kernel: A small, trusted part of a system that provides services on which the other parts of the system depend. (See: security kernel.)

Kernelized Secure Operating System (KSOS): An MLS computer operating system, designed to be a provably secure replacement for UNIX Version 6, and consisting of a security kernel, non-kernel security-related utility programs, and optional UNIX application development and support environments.

Tutorial: KSOS-6 was the implementation on a SCOMP. KSOS-11 was the implementation by Ford Aerospace and Communications Corporation on the DEC PDP-11/45 and PDP-11/70 computers.

Key:

1a. (cryptography) An input parameter used to vary a transformation function performed by a cryptographic algorithm. (See: private key, public key, storage key, symmetric key, traffic key. Compare: initialization value.) 1b. (O) (cryptography) Used in singular form as a collective noun referring to keys or keying material. Example: A fill device can be used transfer key between two cryptographic devices. 2. (I) (anti-jam) An input parameter used to vary a process that determines patterns for an anti-jam measure. (See: frequency hopping, spread spectrum.)

Tutorial: A key is usually specified as a sequence of bits or other symbols. If a key value needs to be kept secret, the sequence of symbols that comprise it should be random, or at least pseudorandom, because that makes the key harder for an adversary to guess. (See: brute-force attack, cryptanalysis, strength.)

Key agreement (algorithm or protocol):

1. A key establishment method (especially one involving asymmetric cryptography) by which two or more entities, without prior arrangement except a public exchange of data (such as public keys), each can generate the same key value. That is, the method does not send a secret from one entity to the other; instead, both entities, without prior arrangement except a public exchange of data, can compute the same secret value, but that value cannot be computed by other, unauthorized entities. (See: Diffie-Hellman- Merkle, key establishment, KEA, MQV. Compare: key transport.)

2. "A method for negotiating a key value on line without transferring the key, even in an encrypted form, e.g., the Diffie-Hellman technique."

3. "The procedure whereby two different parties generate shared symmetric keys such that any of the shared symmetric keys is a function of the information contributed by all legitimate participants, so that no party [alone] can predetermine the value of the key."

Example: A message originator and the intended recipient can each use their own private key and the other's public key with the Diffie-Hellman-Merkle algorithm to first compute a shared secret value and, from that value, derive a session key to encrypt the message.

Key authentication: "The assurance of the legitimate participants in a key agreement [i.e., in a key-agreement protocol] that no non-legitimate party possesses the shared symmetric key."

key-auto-key (KAK): "Cryptographic logic [i.e., a mode of operation] using previous key to produce key." (See: CTAK, (cryptographic operation) under "mode".)

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it is neither well-known nor precisely defined. Instead, use terms associated with modes that are defined in standards, such as CBC, CFB, and OFB.

Key center: A centralized, key-distribution process (used in symmetric cryptography), usually a separate computer system, that uses master keys (i.e., KEKs) to encrypt and distribute session keys needed by a community of users.

Tutorial: An ANSI standard defines two types of key center: "key distribution center" and "key translation center".

Key confirmation: "The assurance [provided to] the legitimate participants in a key establishment protocol that the [parties that are intended to share] the symmetric key actually possess the shared symmetric key."

Key distribution: A process that delivers a cryptographic key from the location where it is generated to the locations where it is used in a cryptographic algorithm. (See: key establishment, key management.)

Key distribution center (KDC):

1. A type of key center (used in symmetric cryptography) that implements a key-distribution protocol to provide keys (usually, session keys) to two (or more) entities that wish to communicate securely. (Compare: key translation center.)
2. "COMSEC facility generating and distributing key in electrical form."

Tutorial: A KDC distributes keys to Alice and Bob, who

(a) wish to communicate with each other but do not currently share keys,

(b) each share a KEK with the KDC, and

(c) may not be able to generate or acquire keys by themselves.

Alice requests the keys from the KDC. The KDC generates or acquires the keys and makes two identical sets. The KDC encrypts one set in the KEK it shares with Alice, and sends that encrypted set to Alice. The KDC encrypts the second set in the KEK it shares with Bob, and either

(a) sends that encrypted set to Alice for her to forward to Bob or

(b) sends it directly to Bob (although the latter option is not supported in the ANSI standard).

Key encapsulation: A key recovery technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties called "recovery agents" can perform the decryption operation to retrieve the stored key.

Key-encrypting key (KEK): A cryptographic key that

(a) is used to encrypt other keys (either DEKs or other TEKs) for transmission or storage but

(b) (usually) is not used to encrypt application data. Usage: Sometimes called "key-encryption key".

Key escrow: A key recovery technique for storing knowledge of a cryptographic key or parts thereof in the custody of one or more third parties called "escrow agents", so that the key can be recovered and used in specified circumstances. (Compare: key encapsulation.)

Tutorial: Key escrow is typically implemented with split knowledge techniques. For example, the Escrowed Encryption Standard entrusts two components of a device-unique split key to separate escrow agents. The agents provide the components only to someone legally authorized to conduct electronic surveillance of telecommunications encrypted by that specific device. The components are used to reconstruct the device-unique key, and it is used to obtain the session key needed to decrypt communications.

Key establishment (algorithm or protocol):

1. A procedure that combines the key-generation and keydistribution steps needed to set up or install a secure communication association.
2. A procedure that results in keying material being shared among two or more system entities.

Tutorial: The two basic techniques for key establishment are "key agreement" and "key transport".

Key Exchange Algorithm (KEA): A key-agreement method that is based on the Diffie-Hellman-Merkle algorithm and uses 1024-bit asymmetric keys. (See: CAPSTONE, CLIPPER, FORTEZZA, SKIPJACK.)

Tutorial: KEA was developed by NSA and formerly classified at the U.S. DoD "Secret" level. On 23 June 1998, the NSA announced that KEA had been declassified.

Key generation: A process that creates the sequence of symbols that comprise a cryptographic key. (See: key management.) key generator

1. An algorithm that uses mathematical rules to deterministically produce a pseudorandom sequence of cryptographic key values.

2. An encryption device that incorporates a key-generation mechanism and applies the key to plain text to produce cipher text (e.g., by exclusive OR-ing (a) a bit-string representation of the key with (b) a bit-string representation of the plaintext).

Key length: The number of symbols (usually stated as a number of bits) needed to be able to represent any of the possible values of a cryptographic key. (See: key space.)

Key lifetime:

1. Synonym for "crypto-period". Deprecated Definition: DOCUMENTs SHOULD NOT use this term with definition 1 because a key's crypto-period may be only a part of the key's lifetime. A key could be generated at some time prior to when its crypto-period begins and might not be destroyed (i.e., zeroized) until some time after its crypto-period ends.

2. (MISSI) An attribute of a MISSI key pair that specifies a time span that bounds the validity period of any MISSI X.509 public-key certificate that contains the public component of the pair. (See: crypto-period.)

Key loader: Synonym for "fill device".

Key loading and initialization facility (KLIF): A place where ECU hardware is activated after being fabricated. (Compare: CLEF.)

Tutorial: Before going to its KLIF, an ECU is not ready to be fielded, usually because it is not yet able to receive DEKs. The KLIF employs trusted processes to complete the ECU by installing needed data such as KEKs, seed values, and, in some cases, cryptographic software. After KLIF processing, the ECU is ready for deployment.

Key management:

1a. The process of handling keying material during its life cycle in a cryptographic system; and the supervision and control of that process. (See: key distribution, key escrow, keying material, public-key infrastructure.)

Usage: Usually understood to include ordering, generating, storing, archiving, escrowing, distributing, loading, destroying, auditing, and accounting for the material.

1b. (NIST) "The activities involving the handling of cryptographic keys and other related security IVs, counters) during the entire life cycle of the keys, including

their generation, storage, distribution, entry and use, deletion or destruction, and archiving."

1c. (OSI-RM) "The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy."

Key Management Protocol (KMP) A protocol to establish a shared symmetric key between a pair (or a group) of users. (One version of KMP was developed by SDNS, and another by SILS.) Superseded by ISAKMP and IKE.

Key material: Synonym for "keying material".

Deprecated Usage: DOCUMENTS SHOULD NOT use this term as a synonym for "keying material".

Key pair: A set of mathematically related keys -- a public key and a private key -- that are used for asymmetric cryptography and are generated in a way that makes it computationally infeasible to derive the private key from knowledge of the public key. (See: Diffie-Hellman-Merkle, RSA.)

Tutorial: A key pair's owner discloses the public key to other system entities so they can use the key to

(a) encrypt data,

(b) verify a digital signature, or

(c) generate a key with a key-agreement algorithm.

The matching private key is kept secret by the owner, who uses it to (a') decrypt data, (b') generate a digital signature, or (c') generate a key with a key-agreement algorithm.

Key recovery:

1. (cryptanalysis) A process for learning the value of a cryptographic key that was previously used to perform some cryptographic operation. (See: cryptanalysis, recovery.)

2. (backup) Techniques that provide an intentional, alternate means to access the key used for data confidentiality service in an encrypted association (Compare: recovery.)

Tutorial: It is assumed that the cryptographic system includes a primary means of obtaining the key through a key-establishment algorithm or protocol. For the secondary means, there are two classes of key recovery techniques: key encapsulation and key escrow.

Key space: The range of possible values of a cryptographic key; or the number of distinct transformations supported by a particular cryptographic algorithm. (See: key length.)

Key translation center: A type of key center that implements a key-distribution protocol (based on symmetric cryptography) to convey keys between two (or more) parties who wish to communicate securely. (Compare: key distribution center.)

Tutorial: A key translation center transfers keys for future communication between Bob and Alice, who

(a) wish to communicate with each other but do not currently share keys,

(b) each share a KEK with the center, and

(c) have the ability to generate or acquire keys by themselves.

Alice generates or acquires a set of keys for communication with Bob. Alice encrypts the set in the KEK she shares with the center and sends the encrypted set to the center. The center decrypts the set, re-encrypts the set in the KEK it shares with Bob, and either (a) sends that re-encrypted set to Alice for her to forward to Bob or (b) sends it directly to Bob (although direct distribution is not supported in the ANSI standard).

Key transport (algorithm or protocol):

1. A key establishment method by which a secret key is generated by a system entity in a communication association and securely sent to another entity in the association. (Compare: key agreement.)

   Tutorial: Either (a) one entity generates a secret key and securely sends it to the other entity, or (b) each entity generates a secret value and securely sends it to the other entity, where the two values are combined to form a secret key.

   For example, a message originator can generate a random session key and then use the RSA algorithm to encrypt that key with the public key of the intended recipient.

2. "The procedure to send a symmetric key from one party to other parties. As a result, all legitimate participants share a common symmetric key in such a way that the symmetric key is determined entirely by one party."

Key update:

1. Derive a new key from an existing key. (Compare: rekey.)
2. Irreversible cryptographic process that modifies a key to produce a new key

Key validation:

1. "The procedure for the receiver of a public key to check that the key conforms to the arithmetic requirements for such a key in order to thwart certain types of attacks." (See: weak key)
2. Synonym for "certificate validation".

Deprecated Usage: DOCUMENTS SHOULD NOT use the term as a synonym for "certificate validation"; that would unnecessarily duplicate the meaning of the latter term and mix concepts in a potentially misleading way. In validating an X.509 public-key certificate, the public key contained in the certificate is normally treated as an opaque data object.

Keyed hash: A cryptographic hash (e.g.) in which the mapping to a hash result is varied by a second input parameter that is a cryptographic key. (See: checksum.)

Tutorial: If the input data object is changed, a new, corresponding hash result cannot be correctly computed without knowledge of the secret key. Thus, the secret key protects the hash result so it can be used as a checksum even when there is a threat of an active attack on the data. There are two basic types of keyed hash:

- A function based on a keyed encryption algorithm. Example: Data Authentication Code.
- A function based on a keyless hash that is enhanced by combining (e.g., by concatenating) the input data object parameter with a key parameter before mapping to the hash result. Example: HMAC.

Keying material:

1. Data that is needed to establish and maintain a cryptographic security association, such as keys, key pairs, and IVs.

2. "Key, code, or authentication information in physical or magnetic form." (Compare: COMSEC material.)

Keying material identifier (KMID):

1. An identifier assigned to an item of keying material.

2. (MISSI) A 64-bit identifier that is assigned to a key pair when the public key is bound in a MISSI X.509 public-key certificate.

Khafre: A patented, symmetric block cipher designed by Ralph C. Merkle as a plug-in replacement for DES.

Tutorial: Khafre was designed for efficient encryption of small amounts of data. However, because Khafre does not precompute tables used for encryption, it is slower than Khufu for large amounts of data.

Khufu: A patented, symmetric block cipher designed by Ralph C. Merkle as a plug-in replacement for DES.

Tutorial: Khufu was designed for fast encryption of large amounts of data. However, because Khufu precomputes tables used in encryption, it is less efficient than Khafre for small amounts of data.

KLIF: See: key loading and initialization facility.

KMID: See: keying material identifier.

Known-plaintext attack: A cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs (although the analyst may also have other clues, such as knowing the cryptographic algorithm).

Kracker: Old spelling for "cracker".

KSOS, KSOS-6, KSOS-11: See: Kernelized Secure Operating System.

L2F: See: Layer 2 Forwarding Protocol.

L2TP: See: Layer 2 Tunneling Protocol.

Label: See: time stamp, security label.

Laboratory attack: "Use of sophisticated signal recovery equipment in a laboratory environment to recover information from data storage media."

LAN: Abbreviation for "local area network"

Land attack: A denial-of-service attack that sends an IP packet that

(a) has the same address in both the Source Address and Destination Address fields

(b) contains a TCP SYN packet that has the same port number in both the Source Port and Destination Port fields.

Derivation: This single-packet attack was named for "land", the program originally published by the cracker who invented this exploit. Perhaps that name was chosen because the inventor thought of multi-packet (i.e., flooding) attacks as arriving by sea.

Language of Temporal Ordering Specification (LOTOS): A language (ISO 8807-1990) for formal specification of computer network protocols; describes the order in which events occur.

Lattice: A finite set together with a partial ordering on its elements such that for every pair of elements there is a least upper bound and a greatest lower bound.

Example: A lattice is formed by a finite set S of security levels

- i.e., a set S of all ordered pairs (x,c), where x is one of a finite set X of hierarchically ordered classification levels X(1), non-hierarchical categories C(1), ..., C(M)
- together with the "dominate" relation. Security level (x,c) is said to "dominate" (x',c') if and only if (a) x is greater (higher) than or equal to x' and (b) c includes at least all of the elements of c'. (See: dominate, lattice model.)

Tutorial: Lattices are used in some branches of cryptography, both as a basis for hard computational problems upon which cryptographic algorithms can be defined, and also as a basis for attacks on cryptographic algorithms.

Lattice model:

1. A description of the semantic structure formed by a finite set of security levels, such as those used in military organizations. (See: dominate, lattice, security model.)
2. (formal model) A model for flow control in a system, based on the lattice that is formed by the finite security levels in a system and their partial ordering. [Denn]

Law Enforcement Access Field (LEAF): A data item that is automatically embedded in data encrypted by devices (e.g., CLIPPER chip) that implement the Escrowed **Encryption Standard.**

Layer 1, 2, 3, 4, 5, 6, 7: See: OSI-RM.

Layer 2 Forwarding Protocol (L2F): An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user. (See: L2TP.)

Layer 2 Tunneling Protocol (L2TP): An Internet client-server protocol that combines aspects of PPTP and L2F and supports tunneling of PPP over an IP network or over frame relay or other switched network. (See: VPN.)

Tutorial: PPP can in turn encapsulate any OSI-RM Layer 3 protocol. Thus, L2TP does not specify security services; it depends on protocols layered above and below it to provide any needed security.

LDAP: See: Lightweight Directory Access Protocol.

Least common mechanism: The principle that a security architecture should minimize reliance on mechanisms that are shared by many users.

Tutorial: Shared mechanisms may include cross-talk paths that permit a breach of data security, and it is difficult to make a single mechanism operate in a correct and trusted manner to the satisfaction of a wide range of users.

Least privilege: The principle that a security architecture should be designed so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work. (Compare: economy of mechanism, least trust.)

Tutorial: This principle tends to limit damage that can be caused by an accident, error, or unauthorized act. This principle also tends to reduce complexity and promote modularity, which can make certification easier and more effective. This principle is similar to the principle of protocol layering, wherein each layer provides

specific, limited communication services, and the functions in one layer are independent of those in other layers.

Least trust: The principle that a security architecture should be designed in a way that minimizes (a) the number of components that require trust and (b) the extent to which each component is trusted. (Compare: least privilege, trust level.)

Legacy system: A system that is in operation but will not be improved or expanded while a new system is being developed to supersede it.

Legal non-repudiation: See: secondary definition under "non-repudiation".

Leap of faith:

1. (general security) Operating a system as though it began operation in a secure state, even though it cannot be proven that such a state was established (i.e., even though a security compromise might have occurred at or before the time when operation began).

2. (COMSEC) The initial part, i.e., the first communication step, or steps, of a protocol that is vulnerable to attack (especially a man-in-the-middle attack) during that part but, if that part is completed without being attacked, is subsequently not vulnerable in later steps (i.e., results in a secure communication association for which no man-in-the-middle attack is possible).

   Usage: This term is listed in English dictionaries, but their definitions are broad and can be interpreted in many ways in Internet contexts. Similarly, the definition stated here can be interpreted in several ways. Therefore, DOCUMENTS that use this term (especially DOCUMENTS that are protocol specifications) SHOULD state a more specific definition for it.

   Tutorial: In a protocol, a leap of faith typically consists of accepting a claim of peer identity, data origin, or data integrity without authenticating that claim. When a protocol includes such a step, the protocol might also be designed so that if a man-in-the-middle attack succeeds during the vulnerable first part, then the attacker must remain in the middle for all subsequent exchanges or else one of the legitimate parties will be able to detect the attack.

Level of concern: (U.S. DoD) A rating assigned to an information system that indicates the extent to which protective measures, techniques, and procedures must be applied. (See: critical, sensitive, level of robustness.)

Level of robustness: (U.S. DoD) A characterization of (a) the strength of a security function, mechanism, service, or solution and (b) the assurance (or confidence) that it is implemented and functioning. (See: level of concern.)

Liberty Alliance: An international consortium of more than 150 commercial, nonprofit, and governmental organizations that was created in 2001 to address technical, business, and policy problems of identity and identity-based Web services and

develop a standard for federated network identity that supports current and emerging network devices.

Lightweight Directory Access Protocol (LDAP): An Internet client-server protocol that supports basic use of the X.500 Directory (or other directory servers) without incurring the resource requirements of the full Directory Access Protocol (DAP).

Tutorial: Designed for simple management and browser applications that provide simple read(write interactive directory service. Supports both simple authentication and strong authentication of the client to the directory server.

Link:

1. A communication facility or physical medium that can sustain data communications between multiple network nodes, in the protocol layer immediately below IP.
2. (subnetwork) A communication channel connecting subnetwork relays (especially one between two packet switches) that is implemented at OSI-RM Layer 2. (See: link encryption.)

   Tutorial: The relay computers assume that links are logically passive. If a computer at one end of a link sends a sequence of bits, the sequence simply arrives at the other end after a finite time, although some bits may have been changed either accidentally (errors) or by active wiretapping.
3. (World Wide Web) See: hyperlink.

Link encryption: Stepwise (link-by-link) protection of data that flows between two points in a network, provided by encrypting data separately on each network link, i.e., by encrypting data when it leaves a host or subnetwork relay and decrypting when it arrives at the next host or relay. Each link may use a different key or even a different algorithm. (Compare: end-to-end encryption.)

Liveness: A property of a communication association or a feature of a communication protocol that provides assurance to the recipient of data that the data is being freshly transmitted by its originator, i.e., that the data is not being replayed, by either the originator or a third party, from a previous transmission. (See: fresh, nonce, replay attack.)

Logic bomb: Malicious logic that activates when specified conditions are met. Usually intended to cause denial of service or otherwise damage system resources. (See: Trojan horse, virus, worm.)

Login:

a. An act by which a system entity establishes a session in which the entity can use system resources. (See: principal, session.)
b. An act by which a system user has its identity authenticated by the system. (See: principal, session.)

Usage: Usually understood to be accomplished by providing an identifier and matching authentication information (e.g., a password) to a security mechanism that authenticates the user's identity; but sometimes refers to establishing a connection with a server when no authentication or specific authorization is involved.

Derivation: Refers to "log" file, a security audit trail that records

(a) security events, such as the beginning of a session,

(b) the names of the system entities that initiate events.

Long title: (U.S. Government) "Descriptive title of [an item of COMSEC material]."

Low probability of detection: Result of TRANSEC measures used to hide or disguise a communication.

Low probability of intercept: Result of TRANSEC measures used to prevent interception of a communication.

LOTOS: See: Language of Temporal Ordering Specification.

MAC: See: mandatory access control, Message Authentication Code, Media Access Control

Deprecated Usage: DOCUMENTS that use this term SHOULD state a definition for it because this abbreviation is ambiguous.

Magnetic remanence: Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared.

Main mode: See: (IKE) under "mode".

Maintenance hook: "Special instructions (trapdoors) in software allowing easy maintenance and additional feature development. Since maintenance hooks frequently allow entry into the code without the usual checks, they are a serious security risk if they are not removed prior to live implementation." (See: back door.)

Malicious logic: Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (See: logic bomb, Trojan horse, spyware, virus, worm. Compare: secondary definitions under "corruption", "incapacitation", "masquerade", and "misuse".)

Malware: A contraction of "malicious software". (See: malicious logic.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it is not listed in most dictionaries and could confuse international readers.

MAN: Metropolitan area network.

Man-in-the-middle attack: A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or

more of the entities involved in a communication association. (See: hijack attack, piggyback attack.)

Tutorial: For example, suppose Alice and Bob try to establish a session key by using the Diffie-Hellman-Merkle algorithm without data origin authentication service. A "man in the middle" could

(a) block direct communication between Alice and Bob and then

(b) masquerade as Alice sending data to Bob,

(c) masquerade as Bob sending data to Alice,

(d) establish separate session keys with each of them, and

(e) function as a clandestine proxy server between them to capture or modify sensitive information that Alice and Bob think they are sending only to each other.

Manager: A person who controls the service configuration of a system or the functional privileges of operators and other users. (See: administrative security. Compare: operator, SSO, user.)

Mandatory access control:

1. An access control service that enforces a security policy based on comparing:

   (a) security labels, which indicate how sensitive or critical system resources are, with

   (b) security clearances, which indicate that system entities are eligible to access certain resources. (See: discretionary access control, MAC, rule-based security policy.)

   Derivation: This kind of access control is called "mandatory" because an entity that has clearance to access a resource is not permitted, just by its own volition, to enable another entity to access that resource.

2. "A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity."

Manipulation detection code Synonym for "checksum".

Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for "checksum"; the word "manipulation" implies protection against active attacks, which an ordinary checksum might not provide. Instead, if such protection is intended, use "protected checksum" or some particular type thereof, depending on which is meant. If such protection is not intended, use "error detection code" or some specific type of checksum that is not protected.

Marking: See: time stamp, security marking.

MARS: A symmetric, 128-bit block cipher with variable key length (128 to 448 bits), developed by IBM as a candidate for the AES.

Martian: (slang) A packet that arrives unexpectedly at the wrong address or on the wrong network because of incorrect routing or because it has a non-registered or ill-formed IP address.

Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term.

Masquerade: A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. (See: deception.) Usage: This type of threat action includes the following subtypes: - "Spoof": Attempt by an unauthorized entity to gain access to a system by posing as an authorized user. - "Malicious logic": In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic. (See: corruption, incapacitation, main entry for "malicious logic", misuse.)

MCA: See: merchant certification authority.

MD2: A cryptographic hash that produces a 128-bit hash result, was designed by Ron Rivest, and is similar to MD4 and MD5 but slower.

MD4: A cryptographic hash that produces a 128-bit hash result and was designed by Ron Rivest. (See: Derivation under "MD2", SHA-1.)

MD5: A cryptographic hash that produces a 128-bit hash result and was designed by Ron Rivest to be an improved version of MD4. (See: Derivation under "MD2".)

Merchant: (SET) "A seller of goods, services, and or other information who accepts payment for these items electronically." A merchant may also provide electronic selling services and or electronic delivery of items for sale. With SET, the merchant can offer its cardholders secure electronic interactions, but a merchant that accepts payment cards is required to have a relationship with an acquirer.

Merchant certificate: (SET) A public-key certificate issued to a merchant. Sometimes used to refer to a pair of such certificates where one is for digital signature use and the other is for encryption.

Merchant certification authority (MCA): (SET) A CA that issues digital certificates to merchants and is operated on behalf of a payment card brand, an acquirer, or another party according to brand rules. Acquirers verify and approve requests for merchant certificates prior to issuance by the MCA. An MCA does not issue a CRL, but does distribute CRLs issued by root CAs, brand CAs, geopolitical CAs, and payment gateway CAs.

Mesh PKI: A non-hierarchical PKI architecture in which there are several trusted CAs rather than a single root. Each certificate user bases path validations on the public key of one of the trusted CAs, usually the one that issued that user's own public-key certificate. Rather than having superior-to-subordinate relationships between CAs, the relationships are peer-to-peer, and CAs issue cross-certificates to each other. (Compare: hierarchical PKI, trust-file PKI.)

Message Authentication Code (MAC), message authentication code

1. (capitalized) A specific ANSI standard for a checksum that is computed with a keyed hash that is based on DES. Usage: a.k.a. Data Authentication Code, which is a U.S. Government standard (See: MAC.)
2. (not capitalized) Synonym for "error detection code".

   Deprecated Term: DOCUMENTS SHOULD NOT use the uncapitalized form "message authentication code". Instead, use "checksum", "error detection code", "hash", "keyed hash", "Message Authentication Code", or "protected checksum", depending on what is meant. (See: authentication code.)

   The uncapitalized form mixes concepts in a potentially misleading way. The word "message" is misleading because it implies that the mechanism is particularly suitable for or limited to electronic mail (see: Message Handling Systems). The word "authentication" is misleading because the mechanism primarily serves a data integrity function rather than an authentication function. The word "code" is misleading because it implies that either encoding or encryption is involved or that the term refers to computer software.

Message digest: Synonym for "hash result". (See: cryptographic hash.)

Deprecated Term: DOCUMENTs SHOULD NOT use this term as a synonym for "hash result"; this term unnecessarily duplicates the meaning of the other, more general term and mixes concepts in a potentially misleading way. The word "message" is misleading because it implies that the mechanism is particularly suitable for or limited to electronic mail (see: Message Handling Systems).

Message handling system: Synonym for the Internet electronic mail system.

Deprecated Term: DOCUMENTS SHOULD NOT use this term, because it could be confused with Message Handling System. Instead, use "Internet electronic mail" or some other, more specific term.

Message Handling System: An ITU-T system concept that encompasses the notion of electronic mail but defines more comprehensive OSI systems and services that enable users to exchange messages on a store-and-forward basis. (The ISO equivalent is "Message Oriented Text Interchange System".)

Message indicator:

1. (cryptographic function) Synonym for "initialization value". (Compare: indicator.)

2. "Sequence of bits transmitted over a communications system for synchronizing cryptographic equipment."

Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for "initialization value"; the term mixes concepts in a potentially misleading way. The word "message" is misleading because it suggests that the mechanism is specific to electronic mail. (See: Message Handling System.) message integrity check

Message integrity code (MIC): Synonyms for some form of "checksum".

Deprecated Term: DOCUMENTS SHOULD NOT use these terms for any form of checksum. Instead, use "checksum", "error detection code", "hash", "keyed hash", "Message Authentication Code", or "protected checksum", depending on what is meant. These two terms mix concepts in potentially misleading ways. The word "message" is misleading because it suggests that the mechanism is particularly suitable for or limited to electronic mail. The word "integrity" is misleading because the checksum may be used to perform a data origin authentication function rather than an integrity function. The word "code" is misleading because it suggests either that encoding or encryption is involved or that the term refers to computer software.

Message Security Protocol (MSP): A secure message handling protocol for use with X.400 and Internet mail protocols. Developed by NSA's SDNS program and used in the U.S. DoD's Defense Message System.

Meta-data: Descriptive information about a data object; i.e., data about data, or data labels that describe other data. (See: security label. Compare: metadata)

Tutorial: Meta-data can serve various management purposes:

- **System management:** File name, type, size, creation date.
- **Application management**: Document title, version, author.
- **Usage management:** Data categories, keywords, classifications. Meta-data can be associated with a data object in two basic ways:
- **Explicitly:** Be part of the data object (e.g., a header field of a data file or packet) or be linked to the object.
- **Implicitly:** Be associated with the data object because of some other, explicit attribute of the object.

metadata, Metadata(trademark), METADATA(trademark) (D) Proprietary variants of "meta-data". (See: SPAM(trademark).)

MHS: See: message handling system.

MIC: See: message integrity code.

MIME See: Multipurpose Internet Mail Extensions.

MIME Object Security Services (MOSS): An Internet protocol that applies end-to-end encryption and digital signature to MIME message content, using symmetric cryptography for encryption and asymmetric cryptography for key distribution and signature. MOSS is based on features and specifications of PEM. (See: S(MIME.) Minimum Interoperability Specification for PKI Components (MISPC)

(N) A technical description to provide a basis for interoperation between PKI components from different vendors; consists primarily of a profile of certificate and CRL extensions and a set of transactions for PKI operation.

Misappropriation: A type of threat action whereby an entity assumes unauthorized logical or physical control of a system resource. (See: usurpation.)

Usage: This type of threat action includes the following subtypes:

- **Theft of data:** Unauthorized acquisition and use of data contained in a system.
- **Theft of service:** Unauthorized use of a system service.
- **Theft of functionality:** Unauthorized acquisition of actual hardware, firmware, or software of a system component.

MISPC: See: Minimum Interoperability Specification for PKI Components.

MISSI: Multilevel Information System Security Initiative, an NSA program to encourage development of interoperable, modular products for constructing secure network information systems in support of a wide variety of U.S. Government missions.

MISSI user: (MISSI) A system entity that is the subject of one or more MISSI X.509 public-key certificates issued under a MISSI certification hierarchy. (See: personality.)

Tutorial: MISSI users include both end users and the authorities that issue certificates. A MISSI user is usually a person but may be a machine or other automated process. Machines that are required to operate nonstop may be issued their own certificates to avoid downtime needed to exchange the FORTEZZA cards of machine operators at shift changes.

Mission: A statement of a (relatively long-term) duty or (relatively short-term) task that is assigned to an organization or system, indicates the purpose and objectives of the duty or task, and may indicate the actions to be taken to achieve it.

Mission critical: A condition of a system service or other system resource such that denial of access to, or lack of availability of, the resource would jeopardize a system user's ability to perform a primary mission function or would result in other serious consequences. (See: Critical. Compare: mission essential.)

Mission essential: (U.S. DoD) Refers to materiel that is authorized and available to combat, combat support, combat service support, and combat readiness training forces to accomplish their assigned missions. (Compare: mission critical.)

Misuse:

1. The intentional use (by authorized users) of system resources for other than authorized purposes. Example: An authorized system administrator creates an unauthorized account for a friend. (See: misuse detection.)

2. A type of threat action that causes a system component to perform a function or service that is detrimental to system security. (See: usurpation.)

Usage: This type of threat action includes the following subtypes:

- "Tampering": (misuse) Deliberately altering a system's logic, data, or control information to cause the system to perform unauthorized functions or services. (See: corruption, main entry for "tampering".)
- "Malicious logic": (misuse) Any hardware, firmware, or software intentionally introduced into a system to perform or control execution of an unauthorized function or service. (See: corruption, incapacitation, main entry for "malicious logic", masquerade.)
- "Violation of authorizations": Action by an entity that exceeds the entity's system privileges by executing an unauthorized function. (See: authorization.)

Misuse detection: An intrusion detection method that is based on rules that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents. (See: IDS, misuse. Compare: anomaly detection.)

MLS: See: multilevel secure

Mobile code:

1a. Software that originates from a remote server, is transmitted across a network, and is loaded onto and executed on a local client system without explicit initiation by the client's user and, in some cases, without that user's knowledge. (Compare: active content.)

Tutorial: One form of mobile code is active content in a file that is transferred across a network.

1b. (U.S. DoD) "Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient."

2a. Technology that enables the creation of executable information that can be delivered to an information system and directly executed on any hardware (software architecture that has an appropriate host execution environment.

2b. "Programs (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics" . (See: active content.)

Mode of operation:

1. (cryptographic operation) A technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream. (See: CBC, CCM, CMAC, CFB, CTR, ECB, OFB.)

2. (system operation) A type of security policy that states the range of classification levels of information that a system is permitted to handle and the range of clearances and authorizations of users who are permitted to access the system. (See: compartmented security mode, controlled security mode, dedicated security mode, multilevel security mode, partitioned security mode, system-high security mode. Compare: protection level.)

3. IKE refers to its various types of ISAKMP-scripted exchanges of messages as "modes". Among these are the following: - "Main mode": One of IKE's two phase 1 modes. (See: ISAKMP.) - "Quick mode": IKE's only phase 2 mode. (See: ISAKMP.)

Model: See: formal model, security model.

Modulus: The defining constant in modular arithmetic, and usually a part of the public key in asymmetric cryptography that is based on modular arithmetic. (See: Diffie-Hellman-Merkle, RSA.)

Mondex: A smartcard-based electronic money system that incorporates cryptography and can be used to make payments via the Internet. (See: IOTP.)

Morris Worm: A worm program that flooded the ARPANET in November 1988, causing problems for thousands of hosts. (See: community isk, worm)

MOSS: See: MIME Object Security Services.

MQV: A key-agreement protocol that was proposed by A.J. Menezes, M. Qu, and S.A. Vanstone in 1995 and is based on the Diffie-Hellman-Merkle algorithm.

MSP: See: Message Security Protocol.

Multicast security: See: secure multicast

Multics: MULTiplexed Information and Computing Service, an MLS computer timesharing system designed and implemented during 1965-69 by a consortium including Massachusetts Institute of Technology, General Electric, and Bell Laboratories, and later offered commercially by Honeywell.

Tutorial: Multics was one of the first large, general-purpose, operating systems to include security as a primary goal from the inception of the design and development and was rated in TCSEC Class B2. Its many innovative hardware and software security mechanisms (e.g., protection ring) were adopted by later systems.

Multilevel secure (MLS): Describes an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security levels. (Examples: BLACKER, CANEWARE, KSOS, Multics, SCOMP.)

Multilevel security mode:

1. A mode of system operation wherein

   (a) two or more security levels of information are allowed to be to be handled concurrently within the same system when some users having access to the system have neither a security clearance nor need-to-know for some of the data handled by the system and

   (b) separation of the users and the classified material on the basis, respectively, of clearance and classification level are dependent on operating system control. (See: (system operation) under "mode", need to know, protection level, security clearance. Compare: controlled mode.)

   Usage: Usually abbreviated as "multilevel mode". This term was defined in U.S. Government policy regarding system accreditation, but the term is also used outside the Government.

2. A mode of system operation in which all three of the following statements are true:

   (a) Some authorized users do not have a security clearance for all the information handled in the system.

   (b) All authorized users have the proper security clearance and appropriate specific access approval for the information to which they have access.

   (c) All authorized users have a need-to-know only for information to which they have access. (See: formal access approval, protection level.)

Multipurpose Internet Mail Extensions (MIME): An Internet protocol that enhances the basic format of Internet electronic mail messages

(a) to enable character sets other than U.S. ASCII to be used for textual headers and content and

(b) to carry non-textual and multi-part content. (See: S(MIME.)

Mutual suspicion: The state that exists between two interacting system entities in which neither entity can trust the other to function correctly with regard to some security requirement.

Name: Synonym for "identifier".

Naming authority: An organizational entity responsible for assigning DNs and for assuring that each DN is meaningful and unique within its domain.

National Computer Security Center (NCSC): A U.S. DoD organization, housed in NSA, that has responsibility for encouraging widespread availability of trusted systems throughout the U.S. Federal Government. It has established criteria for, and performed evaluations of, computer and network systems that have a TCB. (See: Rainbow Series, TCSEC.)

National Information Assurance Partnership (NIAP): A joint initiative of NIST and NSA to enhance the quality of commercial products for information security and increase consumer confidence in those products through objective evaluation and testing methods.

Tutorial: NIAP is registered, through the U.S. DoD, as a National Performance Review Reinvention Laboratory. NIAP functions include the following:

- Developing tests, test methods, and other tools that developers and testing laboratories may use to improve and evaluate security products.
- Collaborating with industry and others on research and testing programs.
- Using the Common Criteria to develop protection profiles and associated test sets for security products and systems.
- Cooperating with the NIST National Voluntary Laboratory
- Accreditation Program to develop a program to accredit private-sector laboratories for the testing of information security products using the Common Criteria.

National Institute of Standards and Technology (NIST): A U.S. Department of Commerce organization that promotes U.S economic growth by working with industry to develop and apply technology, measurements, and standards. Has primary U.S. Government responsibility for INFOSEC standards for sensitive unclassified information. (See: ANSI, DES, DSA, DSS, FIPS, NIAP, NSA.)

National Reliability and Interoperability Council (NRIC): An advisory committee chartered by the U.S. Federal Communications Commission (FCC), with participation by network service providers and vendors, to provide recommendations to the FCC for assuring reliability, interoperability, robustness, and security of wireless, wireline, satellite, cable, and public data communication networks.

National security: (U.S. Government) The national defense or foreign relations of the United States of America.

National Security Agency (NSA): A U.S. DoD organization that has primary U.S. Government responsibility for INFOSEC standards for classified information and for sensitive unclassified information handled by national security systems. (See: FORTEZZA, KEA, MISSI, national security system, NIAP, NIST, SKIPJACK.)

National security information: (U.S. Government) Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure.

National security system: (U.S. Government) Any Government-operated information system for which the function, operation, or use

(a) involves intelligence activities;

(b) involves cryptologic activities related to national security;

(c) involves command and control of military forces;

(d) involves equipment that is an integral part of a weapon or weapon system; or

(e) is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [Title 40 U.S.C. Section 1552, Information Technology Management Reform Act of 1996.] (See: type 2 product.)

Natural disaster: (threat action) See: secondary definitions under "corruption" and "incapacitation".

NCSC: See: National Computer Security Center.

Need to know, need-to-know: The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

Usage: The compound "need-to-know" is commonly used as either an adjective or a noun.

Tutorial: The need-to-know criterion is used in security procedures that require a custodian of sensitive information, prior to disclosing the information to someone else, to establish that the intended recipient has proper authorization to access the information.

Network: An information system comprised of a collection of interconnected nodes. (See: computer network.)

Network Hardware Layer: See: Internet Protocol Suite.

Network Interface Layer: See: Internet Protocol Suite.

Network Layer Security Protocol (NLSP): An OSI protocol (IS0 11577) for end-to-end encryption services at the top of OSI-RM Layer 3. NLSP is derived from SP3 but is more complex. (Compare: IPsec.)

Network Substrate Layer: Synonym for "Network Hardware Layer".

Network weaving: A penetration technique in which an intruder avoids detection and traceback by using multiple, linked, communication networks to access and attack a system.

NIAP: See: National Information Assurance Partnership.

Nibble: Half of a byte (i.e., usually, 4 bits).

Deprecated Term: To avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term; instead, state the size of the block explicitly (e.g., "4-bit block"). (See: Deprecated Usage under "Green Book".)

NIPRNET: The U.S. DoD's common-use Non-Classified Internet Protocol Router Network; the part of the Internet that is wholly controlled by the U.S. DoD and is used for official DoD business.

NIST: See: National Institute of Standards and Technology.

NLSP: See: Network Layer Security Protocol

No-lone zone: A room or other space or area to which no person may have unaccompanied access and that, when occupied, is required to be occupied by two or more appropriately authorized persons.(See: dual control.)

No-PIN ORA (NORA): (MISSI) An organizational RA that operates in a mode in which the ORA performs no card management functions and, therefore, does not require knowledge of either the SSO PIN or user PIN for an end user's FORTEZZA PC card.

Node: A collection of related subsystems located on one or more computer platforms at a single site. (See: site.)

Nonce: A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks. (See: fresh.)

Non-critical: See: critical.

Non-repudiation service:

1. A security service that provide protection against false denial of involvement in an association (especially a communication association that transfers data). (See: repudiation, time stamp.)

   Tutorial: Two separate types of denial are possible -- an entity can deny that it sent a data object, or it can deny that it received a data object -- and, therefore, two separate types of non-repudiation service are possible. (See: non-repudiation with proof of origin, non-repudiation with proof of receipt.)

2. "Assurance [that] the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data."

Deprecated Definition: DOCUMENTS SHOULD NOT use definition 2 because it bundles two security services

- non-repudiation with proof of origin, and non-repudiation with proof of receipt
- that can be provided independently of each other.

Usage: DOCUMENTS SHOULD distinguish between the technical aspects and the legal aspects of a non-repudiation service:

- "Technical non-repudiation": Refers to the assurance a relying party has that if a public key is used to validate a digital signature, then that signature had to have been made by the corresponding private signature key
- "Legal non-repudiation": Refers to how well possession or control of the private signature key can be established

Tutorial: Non-repudiation service does not prevent an entity from repudiating a communication. Instead, the service provides evidence that can be stored and later presented to a third party to resolve disputes that arise if and when a communication is repudiated by one of the entities involved.

Ford describes the six phases of a complete non-repudiation service and uses "critical action" to refer to the act of communication that is the subject of the service

1. Request service: Before the critical action, the service requester asks, either implicitly or explicitly, to have evidence of the action be generated.

2. Generate evidence: When the critical action occurs, evidence is generated by a process involving the potential repudiator and possibly also a trusted third party.

3. Transfer evidence: The evidence is transferred to the requester or stored by a third party, for later use (if needed).

4. Verify evidence: The entity that holds the evidence tests it to be sure that it will suffice if a dispute arises.

5. Retain evidence: The evidence is retained for possible future retrieval and use.

6. Resolve dispute: In this phase, which occurs only if the critical action is repudiated, the evidence is retrieved from storage, presented, and verified to resolve the dispute.

Non-repudiation with proof of origin: A security service that provides the recipient of data with evidence that proves the origin of the data, and thus protects the recipient against an attempt by the originator to falsely deny sending the data. (See: non-repudiation service.)

Tutorial: This service is a strong version of data origin authentication service. This service can not only verify the identity of a system entity that is the original source of received data; it can also provide proof of that identity to a third party.

Non-repudiation with proof of receipt: A security service that provides the originator of data with evidence that proves the data was received as addressed, and thus protects the originator against an attempt by the recipient to falsely deny receiving the data. (See: non-repudiation service.)

Non-volatile media: Storage media that, once written into, provide stable storage of information without an external power supply. (Compare: permanent storage, volatile media.)

NORA: See: no-PIN ORA.

Notarization: Registration of data under the authority or in the care of a trusted third party, thus making it possible to provide subsequent assurance of the accuracy of characteristics claimed for the data, such as content, origin, time of existence, and delivery. (See: digital notary.)

NRIC: See: Network Reliability and Interoperability Council.

NSA: See: National Security Agency

Null: (encryption) "Dummy letter, letter symbol, or code group inserted into an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes."

NULL encryption algorithm: An algorithm that is specified as doing nothing to transform plaintext data; i.e., a no-op. It originated because ESP always specifies the use of an encryption algorithm for confidentiality. The NULL encryption algorithm is a convenient way to represent the option of not applying encryption in ESP (or in any other context where a no-op is needed). (Compare: null.)

OAKLEY: A key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman-Merkle algorithm and designed to be a compatible component of ISAKMP

Tutorial: OAKLEY establishes a shared key with an assigned identifier and associated authenticated identities for parties; i.e., OAKLEY provides authentication service to ensure the entities of each other's identity, even if the Diffie-Hellman-Merkle exchange is threatened by active wiretapping. Also, it provides public-key forward secrecy for the shared key and supports key updates.

Object: (formal model) Trusted-system modeling usage: A system component that contains or receives information. (See: Bell-LaPadula model, object reuse, trusted system.)

Object identifier (OID):

1. An official, globally unique name for a thing, written as a sequence of integers (which are formed and assigned as defined in the ASN.1 standard) and used to reference the thing in abstract specifications and during negotiation of security services in a protocol.

2. "A value (distinguishable from all other such values) [that] is associated with an object."

   Tutorial: Objects named by OIDs are leaves of the object identifier tree (which is similar to but different from the X.500 Directory Information Tree). Each arc (i.e., each branch of the tree) is labeled with a non-negative integer. An OID is the sequence of integers on the path leading from the root of the tree to a named object. The OID tree has three arcs immediately below the root: {0} for use by ITU-T, {1} for use by ISO, and {2} for use by both jointly. Below ITU-T are four arcs, where {0 0} is for ITU-T recommendations. Below {0 0} are 26 arcs, one for each series of recommendations starting with the letters A to Z, and below these are arcs for each recommendation. Thus, the OID for ITU-T Recommendation X.509 is {0 0 24 509}. Below ISO are four arcs, where {1 0 }is for ISO standards, and below these are arcs for each ISO standard. Thus, the OID for ISO(IEC 9594-8 (the ISO number for X.509) is {1 0 9594 8}. ANSI registers organization names below the branch {joint-isoccitt 2) country(16) US(840) organization(1) gov(101) csor(3)}. The NIST CSOR records PKI objects below the branch {joint-iso-itut(2) country(16) us(840) organization (1) gov(101) csor(3)}. The U.S. DoD registers INFOSEC objects below the branch {joint-isoitu-t(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1)}. The IETF's Public-Key Infrastructure (pkix) Working Group registers PKI objects below the branch {iso(1) identifiedorganization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)}.

Object reuse: (COMPUSEC) Reassignment and reuse of an area of a storage medium (e.g., random-access memory, floppy disk, magnetic tape) that once contained sensitive data objects. Before being reassigned for use by a new subject, the area needs to be erased or, in some cases, purged.

Obstruction: A type of threat action that interrupts delivery of system services by hindering system operations. (See: disruption.)

Tutorial: This type of threat action includes the following subtypes:

- "Interference": Disruption of system operations by blocking communication of user data or control information. (See: jamming.)

- "Overload": Hindrance of system operation by placing excess burden on the performance capabilities of a system component. (See: flooding.)

OCSP: See: Online Certificate Status Protocol.

Octet: A data unit of eight bits. (Compare: byte.) Usage: This term is used in networking (especially in OSI standards) in preference to "byte", because some systems use "byte" for data storage units of a size other than eight bits.

OFB: See: output feedback.

Off-line attack: See: secondary definition under "attack".

Ohnosecond: That minuscule fraction of time in which you realize that your private key has been compromised.

Deprecated Usage: DOCUMENTS SHOULD NOT use this term; it is a joke for English speakers. (See: Deprecated Usage under "Green Book".)

OID: See: object identifier.

Online Certificate Status Protocol (OCSP): An Internet protocol used by a client to obtain from a server the validity status and other information about a digital certificate. (Mentioned in but not specified there.)

Tutorial: In some applications, such as those involving high-value commercial transactions, it may be necessary either

(a) to obtain certificate revocation status that is timelier than is possible with CRLs or

(b) to obtain other kinds of status information. OCSP may be used to determine the current revocation status of a digital certificate, in lieu of or as a supplement to checking against a periodic CRL. An OCSP client issues a status request to an OCSP server and suspends acceptance of the certificate in question until the server provides a response.

One-time pad:

1. A manual encryption system in the form of a paper pad for one-time use.
2. An encryption algorithm in which the key is a random sequence of symbols and each symbol is used for encryption only one time -- i.e., used to encrypt only one plaintext symbol and thus produce only one ciphertext symbol -- and a copy of the key is used similarly for decryption.

   Tutorial: To ensure one-time use, the copy of the key used for encryption is destroyed after use, as is the copy used for decryption. This is the only encryption algorithm that is truly unbreakable, even given unlimited resources for cryptanalysis but key management costs and synchronization problems make it impractical except in special situations.

One-time password, One-Time Password (OTP):

1. (not capitalized) A "one-time password" is a simple authentication technique in which each password is used only once as authentication information that verifies an identity. This technique counters the threat of a replay attack that uses passwords captured by wiretapping.
2. (capitalized) "One-Time Password" is an Internet protocol that is based on S(KEY and uses a cryptographic hash function to generate one-time passwords for use as authentication information in system login and in other processes that need protection against replay attacks.

One-way encryption: Irreversible transformation of plain text to cipher text, such that the plain text cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known. (See: brute force, encryption.)

One-way function: "A (mathematical) function, f, [that] is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that f(x) = y. There may be a few values of y for which finding x is not computationally difficult."

Deprecated Usage: DOCUMENTS SHOULD NOT use this term as a synonym for "cryptographic hash".

Onion routing: A system that can be used to provide both

(a) data confidentiality and

(b) traffic-flow confidentiality for network packets, and also provide

(c) anonymity for the source of the packets.

Tutorial: The source, instead of sending a packet directly to the intended destination, sends it to an "onion routing proxy" that builds an anonymous connection through several other "onion routers" to the destination. The proxy defines a route through the "onion routing network" by encapsulating the original payload in a layered data packet called an "onion", in which each layer defines the next hop in the route and each layer is also encrypted. Along the route, each onion router that receives the onion peels off one layer; decrypts that layer and reads from it the address of the next onion router on the route; pads the remaining onion to some constant size; and sends the padded onion to that next router.

Open security environment: A system environment that meets at least one of the following two conditions:

(a) Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic.

(b) Configuration control does not provide sufficient assurance that applications and the equipment are protected against the introduction of malicious logic prior to and during the operation of system applications. (See: "first law" under "Courtney's laws". Compare: closed security environment.)

Open storage: (U.S. Government) "Storage of classified information within an accredited facility, but not in General Services Administration approved secure containers, while the facility is unoccupied by authorized personnel."

Open Systems Interconnection (OSI) Reference Model (OSI-RM): A joint ISO (ITU-T standard for a seven-layer, architectural communication framework for interconnection of computers in networks. (See: OSI-RM Security Architecture. Compare: Internet Protocol Suite.)

Tutorial: OSI-RM-based standards include communication protocols that are mostly incompatible with the IPS, but also include security models, such as X.509, that are used in the Internet. The OSI-RM layers, from highest to lowest, are (7) Application, (6) Presentation, (5) Session, (4) Transport, (3) Network, (2) Data Link, and (1) Physical.

Operational integrity: Synonym for "system integrity"; this synonym emphasizes the actual performance of system functions rather than just the ability to perform them.

Operational security:

1. System capabilities, or performance of system functions, that are needed either

   (a) to securely manage a system or

   (b) to manage security features of a system. (Compare: operations security (OPSEC).)

   Usage: DOCUMENTS that use this term SHOULD state a definition because

   (a) the definition provided here is general and vague and

   (b) the term could easily be confused with "operations security", which is a different concept.

   Tutorial: For example, in the context of an Internet service provider, the term could refer to capabilities to manage network devices in the event of attacks, simplify troubleshooting, keep track of events that affect system integrity, help analyze sources of attacks, and provide administrators with control over network addresses and protocols to help mitigate the most common attacks and exploits.

2. Synonym for "administrative security".

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "administrative security". Any type of security may affect system operations; therefore, the term may be misleading.

Operations security (OPSEC): A process to identify, control, and protect evidence of the planning and execution of sensitive activities and operations, and thereby prevent potential adversaries from gaining knowledge of capabilities and intentions. (See: communications cover. Compare: operational security.)

Operator: A person who has been authorized to direct selected functions of a system. (Compare: manager, user.)

OPSEC

1. Abbreviation for "operations security".
2. Abbreviation for "operational security".

   Deprecated Usage: DOCUMENTS SHOULD NOT use this abbreviation for "operational security" (as defined in this Glossary), because its use for "operations security" has been well established for many years, particular in the military community.

ORA: See: organizational registration authority.

Orange Book: (slang) Synonym for "Trusted Computer System Evaluation Criteria"

Organizational certificate:

1. An X.509 public-key certificate in which the "subject" field contains the name of an institution or set (e.g., a business, government, school, labor union, club, ethnic group, nationality, system, or group of individuals playing the same role), rather than the name of an individual person or device. (Compare: persona certificate, role certificate.)

   Tutorial: Such a certificate might be issued for one of the following purposes:

   - To enable an individual to prove membership in the organization.
   - To enable an individual to represent the organization, i.e., to act in its name and with its powers or permissions.

2. (MISSI) A type of MISSI X.509 public-key certificate that is issued to support organizational message handling for the U.S. DoD's Defense Message System.

Organizational registration authority (ORA):

1. (PKI(An RA for an organization.
2. (MISSI) An end entity that (a) assists a PCA, CA, or SCA to register other end entities, by gathering, verifying, and entering data and forwarding it to the signing authority and (b) may also assist with card management functions. An ORA is a local administrative authority, and the term refers both to the role and to the person who plays that role. An ORA does not sign certificates, CRLs, or CKLs. (See: no-PIN ORA, SSO-PIN ORA, user-PIN ORA.)

Origin authentication: Synonym for "data origin authentication". (See: authentication, data origin authentication.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it suggests careless use of the internationally standardized term "data origin authentication" and also could be confused with "peer entity authentication."

Origin authenticity: Synonym for "data origin authentication". (See: authenticity, data origin authentication.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it suggests careless use of the internationally standardized term "data origin authentication" and mixes concepts in a potentially misleading way.

OSI, OSI-RM: See: Open Systems Interconnection Reference Model.

OSI-RM Security Architecture: The part of the OSI-RM that specifies the security services and security mechanisms that can be applied to protect communications between two systems. (See: security architecture.)

Tutorial: This part of the OSI-RM includes an allocation of security services to protocol layers. The following table shows which security services (see definitions in this Glossary) are permitted by the OSI-RM in each of its layers. (Also, an application process that operates above the Application Layer may itself provide security services.) Similarly, the table suggests which services are suitable for each IPS layer. However, explaining and justifying these allocations is beyond the scope of this Glossary.

OTAR: See: over-the-air rekeying.

OTP: See: One-Time Password.

Out-of-band: (adjective, adverb) Information transfer using a channel or method that is outside (i.e., separate from or different from) the main channel or normal method.

Tutorial: Out-of-band mechanisms are often used to distribute shared secrets (e.g., a symmetric key) or other sensitive information items (e.g., a root key) that are needed to initialize or otherwise enable the operation of cryptography or other security mechanisms. Example: Using postal mail to distribute printed or magnetic media containing symmetric cryptographic keys for use in Internet encryption devices. (See: key distribution.)

Output feedback (OFB): A block cipher mode that modifies ECB mode to operate on plaintext segments of variable length less than or equal to the block length. (See: block cipher.)

Tutorial: This mode operates by directly using the algorithm's previously generated output block as the algorithm's next input block (i.e., by "feeding back" the output block) and combining (exclusive OR-ing) the output block with the next plaintext segment (of block length or less) to form the next ciphertext segment.

Outside attack: See: secondary definition under "attack". Compare: outsider.)

Outsider: A user (usually a person) that accesses a system from a position that is outside the system's security perimeter. (Compare: authorized user, insider, unauthorized user.)

Tutorial: The actions performed by an outsider in accessing the system may be either authorized or unauthorized; i.e., an outsider may act either as an authorized user or as an unauthorized user.

Over-the-air rekeying (OTAR): Changing a key in a remote cryptographic device by sending a new key directly to the device via a channel that the device is protecting.

Overload: (threat action) See: secondary definition under "obstruction".

P1363: See: IEEE P1363.

PAA: See: policy approving authority.

Package: (Common Criteria) A reusable set of either functional or assurance components, combined in a single unit to satisfy a set of identified security objectives. (Compare: protection profile.)

Example: The seven EALs defined in Part 3 of the Common Criteria are predefined assurance packages.

Tutorial: A package is a combination of security requirement components and is intended to be reusable in the construction of either more complex packages or protection profiles and security targets. A package expresses a set of either functional or assurance requirements that meet some particular need, expressed as a set of security objectives.

Packet: A block of data that is carried from a source to a destination through a communication channel or, more generally, across a network. (Compare: datagram, PDU.)

Packet filter: See: secondary definition under "filtering router".

Packet monkey: (slang) Someone who floods a system with packets, creating a denial-of-service condition for the system's users. (See: cracker.)

Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term. (See: Deprecated Usage under "Green Book".)

Pagejacking: (slang) A contraction of "Web page hijacking". A masquerade attack in which the attacker copies (steals) a home page or other material from the target server, re-hosts the page on a server the attacker controls, and causes the re-hosted page to be indexed by the major Web search services, thereby diverting browsers from the target server to the attacker's server.

Deprecated Term: DOCUMENTS SHOULD NOT use this contraction. The term is not listed in most dictionaries and could confuse international readers. (See: Deprecated Usage under "Green Book".)

PAN: See: primary account number.

PAP: See: Password Authentication Protocol.

Parity bit: A checksum that is computed on a block of bits by computing the binary sum of the individual bits in the block and then discarding all but the low-order bit of the sum. (See: checksum.)

Partitioned security mode: A mode of system operation wherein all users having access to the system have the necessary security clearances for all data handled by the system, but some users might not have either formal access approval or need-to-know for all the data. (See: (system operation) under "mode", formal access approval, need to know, protection level, security clearance.)

Usage: Usually abbreviated as "partitioned mode". This term was defined in U.S. Government policy on system accreditation.

PASS: See: personnel authentication system string.

Passive attack: See: secondary definition under "attack".

Passive user: See: secondary definition under "system user".

Passive wiretapping: A wiretapping attack that attempts only to observe a communication flow and gain knowledge of the data it contains, but does not alter or otherwise affect that flow. (See: wiretapping. Compare: passive attack, active wiretapping.)

Password:

a. A secret data value, usually a character string, that is presented to a system by a user to authenticate the user's identity. (See: authentication information, challenge-response, PIN, simple authentication.)

b. "A character string used to authenticate an identity."

c. "A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization."

d. "A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings."

Tutorial: A password is usually paired with a user identifier that is explicit in the authentication process, although in some cases the identifier may be implicit. A password is usually verified by matching it to a stored value held by the access control system for that identifier. Using a password as authentication information is based on assuming that the password is known only by the system entity for

which the identity is being authenticated. Therefore, in a network environment where wiretapping is possible, simple authentication that relies on transmission of static (i.e., repetitively used) passwords in clear-text form is inadequate. (See: one-time password, strong authentication.)

Password Authentication Protocol (PAP): A simple authentication mechanism in PPP. In PAP, a user identifier and password are transmitted in clear-text form.(See: CHAP.)

Password sniffing: (slang) Passive wiretapping to gain knowledge of passwords. (See: Deprecated Usage under "sniffing".)

Path discovery: For a digital certificate, the process of finding a set of public-key certificates that comprise a certification path from a trusted key to that specific certificate.

Path validation: The process of validating (a) all of the digital certificates in a certification path and (b) the required relationships between those certificates, thus validating the contents of the last certificate on the path. (See: certificate validation.)

Tutorial: To promote interoperable PKI applications in the Internet, specifies a detailed algorithm for validation of a certification path.

Payment card: (SET) Collectively refers "to credit cards, debit cards, charge cards, and bank cards issued by a financial institution and which reflects a relationship between the cardholder and the financial institution."

Payment gateway: (SET) A system operated by an acquirer, or a third party designated by an acquirer, to provide electronic commerce services to the merchants in support of the acquirer, and which interfaces to the acquirer to support the authorization, capture, and processing of merchant payment messages, including payment instructions from cardholders.

Payment gateway certification authority (SET PCA): (SET) A CA that issues digital certificates to payment gateways and is operated on behalf of a payment card brand, an acquirer, or another party according to brand rules. A SET PCA issues a CRL for compromised payment gateway certificates. (See: PCA.)

PC card: A type of credit card-sized, plug-in peripheral device that was originally developed to provide memory expansion for portable computers, but is also used for other kinds of functional expansion. (See: FORTEZZA, PCMCIA.)

Tutorial: The international PC Card Standard defines a nonproprietary form factor in three sizes -- Types I, II, and III -- each of which have a 68-pin interface between the card and the socket into which it plugs. All three types have the same length and width, roughly the size of a credit card, but differ in their thickness from 3.3 to 10.5 mm. Examples include storage modules, modems, device interface adapters, and cryptographic modules.

PCA: Abbreviation of various kinds of "certification authority". (See: Internet policy certification authority, (MISSI) policy creation authority, (SET) payment gateway certification authority.) Deprecated Usage: An DOCUMENT that uses this abbreviation SHOULD define it at the point of first use.

PCI: See: "protocol control information" under "protocol data unit".

PCMCIA: Personal Computer Memory Card International Association, a group of manufacturers, developers, and vendors, founded in 1989 to standardize plug-in peripheral memory cards for personal computers and now extended to deal with any technology that works in the PC Card form factor. (See: PC card.)

PDS: See: protective distribution system.

PDU: See: protocol data unit.

Peer entity authentication: "The corroboration that a peer entity in an association is the one claimed." (See: authentication.)

Peer entity authentication service: A security service that verifies an identity claimed by or for a system entity in an association. (See: authentication, authentication service.)

Tutorial: This service is used at the establishment of, or at times during, an association to confirm the identity of one entity to another, thus protecting against a masquerade by the first entity. However, unlike data origin authentication service, this service requires an association to exist between the two entities, and the corroboration provided by the service is valid only at the current time that the service is provided. (See: "relationship between data integrity service and authentication services" under "data integrity service").

PEM: See: Privacy Enhanced Mail.

Penetrate:

a. Circumvent a system's security protections. (See: attack, break, violation.)

b. Successfully and repeatedly gain unauthorized access to a protected system resource.

Penetration: (threat action) See: secondary definition under "intrusion".

Penetration test: A system test, often part of system certification, in which evaluators attempt to circumvent the security features of a system (See: tiger team.)

Tutorial: Penetration testing evaluates the relative vulnerability of a system to attacks and identifies methods of gaining access to a system by using tools and techniques that are available to adversaries. Testing may be performed under various constraints and conditions, including a specified level of knowledge of the system design and implementation. For a TCSEC evaluation, testers are assumed to have all system design and implementation documentation, including

source code, manuals, and circuit diagrams, and to work under no greater constraints than those applied to ordinary users.

Perfect forward secrecy: For a key agreement protocol, the property that compromises long-term keying material does not compromise session keys that were previously derived from the long-term material. (Compare: public-key forward secrecy.)

Usage: Some existing RFCs use this term but either do not define it or do not define it precisely. While preparing this Glossary, we found this to be a muddled area. Experts did not agree. For all practical purposes, the literature defines "perfect forward secrecy" by stating the Diffie-Hellman-Merkle algorithm. The term "public-key forward secrecy" and the definition stated for it in this Glossary were crafted to be compatible with current Internet documents, yet be narrow and leave room for improved terminology. Challenge to the Internet security community: We need a taxonomy of terms and definitions to cover the basic properties discussed here for the full range of cryptographic algorithms and protocols used in Internet Standards: Involvement of session keys vs. long-term keys: Experts disagree about the basic ideas involved:

- One concept of "forward secrecy" is that, given observations of the operation of a key establishment protocol up to time t, and given some of the session keys derived from those protocol runs, you cannot derive unknown past session keys or future session keys.
- A related property is that, given observations of the protocol and knowledge of the derived session keys, you cannot derive one or more of the long-term private keys.

  The "I" definition presented above involves a third concept of "forward secrecy" that refers to the effect of the compromise of long-term keys.
- All three concepts involve the idea that a compromise of "this" encryption key is not supposed to compromise the "next" one. There also is the idea that compromise of a single key will compromise only the data protected by the single key. In Internet literature, the focus has been on protection against decryption of back traffic in the event of a compromise of secret key material held by one or both parties to a communication. Forward vs. backward: Experts are unhappy with the word "forward", because compromise of "this" encryption key also is not supposed to compromise the "previous" one, which is "backward" rather than forward. In S/KEY, if the key used at time t is compromised, then all keys used prior to that are compromised. If the "long-term" key (i.e., the base of the hashing scheme) is compromised, then all keys past and future are compromised; thus, you could say that S/KEY has neither forward nor backward secrecy. Asymmetric cryptography vs. symmetric: Experts disagree about forward secrecy in the context of symmetric cryptographic systems. In the absence of asymmetric cryptography,

compromise of any longterm key seems to compromise any session key derived from the long-term key. For example, Kerberos isn't forward secret, because compromising a client's password (thus compromising the key shared by the client and the authentication server) compromises future session keys shared by the client and the ticket-granting server. Ordinary forward secrecy vs. "perfect" forward secret: Experts disagree about the difference between these two. Some say there is no difference, and some say that the initial naming was unfortunate and suggest dropping the word "perfect". Some suggest using "forward secrecy" for the case where one long-term private key is compromised, and adding "perfect" for when both private keys (or, when the protocol is multi-party, all private keys) are compromised.

Perimeter: See: security perimeter.

Periods processing: A mode of system operation in which information of different sensitivities is processed at distinctly different times by the same system, with the system being properly purged or sanitized between periods. (See: color change.)

Tutorial: The security mode of operation and maximum classification of data handled by the system is established for an interval of time and then is changed for the following interval of time. A period extends from the secure initialization of the system to the completion of any purging of sensitive data handled by the system during the period.

Permanent storage: Non-volatile media that, once written into, can never be completely erased.

Permission:

1. Synonym for "authorization". (Compare: privilege.)
2. An authorization or set of authorizations to perform security-relevant functions in the context of role-based access control.

   Tutorial: A permission is a positively stated authorization for access that

   (a) can be associated with one or more roles and

   (b) enables a user in a role to access a specified set of system resources by causing a specific set of system actions to be performed on the resources.

Persona certificate: An X.509 certificate issued to a system entity that wishes to use a persona to conceal its true identity when using PEM or other Internet services that depend on PKI support. (See: anonymity.)

Tutorial: PEM designers intended that

(a) a CA issuing persona certificates would explicitly not be vouching for the identity of the system entity to whom the certificate is issued,

(b) such certificates would be issued only by CAs subordinate to a policy CA having a policy stating that purpose (i.e., that would warn relying parties that the "subject" field DN represented only a persona and not a true, vetted user identity), and

(c) the CA would not need to maintain records binding the true identity of the subject to the certificate. However, the PEM designers also intended that a CA issuing persona certificates would establish procedures

(d) to enable "the holder of a PERSONA certificate to request that his certificate be revoked" and

(e) to ensure that it did not issue the same subject DN to multiple users. The latter condition implies that a persona certificate is not an organizational certificate unless the organization has just one member or representative.

Personal identification number (PIN):

1. A character string used as a password to gain access to a system resource. (See: authentication information.)

   Example: A cryptographic token typically requires its user to enter a PIN in order to access information stored in the token and invoke the token's cryptographic functions.

2. An alphanumeric code or password used to authenticate an identity.

   Tutorial: Despite the words "identification" and "number", a PIN seldom serves as a user identifier, and a PIN's characters are not necessarily all numeric. Retail banking applications use 4-digit numeric user PINs, but the FORTEZZA PC card uses 12-character alphanumeric SSO PINs. (See: SSO PIN, user PIN.)

   A better name for this concept would have been "personnel authentication system string" (PASS), in which case, an alphanumeric character string for this purpose would have been called, obviously, a "PASSword".

Personal information: Information about a particular person, especially information of an intimate or critical nature, that could cause harm or pain to that person if disclosed to unauthorized parties. Examples: medical record, arrest record, credit report, academic transcript, training report, job application, credit card number, Social Security number. (See: privacy.)

Personality:

1. Synonym for "principal".
2. (MISS) A set of MISSI X.509 public-key certificates that have the same subject DN, together with their associated private keys and usage specifications, that is stored on a FORTEZZA PC card to support a role played by the card's user.

Tutorial: When a card's user selects a personality to use in a FORTEZZA-aware application, the data determines behavior traits (the personality) of the application. A card's user may have multiple personalities on the card. Each has a "personality label", a user-friendly character string that applications can display to the user for selecting or changing the personality to be used. For example, a military user's card might contain three personalities: GENERAL HALFTRACK, COMMANDER FORT SWAMPY, and NEW YEAR'S EVE PARTY CHAIRMAN. Each personality includes one or more certificates of different types (such as DSA versus RSA), for different purposes (such as digital signature versus encryption), or with different authorizations. personnel authentication system string (PASS) (N) See: Tutorial under "personal identification number".

Personnel security: Procedures to ensure that persons who access a system have proper clearance, authorization, and need-to-know as required by the system's security policy. (See: security architecture.)

PGP(trademark): See: Pretty Good Privacy(trademark).

Phase 1 negotiation

Phase 2 negotiation: (ISAKMP) See: secondary definition under "Internet Security Association and Key Management Protocol".

Phishing: (slang) A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a Web site, in which the perpetrator masquerades as a legitimate business or reputable person. (See: social engineering.) Derivation: Possibly from "phony fishing"; the solicitation usually involves some kind of lure or bait to hook unwary recipients. (Compare: phreaking.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it is not listed in most dictionaries and could confuse international readers. (See: Deprecated Usage under "Green Book".)

Photuris: A UDP-based, key establishment protocol for session keys, designed for use with the IPsec protocols AH and ESP. Superseded by IKE.

Phreaking: A contraction of "telephone breaking". An attack on or penetration of a telephone system or, by extension, any other communication or information system.

Deprecated Term: DOCUMENTS SHOULD NOT use this contraction; it is not listed in most dictionaries and could confuse international readers. (See: Deprecated Usage under "Green Book".)

Physical destruction: (threat action) See: secondary definition under "incapacitation".

Physical security: Tangible means of preventing unauthorized physical access to a system. Examples: Fences, walls, and other barriers; locks, safes, and vaults; dogs and armed guards; sensors and alarm bells. (See: security architecture.)

Piggyback attack: A form of active wiretapping in which the attacker gains access to a system via intervals of inactivity in another user's legitimate communication connection. Sometimes called a "between-the-lines" attack. (See: hijack attack, man-in-the-middle attack.)

Deprecated Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term could confuse international readers.

PIN: See: personal identification number.

Ping of death: A denial-of-service attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of causing the destination system to fail. (See: ping sweep, teardrop.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term; instead, use "ping packet overflow attack" or some other term that is specific with regard to the attack mechanism.

Tutorial: This attack seeks to exploit an implementation vulnerability. The IP specification requires hosts to be prepared to accept datagrams of up to 576 octets, but also permits IP datagrams to be up to 65,535 octets long. If an IP implementation does not properly handle very long IP packets, the ping packet may overflow the input buffer and cause a fatal system error.

Ping sweep: An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities. (See: ping of death. Compare: port scan.)

PKCS: See: Public-Key Cryptography Standards.

PKCS #5: A standard from the PKCS series; defines a method for encrypting an octet string with a secret key derived from a password.

Tutorial: Although the method can be used for arbitrary octet strings, its intended primary application in public-key cryptography is for encrypting private keys when transferring them from one computer system to another, as described in PKCS #8.

PKCS #7: A standard from the PKCS series; defines a syntax for data that may have cryptography applied to it, such as for digital signatures and digital envelopes. (See: CMS.)

PKCS #10: A standard from the PKCS series; defines a syntax for certification requests. (See: certification request.)

Tutorial: A PKCS #10 request contains a DN and a public key, and may contain other attributes, and is signed by the entity making the request. The request is sent to a CA, who converts it to an X.509 public-key certificate (or some other form), and returns it, possibly in PKCS #7 format.

PKCS #11: A standard from the PKCS series; defines CAPI called "Cryptoki" for devices that hold cryptographic information and perform cryptographic functions.

PKI: See: public-key infrastructure.

PKINIT: Abbreviation for "Public Key Cryptography for Initial Authentication in Kerberos" (See: Tutorial under "Kerberos".)

PKIX:

1. A contraction of "Public-Key Infrastructure (X.509)", the name of the IETF working group that is specifying an architecture and set of protocols to provide X.509-based PKI services for the Internet.
2. A collective name for that Internet PKI architecture and associated set of protocols.

   Tutorial: The goal of PKIX is to facilitate the use of X.509 public-key certificates in multiple Internet applications and to promote interoperability between different implementations that use those certificates. The resulting PKI is intended to provide a framework that supports a range of trust and hierarchy environments and a range of usage environments. PKIX specifies

   (a) profiles of the v3 X.509 public-key certificate standards and the v2 X.509 CRL standards for the Internet,

   (b) operational protocols used by relying parties to obtain information such as certificates or certificate status,

   (c) management protocols used by system entities to exchange information needed for proper management of the PKI, and

   (d) information about certificate policies and CPSs, covering the areas of PKI security not directly addressed in the rest of PKIX.

Plain text:

1. (noun) Data that is the input to an encryption process. (See: plaintext. Compare: cipher text, clear text.)
2. (noun) Synonym for "clear-text".

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "clear text". Sometimes plain text that is input to an encryption operation is clear text, but other times plain text is cipher text that was output from a previous encryption operation. (See: super-encryption.)

Plaintext:

1. (noun) Synonym for "plain text".
2. (adjective) Referring to plain text. Usage: Commonly used instead of "plain-text". (Compare: cipher-text, clear-text.)
3. (noun) Synonym for "clear-text".

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "clear-text". Clear-text data is, by definition, not encrypted; but plaintext data that is input to an encryption operation may be clear-text data or may be cipher-text data that was output from a previous encryption operation. (See: super-encryption.)

PLI: See: Private Line Interface.

PMA: See: policy management authority.

Point-to-Point Protocol (PPP): An Internet Standard protocol for encapsulation and full-duplex transportation of protocol data packets in OSI-RM Layer 3 over an OSI-RM Layer 2 link between two peers, and for multiplexing different Layer 3 protocols over the same link. Includes optional negotiation to select and use a peer entity authentication protocol to authenticate the peers to each other before they exchange Layer 3 data. (See: CHAP, EAP, PAP.)

Point-to-Point Tunneling Protocol (PPTP): An Internet client-server protocol (originally developed by Ascend and Microsoft) that enables a dial-up user to create a virtual extension of the dial-up link across a network by tunneling PPP over IP. (See: L2TP.)

Tutorial: PPP can encapsulate any IPS Network Interface Layer protocol or OSI-RM Layer 3 protocol. Therefore, PPTP does not specify security services; it depends on protocols above and below it to provide any needed security. PPTP makes it possible to divorce the location of the initial dial-up server (i.e., the PPTP Access Concentrator, the client, which runs on a special-purpose host) from the location at which the dial-up protocol (PPP) connection is terminated and access to the network is provided (i.e., at the PPTP Network Server, which runs on a general-purpose host).

Policy:

a. A plan or course of action that is stated for a system or organization and is intended to affect and direct the decisions and deeds of that entity's components or members. (See: security policy.)

b. A definite goal, course, or method of action to guide and determine present and future decisions, that is implemented or executed within a particular context, such as within a business unit.

Deprecated Abbreviation: DOCUMENTS SHOULD NOT use "policy" as an abbreviation of either "security policy" or "certificate policy". Instead, to avoid misunderstanding, use a fully qualified term, at least at the point of first usage.

Tutorial: The introduction of new technology to replace traditional systems can result in new systems being deployed without adequate policy definition and before the implications of the new technology are fully understand. In some cases, it can be difficult to establish policies for new technology before the technology has been operationally tested and evaluated. Thus, policy changes tend to lag behind technological changes, such that either old policies impede the technical innovation, or the new technology is deployed without adequate policies to govern its use. When new technology changes the ways that things are done, new "procedures" must be defined to establish operational guidelines for using the technology and achieving satisfactory results, and new "practices" must be established for managing new systems and monitoring results. Practices and procedures are more directly coupled to actual systems and business operations than are polices, which tend to be more abstract.

- "Practices" define how a system is to be managed and what controls are in place to monitor the system and detect abnormal behavior or quality problems. Practices are established to ensure that a system is managed in compliance with stated policies. System audits are primarily concerned with whether or not practices are being followed. Auditors evaluate the controls to make sure they conform to accepted industry standards, and then confirm that controls are in place and that control measurements are being gathered. Audit trails are examples of control measurements that are recorded as part of system operations.
- "Procedures" define how a system is operated, and relate closely to issues of what technology is used, who the operators are, and how the system is deployed physically. Procedures define both normal and abnormal operating circumstances.
- For every control defined by a practice statement, there should be corresponding procedures to implement the control and provide ongoing measurement of the control parameters.

Conversely, procedures require management practices to insure consistent and correct operational behavior.

Policy approval authority: (PKI) Synonym for "policy management authority". Deprecated Term: DOCUMENTS SHOULD NOT use this term as synonym for "policy management authority". The term suggests a limited, passive role that is not typical of PMAs.

Policy approving authority (PAA): (MISSI) The top-level signing authority of a MISSI certification hierarchy. The term refers both to that authoritative office or role and

to the person who plays that role. (See: policy management authority, root registry.)

Tutorial: A MISSI PAA

(a) registers MISSI PCAs and signs their X.509 public-key certificates,

(b) issues CRLs but does not issue a CKL, and

(c) may issue cross-certificates to other PAAs.

Policy authority: (PKI) Synonym for "policy management authority".

Deprecated Term: DOCUMENTS SHOULD NOT use this term as synonym for "policy management authority". The term is unnecessarily vague and thus may be confused with other PKI entities, such as CAs and RAs, that enforce of apply various aspects of PKI policy.

Policy certification authority (Internet PCA): An X.509-compliant CA at the second level of the Internet certification hierarchy, under the IPRA. Each PCA operates under its published security policy (see: certificate policy, CPS) and within constraints established by the IPRA for all PCAs.(See: policy creation authority.)

Policy creation authority (MISSI PCA): (MISSI) The second level of a MISSI certification hierarchy; the administrative root of a security policy domain of MISSI users and other, subsidiary authorities. The term refers both to that authoritative office or role and to the person who fills that office. (See: policy certification authority.)

Tutorial: A MISSI PCA's certificate is issued by a PAA. The PCA registers the CAs in its domain, defines their configurations, and issues their X.509 public-key certificates. (The PCA may also issue certificates for SCAs, ORAs, and other end entities, but a PCA does not usually do this.) The PCA periodically issues CRLs and CKLs for its domain.

Policy management authority (PMA): (PKI) A person, role, or organization within a PKI that is responsible for

(a) creating or approving the content of the certificate policies and CPSs that are used in the PKI;

(b) ensuring the administration of those policies; and

(c) approving any cross-certification or interoperability agreements with CAs external to the PKI and any related policy mappings. The PMA may also be the accreditor for the PKI as a whole or for some of its components or applications. (See: policy approving authority.)

Example: In the U.S. Department of Defense, an organization called the Policy Management Authority is responsible for DoD PKI.

Policy mapping: "Recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain."

Policy rule: A building block of a security policy;

(a) defines a set of system conditions and

(b) specifies a set of system actions that are to be performed if those conditions occur.

POP3: See: Post Office Protocol, version 3.

POP3 APOP: A POP3 command (better described as a transaction type, or Sub-protocol by which a POP3 client optionally uses a keyed hash (based on MD5) to authenticate itself to a POP3 server and, depending on the server implementation, to protect against replay attacks. (See: CRAM, POP3 AUTH, IMAP4 AUTHENTICATE.)

Tutorial: The server includes a unique time stamp in its greeting to the client. The subsequent APOP command sent by the client to the server contains the client's name and the hash result of applying MD5 to a string formed from both the time stamp and a shared secret value that is known only to the client and the server. APOP was designed to provide an alternative to using POP3's USER and PASS (i.e., password) command pair, in which the client sends a clear-text password to the server.

POP3 AUTH: A POP3 command (better described as a transaction type, or sub-protocol) by which a POP3 client optionally proposes a mechanism to a POP3 server to authenticate the client to the server and provide other security services. (See: POP3 APOP, IMAP4 AUTHENTICATE.)

Tutorial: If the server accepts the proposal, the command is followed by performing a challenge-response authentication protocol and, optionally, negotiating a protection mechanism for subsequent POP3 interactions. The security mechanisms used by POP3 AUTH are those used by IMAP4.

Port scan: A technique that sends client requests to a range of service-port addresses on a host. (See: probe. Compare: ping sweep.)

Tutorial: A port scan can be used for pre-attack surveillance, with the goal of finding an active port and subsequently exploiting a known vulnerability of that port's service. A port scan can also be used as a flooding attack.

Positive authorization: The principle that a security architecture should be designed so that access to system resources is permitted only when explicitly granted; i.e., in the absence of an explicit authorization that grants access, the default action shall be to refuse access. (See: authorization, access.)

POSIX: Portable Operating System Interface for Computer Environments, a standard (originally IEEE Standard P1003.1) that defines an operating system interface and environment to support application portability at the source code level. It is intended to be used by both application developers and system implementers.

Tutorial: P1003.1 supports security functionality like that on most UNIX systems, including discretionary access control and privileges. IEEE Draft Standard P1003.6 specifies additional functionality not provided in the base standard, including (a) discretionary access control, (b) audit trail mechanisms, (c) privilege mechanisms, (d) mandatory access control, and (e) information label mechanisms.

Post Office Protocol, version 3 (POP3): An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client. (See: IMAP4.)

Tutorial: POP3 has mechanisms for optionally authenticating a client to a server and providing other security services. (See: POP3 APOP, POP3 AUTH.)

PPP: See: Point-to-Point Protocol

PPTP: See: Point-to-Point Tunneling Protocol.

Preauthorization: (PKI A CAW feature that enables certification requests to be automatically validated against data provided in advance to the CA by an authorizing entity.

Precedence:

1. (information system) A ranking assigned to events or data objects that determines the relative order in which they are processed.
2. (communication system) A designation assigned to a communication (i.e., packet, message, data stream, connection, etc.) by the originator to state the importance or urgency of that communication versus other communications, and thus indicate to the transmission system the relative order of handling, and indicate to the receiver the order in which the communication is to be noted. (See: availability, critical, preemption.)

Preemption: The seizure, usually automatic, of system resources that are being used to serve a lower-precedence communication, in order to serve immediately a higher-precedence communication.

Pretty Good Privacy(trademark) (PGP(trademark)): Trademarks of Network Associates, Inc., referring to a computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet. (Compare: DKIM, MOSS, MSP, PEM, S(MIME.) Tutorial: PGP encrypts messages with a symmetric algorithm (originally, IDEA in CFB mode), distributes the symmetric keys by encrypting them with an asymmetric algorithm

(originally, RSA), and creates digital signatures on messages with a cryptographic hash and an asymmetric encryption algorithm (originally, MD5 and RSA). To establish ownership of public keys, PGP depends on the "web of trust".

Prevention: See: secondary definition under "security".

Primary account number (PAN): (SET) "The assigned number that identifies the card issuer and cardholder. This account number is composed of an issuer identification number, an individual account number identification, and an accompanying check digit as defined by ISO 7812-1985." (See: bank identification number.)

Tutorial: The PAN is embossed, encoded, or both on a magnetic strip-based credit card. The PAN identifies the issuer to which a transaction is to be routed and the account to which it is to be applied unless specific instructions indicate otherwise. The authority that assigns the BIN part of the PAN is the American Bankers Association.

Principal: A specific identity claimed by a user when accessing a system. Usage: Usually understood to be an identity that is registered in and authenticated by the system; equivalent to the notion of login account identifier. Each principal is normally assigned to a single user, but a single user may be assigned (or attempt to use) more than one principal. Each principal can spawn one or more subjects, but each subject is associated with only one principal. (Compare: role, subject, user.) (I) (Kerberos) A uniquely identified (i.e., uniquely named) client or server instance that participates in a network communication.

Priority: (information system) Precedence for processing an event or data object, determined by security importance or other factors. (See: precedence.)

Privacy:

1. The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. (See: HIPAA, personal information, Privacy Act of 1974. Compare: anonymity, data confidentiality.)
2. "The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed."
3. Synonym for "data confidentiality".

   Deprecated Definition: DOCUMENTS SHOULD NOT use this term as a synonym for "data confidentiality" or "data confidentiality service", which are different concepts. Privacy is a reason for security rather than a kind of security. For example, a system that stores personal data needs to protect the data to prevent

harm, embarrassment, inconvenience, or unfairness to any person about whom data is maintained, and to protect the person's privacy. For that reason, the system may need to provide data confidentiality service.

Tutorial: The term "privacy" is used for various separate but related concepts, including bodily privacy, territorial privacy, personal information privacy, and communication privacy. DOCUMENTS are expected to address only communication privacy, which in this Glossary is defined primarily by "data confidentiality" and secondarily by "data integrity".

DOCUMENTS are not expected to address information privacy, but this Glossary provides definition 1 for that concept because personal information privacy is often confused with communication privacy. DOCUMENTS are not expected to address bodily privacy or territorial privacy, and this Glossary does not define those concepts because they are not easily confused with communication privacy.

Privacy Act of 1974: A U.S. Federal law that seeks to balance the U.S. Government's need to maintain data about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal data. (See: privacy.)

Tutorial: In 1974, the U.S. Congress was concerned with the potential for abuses that could arise from the Government's increasing use of computers to store and retrieve personal data. Therefore, the Act has four basic policy objectives:

- To restrict disclosure of personally identifiable records maintained by Federal agencies.
- To grant individuals increased rights of access to Federal agency records maintained on themselves.
- To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
- To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records

Privacy Enhanced Mail (PEM): An Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail. (Compare: DKIM, MOSS, MSP, PGP, S(MIME.)

Tutorial: PEM encrypts messages with a symmetric algorithm (originally, DES in CBC mode), provides distribution for the symmetric keys by encrypting them with an asymmetric algorithm (originally, RSA), and signs messages with an

asymmetric encryption algorithm over a cryptographic hash (originally, RSA over either MD2 or MD5). To establish ownership of public keys, PEM uses a certification hierarchy, with X.509 public-key certificates and X.509 CRLs that are signed with an asymmetric encryption algorithm over a cryptographic hash (originally, RSA over MD2). PEM is designed to be compatible with a wide range of key management methods, but is limited to specifying security services only for text messages and, like MOSS, has not been widely implemented in the Internet.

Private component: Synonym for "private key".

Deprecated Usage: In most cases, DOCUMENTS SHOULD NOT use this term; instead, to avoid confusing readers, use "private key". However, the term MAY be used when discussing a key pair; e.g., "A key pair has a public component and a private component."

Private extension: See: secondary definition under "extension".

Private key:

1. The secret component of a pair of cryptographic keys used for asymmetric cryptography. (See: key pair, public key, secret key.)
2. In a public key cryptosystem, "that key of a user's key pair which is known only by that user."

Private Line Interface (PLI): The first end-to-end packet encryption system for a computer network, developed by BBN starting in 1975 for the U.S. DoD, incorporating U.S. Government-furnished, military-grade COMSEC Equipment (TSEC(KG-34). (Compare: IPLI.)

Privilege:

1. (access control) A synonym for "authorization". (See authorization. Compare: permission.)
2. (computer platform) An authorization to perform a security-relevant function in the context of a computer's **operating system.**

Privilege management infrastructure: "The infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a" PKI; i.e., processes concerned with attribute certificates.

Privileged process: A computer process that is authorized (and, therefore, trusted) to perform some security-relevant functions that ordinary processes are not. (See: privilege, trusted process.)

Privileged user: An user that has access to system control, monitoring, or administration functions. (See: privilege, (UNIX) under "root", superuser, user.)

Tutorial: Privileged users include the following types:

- Users with near or complete control of a system, who are authorized to set up and administer user accounts, identifiers, and authentication information, or are authorized to assign or change other users' access to system resources.
- Users that are authorized to change control parameters (e.g., network addresses, routing tables, processing priorities) on routers, multiplexers, and other important equipment.
- Users that are authorized to monitor or perform troubleshooting for a system's security functions, typically using special tools and features that are not available to ordinary users.

Probe: (verb) A technique that attempts to access a system to learn something about the system. (See: port scan.)

Tutorial: The purpose of a probe may be offensive, e.g., an attempt to gather information for circumventing the system's protections; or the purpose may be defensive, e.g., to verify that the system is working properly.

Procedural security: Synonym for "administrative security".

Deprecated Term: DOCUMENTS SHOULD NOT use this term as a synonym for "administrative security". The term may be misleading because any type of security may involve procedures, and procedures may be either external to the system or internal. Instead, use "administrative security", "communication security", "computer security", "emanations security", "personnel security", "physical security", or whatever specific type is meant. (See: security architecture.)

Profile: See: certificate profile, protection profile.

Proof-of-possession protocol: A protocol whereby a system entity proves to another that it possesses and controls a cryptographic key or other secret information. (See: zero-knowledge proof.)

Proprietary: Refers to information (or other property) that is owned by an individual or organization and for which the use is restricted by that entity.

Protected checksum: A checksum that is computed for a data object by means that protect against active attacks that would attempt to change the checksum to make it match changes made to the data object. (See: digital signature, keyed hash, Tutorial under "checksum".)

Protective packaging: "Packaging techniques for COMSEC material that discourage penetration, reveal a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use." (See: tamper-evident, tamper-resistant. Compare: QUADRANT.)

Protection authority: See: secondary definition under "Internet Protocol Security Option".

Protection level: (U.S. Government) An indication of the trust that is needed in a system's technical ability to enforce security policy for confidentiality. (Compare) system operation under "mode of operation".

Tutorial: An organization's security policy could define protection levels that are based on comparing

(a) the sensitivity of information handled by a system to

(b) the authorizations of users that receive information from the system without manual intervention and reliable human review. For each level, the policy could specify security features and assurances that must be included in any system that was intended to operate at that level.

Protection profile: (Common Criteria) An implementation-independent set of security requirements for a category of targets of evaluation that meet specific consumer needs Example: (See: target of evaluation. Compare: certificate profile, package.)

Tutorial: A protection profile (PP) is the kind of document used by consumers to specify functional requirements they want in a product, and a security target (ST) is the kind of document used by vendors to make functional claims about a product. A PP is intended to be a reusable statement of product security needs, which are known to be useful and effective, for a set of information technology security products that could be built. A PP contains a set of security requirements, preferably taken from the catalogs in Parts 2 and 3 of the Common Criteria, and should include an EAL.

Protection ring: One of a hierarchy of privileged operation modes of a system that gives certain access rights to processes authorized to operate in that mode. (See: Multics.)

Protective distribution system (PDS): A wireline or fiber-optic communication system used to transmit clear-text classified information through an area of lesser classification or control protocol

1. A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. Example: Internet Protocol.

2. A series of ordered computing and communication steps that are performed by two or more system entities to achieve a joint objective

Protocol control information (PCI): See: secondary definition under "protocol data unit".

Protocol data unit: (PDU) A data packet that is defined for peer-to-peer transfers in a protocol layer.

Tutorial: A PDU consists of two disjoint subsets of data: the SDU and the PCI. (Although these terms -- PDU, SDU, and PCI --originated in the OSI-RM, they are also useful and permissible in an IPS context.)

- The "service data unit" (SDU) in a packet is data that the protocol transfers between peer protocol entities on behalf of the users of that layer's services. For Layers 1 through 6, the layer's users are peer protocol entities at a higher layer; for Layer 7, the users are application entities outside the scope of the OSI-RM.
- The "protocol control information" (PCI) in a packet is data that peer protocol entities exchange between themselves to control their joint operation of the layer.

Protocol suite: A complementary collection of communication protocols used in a computer network. (See: IPS, OSI.)

Proxy:

1. A computer process that acts on behalf of a user or client.
2. A computer process -- often used as, or as part of, a firewall -- that relays application transactions or a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. (See: SOCKS.)

   Tutorial: In a firewall, a proxy server usually runs on a bastion host, which may support proxies for several applications and protocols (e.g., FTP, HTTP, and TELNET). Instead of a client in the protected enclave connecting directly to an external server, the internal client connects to the proxy server, which in turn connects to the external server. The proxy server waits for a request from inside the firewall, forwards the request to the server outside the firewall, gets the response, then sends the response back to the client. The proxy may be transparent to the clients, or they may need to connect first to the proxy server, and then use that association to also initiate a connection to the real server.

   Proxies are generally preferred over SOCKS for their ability to perform caching, high-level logging, and access control. A proxy can provide security service beyond that which is normally part of the relayed protocol, such as access control based on peer entity authentication of clients, or peer entity authentication of servers when clients do not have that ability. A proxy at OSI-RM Layer 7 can also provide finer-grained security service than can a filtering router at Layer 3. For example, an FTP proxy could permit transfers out of, but not into, a protected network.

Proxy certificate: An X.509 public-key certificate derived from an end-entity certificate, or from another proxy certificate, for the purpose of establishing proxies and delegating authorizations in the context of a PKI-based authentication system

Tutorial: A proxy certificate has the following properties:

- It contains a critical extension that (a) identifies it as a proxy certificate and (b) may contain a certification path length constraint and policy constraints.
- It contains the public component of a key pair that is distinct from that associated with any other certificate.
- It is signed by the private component of a key pair that is associated with an end-entity certificate or another proxy certificate.
- Its associated private key can be used to sign only other proxy certificates (not end-entity certificates).
- Its "subject" DN is derived from its "issuer" DN and is unique.
- Its "issuer" DN is the "subject" DN of an end-entity certificate or another proxy certificate.

Pseudorandom: A sequence of values that appears to be random (i.e., unpredictable) but is actually generated by a deterministic algorithm. (See: compression, random, random number generator.)

Pseudorandom number generator: See: secondary definition under "random number generator".

Public component: Synonym for "public key".

Deprecated Usage: In most cases, DOCUMENTS SHOULD NOT use this term; to avoid confusing readers, use "private key" instead. However, the term MAY be used when discussing a key pair; e.g., "A key pair has a public component and a private component."

Public key:

1. The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography. (See: key pair. Compare: private key.)

2. In a public key cryptosystem, "that key of a user's key pair which is publicly known."

Public-key certificate:

1. A digital certificate that binds a system entity's identifier to a public key value, and possibly to additional, secondary data items; i.e., a digitally signed data structure that attests to the ownership of a public key. (See: X.509 public-key certificate.)

2. "The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it."

Tutorial: The digital signature on a public-key certificate is unforgeable. Thus, the certificate can be published, such as by posting it in a directory, without the directory having to protect the certificate's data integrity.

Public-key cryptography: Synonym for "asymmetric cryptography".

Public-Key Cryptography Standards (PKCS): A series of specifications published by RSA Laboratories for data structures and algorithms used in basic applications of asymmetric cryptography. (See: PKCS #5 through PKCS #11.)

Tutorial: The PKCS were begun in 1991 in cooperation with industry and academia, originally including Apple, Digital, Lotus, Microsoft, Northern Telecom, Sun, and MIT. Today, the specifications are widely used, but they are not sanctioned by an official standards organization, such as ANSI, ITU-T, or IETF. RSA Laboratories retains sole decision-making authority over the PKCS.

Public-key forward secrecy (PFS): For a key-agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future. (See: Usage note and other discussion under "perfect forward secrecy".)

Public-key Kerberos: See: Tutorial under "Kerberos", PKINIT.

Public-key infrastructure (PKI):

1. A system of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography. (See: hierarchical PKI, mesh PKI, security management infrastructure, trust-file PKI.)
2. (PKIX) The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

   Tutorial: The core PKI functions are

   (a) to register users and issue their public-key certificates,

   (b) to revoke certificates when required, and

   (c) to archive data needed to validate certificates at a much later time.

   Key pairs for data confidentiality may be generated (and perhaps escrowed) by CAs or RAs, but requiring a PKI client to generate its own digital signature key pair helps maintain system integrity of the cryptographic system, because then only the client ever possesses the private key it uses. Also, an authority may be established to approve or coordinate CPSs, which are security policies under which components of a PKI operate. A number of other servers and agents may

support the core PKI, and PKI clients may obtain services from them, such as certificate validation services. The full range of such services is not yet fully understood and is evolving, but supporting roles may include archive agent, certified delivery agent, confirmation agent, digital notary, directory, key escrow agent, key generation agent, naming agent who ensures that issuers and subjects have unique identifiers within the PKI, repository, ticket-granting agent, time-stamp agent, and validation agent.

Purge:

1. Synonym for "erase".

2. (U.S. Government) Use degaussing or other methods to render magnetically stored data unusable and irrecoverable by any means, including laboratory methods. (Compare: (U.S. Government) erase.)

QUADRANT: (U.S. Government) Short name for technology and methods that protect cryptographic equipment by making the equipment tamper-resistant.

Tutorial: Equipment cannot be made completely tamper-proof, but it can be made tamper-resistant or tamper-evident.

Qualified certificate: A public-key certificate that has the primary purpose of identifying a person with a high level of assurance, where the certificate meets some qualification requirements defined by an applicable legal framework, such as the European Directive on Electronic Signature.

Quick mode: See: (IKE) under "mode".

RA: See: registration authority.

RA domains: A feature of a CAW that allows a CA to divide the responsibility for certificate requests among multiple RAs.

Tutorial: This ability might be used to restrict access to private authorization data that is provided with a certificate request, and to distribute the responsibility to review and approve certificate requests in high-volume environments. RA domains might segregate certificate requests according to an attribute of the Certificate's subject, such as an organizational unit.

RADIUS: See: Remote Authentication Dial-In User Service.

Rainbow Series: (COMPUSEC) A set of more than 30 technical and policy documents with colored covers, issued by the NCSC, that discuss in detail the TCSEC and provide guidance for meeting and applying the criteria. (See: Green Book, Orange Book, Red Book, Yellow Book.)

Random: In essence, "random" means "unpredictable". (See: cryptographic key, pseudorandom.)

- **"Random sequence":** A sequence in which each successive value is obtained merely by chance and does not depend on the preceding values of the sequence. In a random sequence of bits, each bit is unpredictable; i.e., (a) the probability of each bit being a "0" or "1" is 1(2, and (b) the value of each bit is independent of any other bit in the sequence.
- **"Random value":** An individual value that is unpredictable; i.e., each value in the total population of possibilities has equal probability of being selected.

Random number generator: A process that is invoked to generate a random sequence of values (usually a sequence of bits) or an individual random value.

Tutorial: There are two basic types of generators.

- "(True) random number generator": It uses one or more non-deterministic bit sources (e.g., electrical circuit noise, timing of human processes such as key strokes or mouse movements, semiconductor quantum effects, and other physical phenomena) and a processing function that formats the bits, and it outputs a sequence of values that is unpredictable and uniformly distributed.
- "Pseudorandom number generator": It uses a deterministic computational process (usually implemented by software) that has one or more inputs called "seeds", and it outputs a sequence of values that appears to be random according to specified statistical tests.

RBAC: See: role-based access control, rule-based access control.

Deprecated Usage: DOCUMENTS that use this term SHOULD state a definition for it because the abbreviation is ambiguous.

RC2, RC4, RC6 See: Rivest Cipher #2, #4, #6.

Read: (security model) A system operation that causes a flow of information from an object to a subject. (See: access mode. Compare: write.)

Realm: (Kerberos) A domain consisting of a set of Kerberized clients, Kerberized application servers, and one or more Kerberos authentication servers and ticket-granting servers that support the clients and applications, all operating under the same security policy. (See: domain.)

Recovery:

1. (cryptography) The process of learning or obtaining cryptographic data or plain text through cryptanalysis. (See: key recovery, data recovery.)
2. (system integrity) The process of restoring a secure state in a system after there has been an accidental failure or a successful attack. (See: secondary definition under "security", system integrity.)
3. (system integrity) The process of restoring an information system’s assets and operation following damage or destruction. (See: contingency plan.)

RED

1. Designation for data that consists only of clear text, and for information system equipment items and facilities that handle clear text. Example: "RED key". (See: BCR, color change, RED (BLACK separation. Compare: BLACK.)
2. Derivation: From the practice of marking equipment with colors to prevent operational errors.
3. (U.S. Government) Designation applied to information systems, and to associated areas, circuits, components, and equipment, "in which unencrypted national security information is being processed."

RED-BLACK separation: An architectural concept for cryptographic systems that strictly separates the parts of a system that handle plain text (i.e., RED information) from the parts that handle cipher text (i.e., BLACK information). (See: BLACK, RED.)

Red Book: (slang) Synonym for "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria".

Deprecated Term: DOCUMENTS SHOULD NOT use this term. Instead, use the full proper name of the document or, in subsequent references, a more conventional abbreviation, e.g., TNI-TCSEC. (See: TCSEC, Rainbow Series, Deprecated Usage under "Green Book".)

RED key: A cleartext key, which is usable in its present form (i.e., it does not need to be decrypted before being used). (See: RED. Compare: BLACK key.)

Reference monitor: "An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects."

Tutorial: This concept was described in the Anderson report. A reference monitor should be

(a) complete (i.e., it mediates every access),

(b) isolated (i.e., it cannot be modified by other system entities), and

(c) verifiable (i.e., small enough to be subjected to analysis and tests to ensure that it is correct).

Reflection attack: An attack in which a valid data transmission is replayed to the originator by an attacker who intercepts the original transmission. (Compare: indirect attack, replay attack.)

reflector attack: Synonym for "indirect attack".

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it could be confused with "reflection attack", which is a different concept.

Registered user: A system entity that is authorized to receive a system's products and services or otherwise access system resources. (See: registration, user.)

Registration:

1. (information system) A system process that

   (a) initializes an identity (of a system entity) in the system,

   (b) establishes an identifier for that identity,

   (c) may associate authentication information with that identifier, and (d) may issue an identifier credential (depending on the type of authentication mechanism being used). (See: authentication information, credential, identifier, identity, identity proofing.)

2. (PKI) An administrative act or process whereby an entity's name and other attributes are established for the first time at a CA, prior to the CA issuing a digital certificate that has the entity's name as the subject. (See: registration authority.)

   Tutorial: Registration may be accomplished either directly, by the CA, or indirectly, by a separate RA. An entity is presented to the CA or RA, and the authority either records the name(s) claimed for the entity or assigns the entity's name(s). The authority also determines and records other attributes of the entity that are to be bound in a certificate (such as a public key or authorizations) or maintained in the authority's database (such as street address and telephone number). The authority is responsible, possibly assisted by an RA, for verifying the entity's identity and vetting the other attributes, in accordance with the CA's CPS. Among the registration issues that a CPS may address are the following:

   - How a claimed identity and other attributes are verified.
   - How organization affiliation or representation is verified.
   - What forms of names are permitted, such as X.500 DN, domain name, or IP address.
   - Whether names are required to be meaningful or unique, and within what domain.
   - How naming disputes are resolved, including the role of trademarks.
   - Whether certificates are issued to entities that are not persons.
   - Whether a person is required to appear before the CA or RA, or can instead be represented by an agent.
   - Whether and how an entity proves possession of the private key matching a public key.

Registration authority (RA)

1. An optional PKI entity (separate from the CAs) that does not sign either digital certificates or CRLs but has responsibility for recording or verifying some or all of the information (particularly the identities of subjects) needed by a CA to issue certificates and CRLs and to perform other certificate management functions. (See: ORA, registration.)

2. (PKIX) An optional PKI component, separate from the CA(s). The functions that the RA performs will vary from case to case but may include identity authentication and name assignment, key generation and archiving of key pairs, token distribution, and **revocation reporting.**

Tutorial: Sometimes, a CA may perform all certificate management functions for all end users for which the CA signs certificates. Other times, such as in a large or geographically dispersed community, it may be necessary or desirable to offload secondary CA functions and delegate them to an assistant, while the CA retains the primary functions (signing certificates and CRLs). The tasks that are delegated to an RA by a CA may include personal authentication, name assignment, token distribution, revocation reporting, key generation, and archiving. An RA is an optional PKI entity, separate from the CA, that is assigned secondary functions. The duties assigned to RAs vary from case to case but may include the following:

- Verifying a subject's identity, i.e., performing personal authentication functions.
- Assigning a name to a subject. (See: distinguished name.)
- Verifying that a subject is entitled to have the attributes requested for a certificate.
- Verifying that a subject possesses the private key that matches the public key requested for a certificate.
- Performing functions beyond mere registration, such as generating key pairs, distributing tokens, handling revocation reports, and archiving data. (Such functions may be assigned to a PKI component that is separate from both the CA and the RA.)

3. (SET) "An independent third-party organization that processes payment card applications for multiple payment card brands and forwards applications to the appropriate financial institutions."

Regrade: Deliberately change the security level (especially the hierarchical classification level) of information in an authorized manner. (See: downgrade, upgrade.)

Rekey: Change the value of a cryptographic key that is being used in an application of a cryptographic system. (See: certificate rekey.)

Tutorial: Rekey is required at the end of a crypto-period or key lifetime.

Reliability: The ability of a system to perform a required function under stated conditions for a specified period of time. (Compare: availability, survivability.)

Reliable human review: Any manual, automated, or hybrid process or procedure that ensures that a human examines a digital object, such as text or an image, to determine whether the object may be permitted, according to some security policy, to be transferred across a controlled interface. (See: guard.)

Relying party: Synonym for "certificate user".

Usage: Used in a legal context to mean a recipient of a certificate who acts in reliance on that certificate. (See: ABA Guidelines.)

Remanence: Residual information that can be recovered from a storage medium after clearing. (See: clear, magnetic remanence, purge.)

Remote Authentication Dial-In User Service (RADIUS): An Internet protocol for carrying dial-in users' authentication information and configuration information between a shared, centralized authentication server (the RADIUS server) and a network access server (the RADIUS client) that needs to authenticate the users of its network access ports. (See: TACACS.) User presents authentication and possibly other information to the RADIUS client (e.g., health information regarding the user device).

Tutorial: A user presents authentication information and possibly other information to the RADIUS client, and the client passes that information to the RADIUS server. The server authenticates the client using a shared secret value and checks the presented information, and then returns to the client all authorization and configuration information needed by the client to serve the user.

Renew: See: certificate renewal.

Reordering: (packet) See: secondary definition under "stream integrity service".

Replay attack: An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it, possibly as part of a masquerade attack. (See: active wiretapping, fresh, liveness, nonce. Compare: indirect attack, reflection attack.)

Repository:

1. A system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users. (Compare: archive, directory.)
2. "A trustworthy system for storing and retrieving certificates or other information relevant to certificates."

Tutorial: A certificate is published to those who might need it by putting it in a repository. The repository usually is a publicly accessible, on-line server. In the FPKI, for example, the expected repository is a directory that uses LDAP, but also may be an X.500 Directory that uses DAP, or an HTTP server, or an FTP server that permits anonymous login.

Repudiation:

1. Denial by a system entity that was involved in an association (especially a communication association that transfers data) of having participated in the relationship. (See: accountability, non-repudiation service.)
2. A type of threat action whereby an entity deceives another by falsely denying responsibility for an act. (See: deception.)
3. (OSI-RM) "Denial by one of the entities involved in a communication of having participated in all or part of the communication."

Request for Comment (RFC):

1. One of the documents in the archival series that is the official channel for DOCUMENTS and other publications of the Internet Engineering Steering Group, the Internet Architecture Board, and the Internet community in general. (See: Internet Standard.)
2. A popularly misused synonym for a document on the Internet Standards Track, i.e., an Internet Standard, Draft Standard, or Proposed Standard. (See: Internet Standard.) Deprecated Definition: DOCUMENTS SHOULD NOT use this term with definition 2 because many other types of documents also are published as RFCs.

Residual risk: The portion of an original risk or set of risks that remains after countermeasures have been applied. (Compare: acceptable risk, risk analysis.)

Restore: See: card restore.

Reverse engineering: (threat action) See: secondary definition under "intrusion".

Revocation: See: certificate revocation.

Revocation date: (X.509) In a CRL entry, a date-time field that states when the certificate revocation occurred, i.e., when the CA declared the digital certificate to be invalid. (See: invalidity date.)

Tutorial: The revocation date may not resolve some disputes because, in the worst case, all signatures made during the validity period of the certificate may have to be considered invalid. However, it may be desirable to treat a digital signature as valid even though the private key used to sign was compromised after the signing. If more is known about when the compromise actually occurred,

a second date-time, an "invalidity date", can be included in an extension of the CRL entry.

Revocation list: See: certificate revocation list.

Revoke: See: certificate revocation.

RFC: See: Request for Comment.

Rijndael: A symmetric, block cipher that was designed by Joan Daemen and Vincent Rijmen as a candidate for the AES, and that won that competition. (See: Advanced Encryption Standard.)

Risk:

1. An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. (See: residual risk.)
2. (SET) "The possibility of loss because of one or more threats to information (not to be confused with financial or business risk)."

   Tutorial: There are four basic ways to deal with a risk :

   - "Risk avoidance": Eliminate the risk by either countering the threat or removing the vulnerability. (Compare: "avoidance" under "security".)
   - "Risk transference": Shift the risk to another system or entity; e.g., buy insurance to compensate for potential loss.
   - "Risk limitation": Limit the risk by implementing controls that minimize resulting loss.
   - "Risk assumption": Accept the potential for loss and continue operating the system.

Risk analysis: An assessment process that systematically

(a) identifies valuable system resources and threats to those resources,

(b) quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and

(c) (optionally) recommends how to allocate available resources to countermeasures so as to minimize total exposure. (See: risk management, business-case analysis. Compare: threat analysis.)

Tutorial: Usually, it is financially and technically infeasible to avoid or transfer all risks (see: "first corollary" of "second law" under "Courtney's laws"), and some residual risks will remain, even after all available countermeasures have been deployed (see: "second corollary" of "second law" under "Courtney's laws"). Thus, a risk analysis typically lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first. In some contexts, it

is infeasible or inadvisable to attempt a complete or quantitative risk analysis because needed data, time, and expertise are not available. Instead, basic answers to questions about threats and risks may be already built into institutional security policies. For example, U.S. DoD policies for data confidentiality "do not explicitly itemize the range of expected threats" but instead "reflect an operational approach ... by stating the particular management controls that must be used to achieve [confidentiality] ... Thus, they avoid listing threats, which would represent a severe risk in itself, and avoid the risk of poor security design implicit in taking a fresh approach to each new problem".

Risk assumption: See: secondary definition under "risk".

Risk avoidance: See: secondary definition under "risk".

Risk limitation: See: secondary definition under "risk".

Risk management:

1. The process of identifying, measuring, and controlling (i.e., mitigating) risks in information systems so as to reduce the risks to a level commensurate with the value of the assets protected. (See: risk analysis.)
2. The process of controlling uncertain events that may affect information system resources.
3. "The total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws."

Risk transference: See: secondary definition under "risk".

Rivest Cipher #2 (RC2): A proprietary, variable-key-length block cipher invented by Ron Rivest for RSA Data Security, Inc.

Rivest Cipher #4 (RC4): A proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc.

Rivest Cipher #6 (RC6): A symmetric, block cipher with 128-bit or longer key length, developed by Ron Rivest for RSA Data Security, Inc. as a candidate for the AES.

Rivest-Shamir-Adleman (RSA): An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Tutorial: RSA uses exponentiation modulo the product of two large prime numbers. The difficulty of breaking RSA is believed to be equivalent to the difficulty of factoring integers that are the product of two large prime numbers of approximately equal size. To create an RSA key pair, randomly choose two large prime numbers, p and q, and compute the modulus, n = pq. Randomly choose a

number e, the public exponent, that is less than n and relatively prime to (p-1)(q-1). Choose another number d, the private exponent, such that ed-1 evenly divides (p-1)(q-1). The public key is the set of numbers (n,e), and the private key is the set (n,d). It is assumed to be difficult to compute the private key (n,d) from the public key (n,e). However, if n can be factored into p and q, then the private key d can be computed easily. Thus, RSA security depends on the assumption that it is computationally difficult to factor a number that is the product of two large prime numbers. (Of course, p and q are treated as part of the private key, or else are destroyed after computing n.)

For encryption of a message, m, to be sent to Bob, Alice uses Bob's public key (n,e) to compute m**e (mod n) = c. She sends c to Bob. Bob computes c**d (mod n) = m. Only Bob knows d, so only Bob can compute c**d (mod n) to recover m.

To provide data origin authentication of a message, m, to be sent to Bob, Alice computes m**d (mod n) = s, where (d,n) is Alice's private key. She sends m and s to Bob. To recover the message that only Alice could have sent, Bob computes s**e (mod n) = m, where (e,n) is Alice's public key. To ensure data integrity in addition to data origin authentication requires extra computation steps in which Alice and Bob use a cryptographic hash function h (see: digital signature). Alice computes the hash value h(m) = v, and then encrypts v with her private key to get s. She sends m and s. Bob receives m' and s', either of which might have been changed from the m and s that Alice sent. To test this, he decrypts s' with Alice's public key to get v'. He then computes h(m') = v". If v' equals v", Bob is assured that m' is the same m that Alice sent.

Robustness: See: level of robustness.

Role:

1. A job function or employment position to which people or other system entities may be assigned in a system. (See: role-based access control. Compare: duty, billet, principal, user.)
2. (Common Criteria) A pre-defined set of rules establishing the allowed interactions between a user and the TOE.

Role-based access control: A form of identity-based access control wherein the system entities that are identified and controlled are functional positions in an organization or process. (See: authorization, constraint, identity, principal, role.)

Tutorial: Administrators assign permissions to roles as needed to perform functions in the system. Administrators separately assign user identities to roles. When a user accesses the system in an identity (for which the user has been registered) and initiates a session using a role (to which the user has been assigned), then the permissions that have been assigned to the role are available to be exercised by the user.

Root, root CA:

1. (PKI) A CA that is directly trusted by an end entity. (See: trust anchor, trusted CA.)
2. (hierarchical PKI) The CA that is the highest level (most trusted) CA in a certification hierarchy; i.e., the authority upon whose public key all certificate users base their validation of certificates, CRLs, certification paths, and other constructs.(See: top CA.)

   Tutorial: The root CA in a certification hierarchy issues public-key certificates to one or more additional CAs that form the second-highest level. Each of these CAs may issue certificates to more CAs at the third-highest level, and so on. To initialize operation of a hierarchical PKI, the root's initial public key is Securely distributed to all certificate users in a way that does not depend on the PKI's certification relationships, i.e., by an out-of-band procedure. The root's public key may be distributed simply as a numerical value, but typically is distributed in a self-signed certificate in which the root is the subject. The root's certificate is signed by the root itself because there is no higher authority in a certification hierarchy. The root's certificate is then the first certificate in every certification path.
3. (DNS) The base of the tree structure that defines the name space for the Internet DNS. (See: domain name.)
4. (MISSI) A name previously used for a MISSI policy creation authority, which is not a root as defined above for general usage, but is a CA at the second level of the MISSI hierarchy, immediately subordinate to a MISSI policy approving authority.
5. (UNIX) A user account (a.k.a. "superuser") that has all privileges (including all security-related privileges) and thus can manage the system and its other user accounts.

Root certificate:

1. (PKI) A certificate for which the subject is a root. (See: trust anchor certificate, trusted certificate.)
2. (hierarchical PKI) The self-signed public-key certificate at the top of a certification hierarchy.

Root key: (I) (PKI) A public key for which the matching private key is held by a root. (See: trust anchor key, trusted key.)

Root registry: (MISSI) A name previously used for a MISSI PAA.

ROT13: See: secondary definition under "Caesar cipher".

Router:

1. (IP) A networked computer that forwards IP packets that are not addressed to the computer itself. (Compare: host.)

2. (IPS) A gateway that operates in the IPS Internet Layer to connect two or more subnetworks.

3. (OSI-RM) A computer that is a gateway between two networks at OSI-RM Layer 3 and that relays and directs data packets through that internetwork. (Compare: bridge, proxy.)

RSA: See: Rivest-Shamir-Adleman.

Rule: See: policy rule.

Rule-based security policy: "A security policy based on global rules [i.e., policy rules] imposed for all users. These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users." (Compare: identity based security policy, policy rule, RBAC.)

Rules of behavior: A body of security policy that has been established and implemented concerning the responsibilities and expected behavior of entities that have access to a system.

Tutorial: For persons employed by a corporation or government, the rules might cover such matters as working at home, remote access, use of the Internet, use of copyrighted works, use of system resources for unofficial purpose, assignment and limitation of system privileges, and individual accountability.

S field: See: Security Level field.

S-BGP: See: Secure BGP.

S-HTTP: See: Secure Hypertext Transfer Protocol.

S-Key: A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login.

Tutorial: The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one. (Thus, an intruder using wiretapping cannot compute a valid password from knowledge of one previously used.) The server verifies a password by hashing the currently presented password (or initialization value) one time and comparing the hash result with the previously presented password.

S-MIME: See: Secure-MIME.

SAD: See: Security Association Database.

Safety: The property of a system being free from risk of causing harm (especially physical harm) to its system entities. (Compare: security.)

SAID: See: security association identifier.

Salami swindle: (slang) "Slicing off a small amount from each transaction. This kind of theft was made worthwhile by automation. Given a high transaction flow, even rounding down to the nearest cent and putting the 'extra' in a bogus account can be very profitable."

Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term. (See: Deprecated Usage under "Green Book".)

Salt: A data value used to vary the results of a computation in a security mechanism, so that an exposed computational result from one instance of applying the mechanism cannot be reused by an attacker in another instance. (Compare: initialization value.)

Example: A password-based access control mechanism might protect against capture or accidental disclosure of its password file by applying a one-way encryption algorithm to passwords before storing them in the file. To increase the difficulty of off-line, dictionary attacks that match encrypted values of potential passwords against a copy of the password file, the mechanism can concatenate each password with its own random salt value before applying the one-way function.

SAML: See: Security Assertion Markup Language (SAML).

Sandbox: A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

1. Delete sensitive data from a file, device, or system. (See: erase, zeroize.)

2. Modify data so as to be able either (a) to completely declassify it or (b) to downgrade it to a lower security level.

SAP: See: special access program.

SASL: See: Simple Authentication and Security Layer.

SCA: See: subordinate certification authority.

Scavenging: (threat action) See: secondary definition under "exposure".

SCI: See: sensitive compartmented information.

SCIF: See: sensitive compartmented information facility.

SCOMP: Secure COMmunications Processor; an enhanced, MLS version of the Honeywell Level 6 minicomputer. It was the first system to be rated in TCSEC Class A1. (See: KSOS.)

Screen room: (slang) Synonym for "shielded enclosure" in the context of electromagnetic emanations. (See: EMSEC, TEMPEST.)

Deprecated Term: To avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term.

Screening router: Synonym for "filtering router".

Script kiddy: (slang) A cracker who is able to use existing attack techniques (i.e., to read scripts) and execute existing attack software, but is unable to invent new exploits or manufacture the tools to perform them; pejoratively, an immature or novice cracker.

Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term. (See: Deprecated Usage under "Green Book".)

SDE: See: Secure Data Exchange.

SDNS: See: Secure Data Network System.

SDU: See: "service data unit" under "protocol data unit".

Seal: To use asymmetric cryptography to encrypt plain text with a public key in such a way that only the holder of the matching private key can learn what was the plain text (Compare: shroud, wrap.)

Deprecated Usage: A DOCUMENT SHOULD NOT use this term with this definition unless the DOCUMENT includes the definition, because the definition is not widely known and the concept can be expressed by using other, standard terms. Instead, use "salt and encrypt" or other terminology that is specific with regard to the mechanism being used.

Tutorial: The definition does *not* say "only the holder of the matching private key can decrypt the cipher-text to learn what was the plaintext"; sealing is stronger than that. If Alice simply encrypts a plaintext P with a public key K to produce cipher-text C = K(P), then if Bob guesses that P = X, Bob could verify the guess by checking whether K(P) = K(X). To "seal" P and block Bob's guessing attack, Alice could attach a long string R of random bits to P before encrypting to produce C = K(P,R); if Bob guesses that P = X, Bob can only test the guess by also guessing R. (See: salt.)

Secret:

1a. (adjective) The condition of information being protected from being known by any system entities except those that are intended to know it. (See: data confidentiality.)

1b. (noun) An item of information that is protected thusly.

Usage: This term applies to symmetric keys, private keys, and passwords.

Secret key: A key that is kept secret or needs to be kept secret.

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it mixes concepts in a potentially misleading way. In the context of asymmetric cryptography, DOCUMENTS SHOULD use "private key". In the context of symmetric cryptography, the adjective "secret" is unnecessary because all keys must be kept secret.

Secret-key cryptography: Synonym for "symmetric cryptography".

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it could be confused with "asymmetric cryptography", in which the private key is kept secret.

Derivation: Symmetric cryptography is sometimes called "secret-key cryptography" because entities that share the key, such as the originator and the recipient of a message, need to keep the key secret from other entities.

Secure BGP (S-BGP): A project of BBN Technologies, sponsored by the U.S. DoD's Defense Advanced Research Projects Agency, to design and Demonstrate an architecture to secure the Border Gateway Protocol and to promote deployment of that architecture in the Internet. Tutorial: S-BGP incorporates three security mechanisms:

- A PKI supports authentication of ownership of IP address blocks, autonomous system (AS) numbers, an AS's identity, and a BGP router's identity and its authorization to represent an AS. This PKI parallels and takes advantage of the Internet's existing IP address and AS number assignment system.
- A new, optional, BGP transitive path attribute carries digital signatures (in "attestations") covering the routing information in a BGP UPDATE. These signatures along with certificates from the S-BGP PKI enable the receiver of a BGP routing UPDATE to validate the attribute and gain trust in the address prefixes and path information that it contains.
- IPsec provides data and partial sequence integrity, and enables BGP routers to authenticate each other for exchanges of BGP control traffic.

Secure Data Exchange (SDE): A LAN security protocol defined by the IEEE 802.10 standard.

Secure Data Network System (SDNS): An NSA program that developed security protocols for electronic mail (see: MSP), OSI-RM Layer 3 (see: SP3), OSI-RM Layer 4 (see: SP4), and key establishment (see: KMP).

Secure distribution: See: trusted distribution.

Secure Hash Algorithm (SHA): A cryptographic hash function (specified in SHS) that produces an output (see: "hash result") -- of selectable length of either 160, 224, 256, 384, or 512 bits -- for input data of any length < 2**64 bits.

Secure Hash Standard (SHS): The U.S. Government standard that specifies SHA.

Secure Hypertext Transfer Protocol (S-HTTP): An Internet protocol for providing client-server security services for HTTP communications. (Compare: https.)

Tutorial: S-HTTP was originally specified by CommerceNet, a coalition of businesses interested in developing the Internet for commercial uses. Several message formats may be incorporated into S-HTTP clients and servers, particularly CMS and MOSS. S-HTTP supports choice of security policies, key management mechanisms, and cryptographic algorithms through option negotiation between parties for each transaction. S-HTTP supports modes of operation for both asymmetric and symmetric cryptography. S-HTTP attempts to avoid presuming a particular trust model, but it attempts to facilitate multiply rooted, hierarchical trust and anticipates that principals may have many public-key certificates.

Secure-MIME: Secure Multipurpose Internet Mail Extensions: an Internet protocol to provide encryption and digital signatures for Internet mail messages.

Secure multicast: Refers generally to providing security services for multicast groups of various types (e.g., 1-to-N and M-to-N) and to classes of protocols used to protect multicast packets.

Tutorial: Multicast applications include video broadcast and multicast file transfer, and many of these applications require network security services. The Multicast Security Reference Framework covers three functional areas:

- Multicast data handling: Security-related treatment of multicast data by the sender and the receiver.
- Group key management: Secure distribution and refreshment of keying material. (See: Group Domain of Interpretation.) - Multicast security policy: Policy translation and interpretation across the multiple administrative domains that typically are spanned by a multicast application.

Secure Shell(trademark) (SSH(trademark)): Refers to a protocol for secure remote login and other secure network services.

Usage: On the Web site of SSH Communication Security Corporation, at it says, "SSH [and] the SSH logo ... are either trademarks or registered trademarks of SSH." This Glossary seeks to make readers aware of this trademark claim but takes no position on its validity.

Tutorial: SSH has three main parts:

- Transport layer protocol: Provides server authentication, confidentiality, and integrity; and can optionally provide compression. This layer typically runs over a TCP connection, but might also run on top of any other reliable data stream.

- User authentication protocol: Authenticates the client-side user to the server. It runs over the transport layer protocol.
- Connection protocol: Multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

Secure Sockets Layer (SSL): An Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-oriented end-to-end Encryption to provide data confidentiality service and data integrity service for traffic between a client (often a web browser) and a server, and that can optionally provide peer entity authentication between the client and the server. (See: Transport Layer Security.)

Tutorial: SSL has two layers; SSL's lower layer, the SSL Record Protocol, is layered on top of an IPS Transport-Layer protocol and encapsulates protocols that run in the upper layer. The upperlayer protocols are the three SSL management protocols – SSL Handshake Protocol, SSL Change Cipher Spec Protocol, or SSL Alert Protocol -- and some Application-Layer protocol (e.g., HTTP). The SSL management protocols provide asymmetric cryptography for server authentication (verifying the server's identity to the client) and optional client authentication (verifying the client's identity to the server), and also enable them, before the application protocol transmits or receives data, to negotiate a symmetric encryption algorithm and secret session key (to use for data confidentiality service) and a keyed hash (to use for data integrity service). SSL is independent of the application it encapsulates, and any application can layer on top of SSL transparently. However, many Internet applications might be better served by IPsec.

Secure state:

1a. A system condition in which the system is in conformance with the applicable security policy. (Compare: clean system, transaction.)

1b. (formal model) A system condition in which no subject can access any object in an unauthorized manner. (See: secondary definition under "Bell-LaPadula model".)

Security:

1a. A system condition that results from the establishment and maintenance of measures to protect the system.

1b. A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss. (Compare: safety.)

2. Measures taken to protect a system.

Tutorial: Parker suggests that providing a condition of system security may involve the following six basic functions, which overlap to some extent:

- "Deterrence": Reducing an intelligent threat by discouraging action, such as by fear or doubt. (See: attack, threat action.)
- "Avoidance": Reducing a risk by either reducing the value of the potential loss or reducing the probability that the loss will occur. (See: risk analysis. Compare: "risk avoidance" under "risk".)
- "Prevention": Impeding or thwarting a potential security violation by deploying a countermeasure.
- "Detection": Determining that a security violation is impending, is in progress, or has recently occurred, and thus make it possible to reduce the potential loss. (See: intrusion detection.)
- "Recovery": Restoring a normal state of system operation by compensating for a security violation, possibly by eliminating or repairing its effects. (See: contingency plan, main entry for "recovery".)
- "Correction": Changing a security architecture to eliminate or reduce the risk of reoccurrence of a security violation or threat consequence, such as by eliminating a vulnerability.

Security architecture: A plan and set of principles that describe (a) the security services that a system is required to provide to meet the needs of its users, (b) the system components required to implement the services, and (c) the performance levels required in the components to deal with the threat environment.

(See: defense in depth, IATF, OSI-RM Security Architecture, security controls, Tutorial under "security policy".)

Tutorial: A security architecture is the result of applying the system engineering process. A complete system security architecture includes administrative security, communication security, computer security, emanations security, personnel security, and physical security. A complete security architecture needs to deal with both intentional, intelligent threats and accidental threats.

Security Assertion Markup Language (SAML): A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners.

Security association:

1. A relationship established between two or more entities to enable them to protect data they exchange. (See: association, ISAKMP, SAD. Compare: session.)

Tutorial: The relationship is represented by a set of data that is shared between the entities and is agreed upon and considered a contract between them. The data describes how the associated entities jointly use security services. The relationship is used to negotiate characteristics of security mechanisms, but the relationship is usually understood to exclude the mechanisms themselves.

2. A simplex (uni-directional) logical connection created for security purposes and implemented with either AH or ESP (but not both). The security services offered by a security association depend on the protocol (AH or ESP), the IPsec mode (transport or tunnel), the endpoints, and the election of optional services within the protocol. A security association is identified by a triple consisting of (a) a destination IP address, (b) a protocol (AH or ESP) identifier, and (c) a Security Parameter Index.
3. "A set of policy and cryptographic keys that provide security services to network traffic that matches that policy". (See: cryptographic association, group security association.)
4. "The totality of communications and security mechanisms and functions (e.g., communications protocols, security protocols, security mechanisms and functions) that securely binds together two security contexts in different end systems or relay systems supporting the same information domain."

Security Association Database (SAD): In an IPsec implementation that operates in a network node, a database that contains parameters to describe the status and operation of each of the active security associations that the node has established with other nodes. Separate inbound and outbound SADs are needed because of the directionality of IPsec security associations.

Security association identifier (SAID): A data field in a security protocol (such as NLSP or SDE), used to identify the security association to which a PDU is bound. The SAID value is usually used to select a key for decryption or authentication at the destination.

Security assurance:

1. An attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced. (Compare: trust.)
2. A procedure that ensures a system is developed and operated as intended by the **system's security policy.**
3. "The degree of confidence one has that the security controls operate correctly and protect the system as intended."

   Deprecated Definition: DOCUMENTS SHOULD NOT use definition 3; it is a definition for "assurance level" rather than for "assurance".

4. (U.S. Government, identity authentication) The (a) "degree of confidence in the vetting process used to establish the identity of the individual to whom the [identity] credential was issued" and the (b) "degree of confidence that the individual who uses the credential is the individual to whom the credential was issued".

Deprecated Definition: DOCUMENTS SHOULD NOT use definition 4; it mixes concepts in a potentially misleading way. Part "a" is a definition for "assurance level" (rather than "security assurance") of an identity registration process; and part "b" is a definition for "assurance level" (rather than "security assurance") of an identity authentication process. Also, the processes of registration and authentication should be defined and designed separately to ensure clarity in certification.

Security audit: An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

Tutorial: The basic audit objective is to establish accountability for system entities that initiate or participate in security relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate security violations. security audit trail

A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results

Security by obscurity: Attempting to maintain or increase security of a system by keeping secret the design or construction of a security mechanism.

Tutorial: This approach has long been discredited in cryptography, where the phrase refers to trying to keep an algorithm secret, rather than just concealing the keys. One must assume that mass-produced or widely fielded cryptographic devices eventually will be lost or stolen and, therefore, that the algorithms will be reverse engineered and become known to the adversary. Thus, one should rely on only those algorithms and protocols that are strong enough to have been published widely, and have been peer reviewed for long enough that their flaws have been found and removed. For example, NIST used a long, public process to select AES to replace DES. In computer and network security, the principle of "no security by obscurity" also applies to security mechanisms other than cryptography. For example, if the design and implementation of a protocol for access control are strong, then reading the protocol's source code should not enable you to find a way to evade the protection and penetrate the system. security class (D) Synonym for "security level".

Security clearance: A determination that a person is eligible, under the standards of a specific security policy, for authorization to access sensitive information or other system resources. (See: clearance level.)

Security compromise: A security violation in which a system resource is exposed, or is potentially exposed, to unauthorized access. (Compare: data compromise, exposure, violation.)

Security controls: The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. (See: security architecture.)

Security doctrine: A specified set of procedures or practices that direct or provide guidance for how to comply with security policy. (Compare: security mechanism, security policy.)

Tutorial: Security policy and security doctrine are closely related. However, policy deals mainly with strategy, and doctrine deals with tactics. Security doctrine is often understood to refer mainly to administrative security, personnel security, and physical security. For example, security mechanisms and devices that implement them are normally designed to operate in a limited range of environmental and administrative conditions, and these conditions must be met to complement and ensure the technical protection afforded by the hardware, firmware, and software in the devices. Security doctrine specifies how to achieve those conditions. (See: "first law" under "Courtney's laws".)

S**ecurity domain:** See: domain.

Security environment: The set of external entities, procedures, and conditions that affect secure development, operation, and maintenance of a system. (See: "first law" under "Courtney's laws".)

Security event: An occurrence in a system that is relevant to the security of the system. (See: security incident.)

Tutorial: The term covers both events that are security incidents and those that are not. In a CA workstation, for example, a list of security events might include the following:

- Logging an operator into or out of the system.
- Performing a cryptographic operation, e.g., signing a digital certificate or CRL.
- Performing a cryptographic card operation: creation, insertion, removal, or backup.
- Performing a digital certificate lifecycle operation: rekey, renewal, revocation, or update.

- Posting a digital certificate to an X.500 Directory.
- Receiving a key compromise notification.
- Receiving an improper certification request.
- Detecting an alarm condition reported by a cryptographic module.
- Failing a built-in hardware self-test or a software system integrity check.

Security fault analysis: A security analysis, usually performed on hardware at the level of gate logic, gate-by-gate, to determine the security properties of a device when a hardware fault is encountered.

Security function: A function in a system that is relevant to the security of the system; i.e., a system function that must operate correctly to ensure adherence to the system's security policy.

Security gateway:

1. An internetwork gateway that separates trusted (or relatively more trusted) hosts on one side from untrusted (or less trusted) hosts on the other side. (See: firewall and guard.)

2. "An intermediate system that implements IPsec protocols."

Tutorial: IPsec's AH or ESP can be implemented on a gateway between a protected network and an unprotected network, to provide security services to the protected network's hosts when they communicate across the unprotected network to other hosts and gateways.

Security incident:

1. A security event that involves a security violation. (See: CERT, security event, security intrusion, security violation.)

Tutorial: In other words, a security event in which the system's security policy is disobeyed or otherwise breached.

2. "Any adverse event [that] compromises some aspect of computer or network security."

Deprecated Definition: DOCUMENTS SHOULD NOT use definition 2 because

(a) a security incident may occur without actually being harmful (i.e., adverse) and because

(b) this Glossary defines "compromise" more narrowly in relation to unauthorized access.

3. "A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices."

Deprecated Definition: DOCUMENTS SHOULD NOT use definition 3 because it mixes concepts in way that does not agree with common usage; a security incident is commonly thought of as involving a realization of a threat (see: threat action), not just a threat.

Security intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Security kernel: "The hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct." (See: kernel, TCB.)

Tutorial: A security kernel is an implementation of a reference monitor for a given hardware base.

Security label: An item of meta-data that designates the value of one or more security-relevant attributes (e.g., security level) of a system resource. (Compare: security marking.)

Deprecated usage: To avoid confusion, DOCUMENTS SHOULD NOT use "security label" for "security marking", or vice versa, even though that is commonly done (including in some national and international standards that should know better).

Tutorial: Humans and automated security mechanisms use a security label of a system resource to determine, according to applicable security policy, how to control access to the resource (and they affix appropriate, matching security markings to physical instances of the resource). Security labels are most often used to support data confidentiality policy, and sometimes used to support data integrity policy.

As explained in the form that is taken by security labels of a protocol's packets varies depending on the OSI-RM layer in which the protocol operates. Like meta-data generally, a security label of a data packet may be either explicit (e.g., IPSO) or implicit (e.g., Alice treats all messages received from Bob as being labeled "Not For Public Release"). In a connectionless protocol, every packet might have an explicit label; but in a connection-oriented protocol, all packets might have the same implicit label that is determined at the time the connection is established. Both classified and unclassified system resources may require a security label.

Security level: The combination of a hierarchical classification level and a set of non-hierarchical category designations that represents how sensitive a specified type or item of information is. (See: dominate, lattice model. Compare: classification level.)

Usage: DOCUMENTS that use this term SHOULD state a definition for it. The term is usually understood to involve sensitivity to disclosure, but it also is used in many other ways and could easily be misunderstood.

Security Level field: A 16-bit field that specifies a security level value in the security option (option type 130) of version 4 IP's datagram header format.

Deprecated Abbreviation: DOCUMENTS SHOULD NOT use the abbreviation "S field", which is potentially ambiguous.

Security management infrastructure (SMI): System components and activities that support security policy by monitoring and controlling security services and mechanisms, distributing security information, and reporting security events. Tutorial: The associated functions are as follows:

Controlling (granting or restricting) access to system resources: This includes verifying authorizations and identities, controlling access to sensitive security data, and modifying access priorities and procedures in the event of attacks.

Retrieving (gathering) and archiving (storing) security information: This includes logging security events and analyzing the log, monitoring and profiling usage, and reporting security violations.

Managing and controlling the encryption process: This includes performing the functions of key management and reporting on key management problems. (See: PKI.)

Security marking: A physical marking that is bound to an instance of a system resource and that represents a security label of the resource, i.e., that names or designates the value of one or more security relevant attributes of the resource. (Compare: security label.)

Tutorial: A security label may be represented by various equivalent markings depending on the physical form taken by the labeled resource. For example, a document could have a marking composed of a bit pattern when the document is stored electronically as a file in a computer, and also a marking of printed alphabetic characters when the document is in paper form.

Security mechanism: A method or process (or a device incorporating it) that can be used in a system to implement a security service that is provided by or within the system. (See: Tutorial under "security policy". Compare: security doctrine.)

Usage: Usually understood to refer primarily to components of communication security, computer security, and emanation security. Examples: Authentication exchange, checksum, digital signature, encryption, and traffic padding.

Security model: A schematic description of a set of entities and relationships by which a specified set of security services are provided by or within a system. Example: Bell-LaPadula model, OSI-RM. (See: Tutorial under "security policy".)

Security parameters index (SPI):

1. (IPsec) A 32-bit identifier used to distinguish among security associations that terminate at the same destination (IP address) and use the same security protocol (AH or ESP). Carried in AH and ESP to enable the receiving system to determine under which security association to process a received packet.

2. (mobile IP) A 32-bit index identifying a security association from among the collection of associations that are available between a pair of nodes, for application to mobile IP protocol messages that the nodes exchange.

Security perimeter: A physical or logical boundary that is defined for a domain or enclave and within which a particular security policy or security Architecture applies. (See: insider, outsider.)

Security policy:

1. A definite goal, course, or method of action to guide and determine present and future decisions concerning security in a system.

2a. A set of policy rules (or principles) that direct how a system (or an organization) provides security services to protect sensitive and critical system resources. (See: identity-based security policy, policy rule, rule-based security policy, rules of behavior. Compare: security architecture, security doctrine, security mechanism, security model,

2b. A set of rules to administer, manage, and control access to network resources.

2c. (X.509) A set of rules laid down by an authority to govern the use and provision of security services and facilities.

2d. (Common Criteria) A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

Tutorial: Ravi Sandhu suggests that security policy is one of four layers of the security engineering process. We suggest that each of Sandhu's four layers is a mapping between two points of view that differ in their degree of abstraction, according to the perspectives of various participants in system design, development, and operation activities, as follows:.

- Mission functions view: The perspective of a user of system resources. States time-phased protection needs for resources and identifies sensitive and critical resources -- networks, hosts, applications, and databases. Independent of rules and practices used to achieve protection.
- Domain practices view: The perspective of an enterprise manager who sets protection standards for resources. States rules and practices for protection. Identifies domain members; i.e., entities (users(providers) and resources (including data objects). Independent of system topology. Not required to be hierarchical.

- Enclave services view: The perspective of a system designer who allocates security functions to major components. Assigns security services to system topology structures and their contents. Independent of security mechanisms. Hierarchical across all domains.
- Agent mechanisms view: The perspective of a system engineer who specifies security mechanisms to implement security services. Specifies mechanisms to be used by protocol, database, and application engines. Independent of type and manufacture of platforms and other physical devices.
- Platform devices view: The perspective of an as-built description of the system in operation. Specifies exactly how to build or assemble the system, and also specifies procedures for operating the system.

Security Policy Database (SPD): In an IPsec implementation operating in a network node, a database that contains parameters that specify policies set by a user or administrator to determine what IPsec services, if any, are to be provided to IP datagrams sent or received by the node, and in what fashion they are provided. For each datagram, the SPD specifies one of three choices: discard the datagram, apply IPsec services (e.g., AH or ESP), or bypass IPsec. Separate inbound and outbound SPDs are needed because of the directionality of IPsec security associations. (Compare: SAD.)

Security Protocol 3 (SP3): A protocol developed by SDNS to provide connectionless data security at the top of OSI-RM Layer 3.

Security Protocol 4: (SP4) A protocol developed by SDNS to provide either connectionless or end-to-end connection-oriented data security at the bottom of OSI-RM Layer 4. (See: TLSP.)

Security-relevant event: Synonym for "security event".

Security-sensitive function: Synonym for "security function".

Security service:

1. A processing or communication service that is provided by a system to give a specific kind of protection to system resources. (See: access control service, audit service, availability service, data confidentiality service, data integrity service, data origin authentication service, non-repudiation service, peer entity authentication service, system integrity service.)

   Tutorial: Security services implement security policies, and are implemented by security mechanisms.

2. "A service, provided by a layer of communicating open systems, ensures adequate security of the systems or the data transfers."

Security situation: (ISAKMP) The set of all security-relevant information (e.g., network addresses, security classifications, manner of operation such as normal or emergency) that is needed to decide the security services that are required to protect the association that is being negotiated.

Security target: A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Tutorial: A security target (ST) is a statement of security claims for a particular information technology security product or system, and is the basis for agreement among all parties as to what security the product or system offers. An ST parallels the structure of a protection profile, but has additional elements that inc lude product-specific detailed information. An ST contains a summary specification, which defines the specific measures taken in the product or system to meet the security requirements.

Security token: See: token.

Security violation: An act or event that disobeys or otherwise breaches security policy. (See: compromise, penetration, security incident.)

Seed: A value that is an input to a pseudorandom number generator.

Selective-field confidentiality: A data confidentiality service that preserves confidentiality for one or more parts (i.e., fields) of each packet. (See: selective-field integrity.)

Tutorial: Data confidentiality service usually is applied to entire SDUs, but some situations might require protection of only part of each packet. For example, when Alice uses a debit card at an automated teller machine (ATM), perhaps only her PIN is enciphered for confidentiality when her transaction request is transmitted from the ATM to her bank's computer.

In any given operational situation, there could be many different reasons for using selective field confidentiality. In the ATM example, there are at least four possibilities: The service may provide a fail-safe mode of operation, ensuring that the bank can still process transactions (although with some risk) even when the encryption system fails. It may make messages easier to work with when doing system fault isolation. It may avoid problems with laws that prevent shipping enciphered data across international borders. It may improve efficiency by reducing processing load at a central computer site.

Selective-field integrity: A data integrity service that preserves integrity for one or more parts (i.e., fields) of each packet. (See: selective-field confidentiality.)

Tutorial: Data integrity service may be implemented in a protocol to protect the SDU part of packets, the PCI part, or both.

- SDU protection: When service is provided for SDUs, it usually is applied to entire SDUs, but it might be applied only to parts of SDUs in some situations. For example, an IPS Application-Layer protocol might need protection of only part of each packet, and this might enable faster processing.
- PCI protection: To prevent active wiretapping, it might be desirable to apply data integrity service to the entire PCI, but some PCI fields in some protocols need to be mutable in transit. For example, the "Time to Live" field in IPv4 is changed each time a packet passes through a router in the Internet Layer. Thus, the value that the field will have when the packet arrives at its destination is not predictable by the sender and cannot be included in a checksum computed by the sender. (See: Authentication Header.)

Self-signed certificate: A public-key certificate for which the public key bound by the certificate and the private key used to sign the certificate are components of the same key pair, which belongs to the signer. (Compare: root certificate.)

Tutorial: In a self-signed X.509 public-key certificate, the issuer's DN is the same as the subject's DN.

Semantic security: An attribute of an encryption algorithm that is a formalization of the notion that the algorithm not only hides the plain text but also reveals no partial information about the plain text; i.e., whatever is computable about the plain text when given the cipher text, is also computable without the cipher text.(Compare: indistinguishability.)

Semiformal: Expressed in a restricted syntax language with defined semantics. (Compare: formal, informal.)

Sensitive: A condition of a system resource such that the loss of some specified property of that resource, such as confidentiality or integrity, would adversely affect the interests or business of its owner or user. (See: sensitive information. Compare: critical.)

Sensitive compartmented information (SCI): (U.S. Government) Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal control systems established by the Director of Central Intelligence.

Sensitive compartmented information facility (SCIF): (U.S. Government) "An accredited area, room, group of rooms, building, or installation where SCI may be stored, used, discussed, and (or processed."

Sensitive information:

1. Information for which (a) disclosure, (b) alteration, or (c) destruction or loss could adversely affect the interests or business of its owner or user. (See: data confidentiality, data integrity, sensitive. Compare: classified, critical.)

2. (U.S. Government) Information for which (a) loss, (b) misuse, (c) unauthorized access, or (d) unauthorized modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974, but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Tutorial: Systems that are not U.S. national security systems, but contain sensitive U.S. Federal Government information, must be protected according to the Computer Security Act of 1987 (Public Law 100-235). (See: national security.)

Sensitivity label: Synonym for "classification label".

Deprecated term: DOCUMENTS SHOULD NOT use this term because the definition of "sensitive" involves not only data confidentiality, but also data integrity.

Sensitivity level: Synonym for "classification level".

Deprecated term: DOCUMENTs SHOULD NOT use this term because the definition of "sensitive" involves not only data confidentiality, but also data integrity.

Separation of duties: The practice of dividing the steps in a system process among different individual entities (i.e., different users or different roles) so as to prevent a single entity acting alone from being able to subvert the process. Usage: a.k.a. "separation of privilege". (See: administrative security, dual control.)

Serial number: See: certificate serial number.

Serpent: A symmetric, 128-bit block cipher designed by Ross Anderson, Eli Biham, and Lars Knudsen as a candidate for the AES.

Server: A system entity that provides a service in response to requests from other system entities called clients.

Service data unit (SDU): See: secondary definition under "protocol data unit".

Session:

1a. (computer usage) A continuous period of time, usually initiated by a login, during which a user accesses a computer System **:**

1b. (computer activity) The set of transactions or other computer activities that are performed by or for a user during a period of computer usage.

2. (access control) A temporary mapping of a principal to one or more roles. (See: role-based access control.)

Tutorial: A user establishes a session as a principal and activates some subset of roles to which the principal has been assigned. The authorizations available to

the principal in the session are the union of the permissions of all the roles activated in the session. Each session is associated with a single principal and, therefore, with a single user. A principal may have multiple, concurrent sessions and may activate a different set of roles in each session.

3. (computer network) A persistent but (normally) temporary association between a user agent (typically a client) and a second process (typically a server). The association may persist across multiple exchanges of data, including multiple connections. (Compare: security association.)

Session key: In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. (See: ephemeral, KDC, session. Compare: master key.)

Tutorial: A session key is used for a defined period of communication between two system entities or components, such as for the duration of a single connection or transaction set; or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be rekeyed frequently.

SET(trademark) See: SET Secure Electronic Transaction(trademark).

SET private extension: One of the private extensions defined by SET for X.509 certificates. Carries information about hashed root key, certificate type, merchant data, cardholder certificate requirements, encryption support for tunneling, or message support for payment instructions.

SET qualifier: A certificate policy qualifier that provides information about the location and content of a SET certificate policy.

Tutorial: Besides the policies and qualifiers inherited from its own certificate, each CA in the SET certification hierarchy may add one qualifying statement to the root policy when the CA issues a certificate. The additional qualifier is a certificate policy for that CA. Each policy in a SET certificate may have these qualifiers:

(a) a URL where a copy of the policy statement may be found;

(b) an electronic mail address where a copy of the policy statement may be found;

(c) a hash result of the policy statement, computed using the indicated algorithm;

(d) a statement declaring any disclaimers associated with the issuing of the certificate.

SET Secure Electronic Transaction(trademark) or SET(trademark): A protocol developed jointly by MasterCard International and Visa International and published as an open standard to provide confidentiality of transaction information, payment integrity, and authentication of transaction participants for payment card transactions over unsecured networks, such as the Internet. (See: acquirer, brand, cardholder, dual signature, electronic commerce, IOTP, issuer, merchant, payment gateway, third party.)

Tutorial: This term and acronym are trademarks of SETCo. MasterCard and Visa announced the SET standard on 1 February 1996.

SETCo: Abbreviation of "SET Secure Electronic Transaction LLC", formed on 19 December 1997 by MasterCard and Visa for implementing the SET Secure Electronic Transaction(trademark) standard. A later memorandum of understanding added American Express and JCB Credit Card Company as co-owners of SET Co.

SHA, SHA-1, SHA-2: See: Secure Hash Algorithm.

Shared identity: See: secondary definition under "identity".

Shared secret: Synonym for "cryptographic key" or "password".

Deprecated Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term is used in many ways and could easily be misunderstood.

Shielded enclosure: "Room or container designed to attenuate electromagnetic radiation, acoustic signals, or emanations." (See: emanation. Compare: SCIF.)

Short title: "Identifying combination of letters and numbers assigned to certain items of COMSEC material to facilitate handling, accounting, and controlling." (Compare: KMID, long title.)

Shroud: (verb) To encrypt a private key, possibly in concert with a policy that prevents the key from ever being available in clear-text form beyond a certain, well-defined security perimeter. (See: encrypt. Compare: seal, wrap.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term as defined here; the definition duplicates the meaning of other, standard terms. Instead, use "encrypt" or other terminology that is specific with regard to the mechanism being used.

SHS: See: Secure Hash Standard.

Sign: Create a digital signature for a data object. (See: signer.)

Signal analysis: Gaining indirect knowledge (inference) of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data. (See: emanation. Compare: traffic analysis.)

Signal intelligence: The science and practice of extracting information from signals. (See: signal security.)

Signal security: The science and practice of protecting signals. (See: cryptology, security.)

Tutorial: The term "signal" denotes

(a) communication in almost any form and also

(b) emanations for other purposes, such as radar. Signal security is opposed by signal intelligence, and each discipline includes opposed sub-disciplines as follows:

Signal Security Signal Intelligence

1. Communication Security	**1.** Communication Intelligence
1a. Cryptography	**1a.** Cryptanalysis
1b. Traffic Security	**1b.** Traffic Analysis
1c. Steganography	**1c**. Detection and Interception
2. Electronic Security	**2.** Electronic Intelligence
2a. Emission Security	**2a.** Electronic Reconnaissance
2b. Counter-Countermeasures	**2b.** Countermeasures

Signature: A symbol or process adopted or executed by a system entity with present intention to declare that a data object is genuine. (See: digital signature, electronic signature.)

Signature certificate: A public-key certificate that contains a public key that is intended to be used for verifying digital signatures, rather than for encrypting data or performing other cryptographic functions.

Tutorial: A v3 X.509 public-key certificate may have a "keyUsage" extension that indicates the purpose for which the certified public key is intended. (See: certificate profile.)

Signed receipt: A MIME service that

(a) provides, to the originator of a message, proof of delivery of the message and

(b) enables the originator to demonstrate to a third party that the recipient was able to verify the signature of the original message.

Tutorial: The receipt is bound to the original message by a signature; consequently, the service may be requested only for a message that is signed. The receipt sender may optionally also encrypt the receipt to provide confidentiality between the receipt sender and the receipt recipient.

Signer: A human being or organization entity that uses a private key to sign (i.e., create a digital signature on) a data object.

SILS: See: Standards for Interoperable LAN-MAN Security.

Simple authentication:

1. An authentication process that uses a password as the information needed to verify an identity claimed for an entity. (Compare: strong authentication.)

2. "Authentication by means of simple password arrangements." Simple Authentication and Security Layer (SASL)

   An Internet specification for adding authentication service to connection-based protocols. (Compare: EAP, GSS-API.)

   Tutorial: To use SASL, a protocol includes a command for authenticating a user to a server and for optionally negotiating protection of subsequent protocol interactions. The command names a registered security mechanism. SASL mechanisms include Kerberos, GSS-API, S(KEY, and others. Some protocols that use SASL are IMAP4 and POP3.

Simple Key Management for Internet Protocols (SKIP) (I) A key-distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

Tutorial: SKIP was designed by Ashar Aziz and Whitfield Diffie at Sun Microsystems and proposed as the standard key management protocol for IPsec, but IKE was chosen instead. Although IKE is mandatory for an IPsec implementation, the use of SKIP is not excluded. SKIP uses the Diffie-Hellman-Merkle algorithm (or could use another key-agreement algorithm) to generate a key-encrypting key for use between two entities. A session key is used with a symmetric algorithm to encrypt data in one or more IP packets that are to be sent from one entity to the other. A symmetric KEK is established and used to encrypt the session key, and the encrypted session key is placed in a SKIP header that is added to each IP packet that is encrypted with that session key.

Simple Mail Transfer Protocol (SMTP): A TCP-based, Application-Layer, Internet Standard protocol for moving electronic mail messages from one computer to another.

Simple Network Management protocol (SNMP): A (usually) UDP-based, Application-Layer, Internet Standard protocol (RFCs 3410-3418) for conveying management information between system components that act as managers and agents.

Simple Public Key Infrastructure (SPKI): A set of experimental concepts (RFCs 2692, 2693) that were proposed as alternatives to the concepts standardized in PKIX.

Simple security property: (formal model) Property of a system whereby a subject has read access to an object only if the clearance of the subject dominates the classification of the object. See: Bell-LaPadula model.

Single sign-on:

1. An authentication subsystem that enables a user to access multiple, connected system components (such as separate hosts on a network) after a single login at only one of the components. (See: Kerberos.)

2. (Liberty Alliance) A security subsystem that enables a user identity to be authenticated at an identity provider -- i.e., at a service that authenticates and asserts the user's identity – and then have that authentication be honored by other service providers.

Tutorial: A single sign-on subsystem typically requires a user to log in once at the beginning of a session, and then during the session transparently grants access by the user to multiple, separately protected hosts, applications, or other system resources, without further login action by the user (unless, of course, the user logs out). Such a subsystem has the advantages of being user friendly and enabling authentication to be managed consistently across an entire enterprise. Such a subsystem also has the disadvantage of requiring all the accessed components to depend on the security of the same authentication information.

Singular identity: See: secondary definition under "identity".

Site: A facility -- i.e., a physical space, room, or building together with its physical, personnel, administrative, and other safeguards -- in which system functions are performed. (See: node.)

Situation: See: security situation.

SKEME: A key-distribution protocol from which features were adapted for IKE.

SKIP: See: Simple Key Management for Internet Protocols.

SKIPJACK: A type 2, 64-bit block cipher with a key size of 80 bits. (See: CAPSTONE, CLIPPER, FORTEZZA, Key Exchange Algorithm.)

Tutorial: SKIPJACK was developed by NSA and formerly classified at the U.S. DoD "Secret" level. On 23 June 1998, NSA announced that SKIPJACK had been declassified.

Slot: (MISSI) One of the FORTEZZA PC card storage areas that are each able to hold an X.509 certificate plus other data, including the private key that is associated with a public-key certificate.

Smart card: A credit-card sized device containing one or more integrated circuit chips that perform the functions of a computer's central processor, memory, and input /output interface. (See: PC card, smart token.)

Usage: Sometimes this term is used rather strictly to mean a card that closely conforms to the dimensions and appearance of the kind of plastic credit card issued by banks and merchants.

Smart token: A device that conforms to the definition of "smart card" except that rather than having the standard dimensions of a credit card, the token is packaged in some other form, such as a military dog tag or a door key. (See: smart card, cryptographic token.)

SMI: See: security management infrastructure.

SMTP: See: Simple Mail Transfer Protocol.

Smurf attack: (slang) A denial-of-service attack that uses IP broadcast addressing to send ICMP ping packets with the intent of flooding a system. (See: fraggle attack, ICMP flood.)

Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term.

Derivation: The Smurfs are a fictional race of small, blue creatures that were created by a cartoonist. Perhaps the inventor of this attack thought that a swarm of ping packets resembled a gang of smurfs. (See: Deprecated Usage under "Green Book".)

Tutorial: The attacker sends ICMP echo request ("ping") packets that appear to originate not from the attacker's own IP address, but from the address of the host or router that is the target of the attack. Each packet is addressed to an IP broadcast address, e.g., to all IP addresses in a given network. Thus, each echo request that is sent by the attacker results in many echo responses being sent to the target address. This attack can disrupt service at a particular host, at the hosts that depend on a particular router, or in an entire network.

Sneaker net: (slang) A process that transfers data between systems only manually, under human control; i.e., a data transfer process that involves an air gap. Deprecated Term: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term.

Snefru: A public-domain, cryptographic hash function (a.k.a. "The Xerox Secure Hash Function") designed by Ralph C. Merkle at Xerox Corporation. Snefru can produce either a 128-bit or 256-bit output (i.e., hash result). (See: Khafre, Khufu.)

Sniffing: (slang) Synonym for "passive wiretapping"; most often refers to capturing and examining the data packets carried on a LAN

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it unnecessarily duplicates the meaning of a term that is better established. (See: Deprecated Usage under "Green Book".

SNMP: See: Simple Network Management Protocol.

Social engineering: Euphemism for non-technical or low-technology methods, often involving trickery or fraud, that are used to attack information Systems. Example: phishing.

Deprecated Term: DOCUMENTS SHOULD NOT use this term; it is too vague. Instead, use a term that is specific with regard to the means of attack, e.g., blackmail, bribery, coercion, impersonation, intimidation, lying, or theft.

SOCKS: An Internet protocol that provides a generalized proxy server that enables client-server applications (e.g., TELNET, FTP, or HTTP; running over either TCP or UDP) to use the services of a firewall.

Tutorial: SOCKS is layered under the IPS Application Layer and above the Transport Layer. When a client inside a firewall wishes to establish a connection to an object that is reachable only through the firewall, it uses TCP to connect to the SOCKS server, negotiates with the server for the authentication method to be used, authenticates with the chosen method, and then sends a relay request. The SOCKS server evaluates the request, typically based on source and destination addresses, and either establishes the appropriate connection or denies it.

Soft TEMPEST: The use of software techniques to reduce the radio frequency information leakage from computer displays and keyboards. (See: TEMPEST.)

Soft token: A data object that is used to control access or authenticate authorization. (See: token.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term as defined here; the definition duplicates the meaning of other, standard terms. Instead, use "attribute certificate" or another term that is specific with regard to the mechanism being used.

Software: Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution. (Compare: firmware.)

Software error: (threat action) See: secondary definitions under "corruption", "exposure", and "incapacitation".

SORA: See: SSO-PIN ORA.

Source authentication: Synonym for "data origin authentication" or "peer entity authentication". (See: data origin authentication, peer entity authentication).

Deprecated Term: DOCUMENTS SHOULD NOT use this term because it is ambiguous and, in either meaning, duplicates the meaning of internationally standardized terms. If the intent is to authenticate the original creator or packager of data received, then use "data origin authentication". If the intent is to authenticate the identity of the sender of data in the current instance, then use "peer entity authentication".

Source integrity: The property that data is trustworthy (i.e., worthy of reliance or trust), based on the trustworthiness of its sources and the trustworthiness of any procedures used for handling data in the system. Usage: a.k.a. Biba integrity. (See: integrity. Compare: correctness integrity, data integrity.)

Tutorial: For this kind of integrity, there are formal models of unauthorized modification (see: Biba model) that logically complement the more familiar models of unauthorized disclosure (see: Bell-LaPadula model). In these models, objects are labeled to indicate the credibility of the data they contain, and there are rules for access control that depend on the labels.

SP3: See: Security Protocol 3.

SP4: See: Security Protocol 4.

Spam:

1a. (slang verb) To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities.

1b. (slang noun) Electronic "junk mail".

Deprecated Usage: DOCUMENTS SHOULD NOT use this term in uppercase letters, because SPAM(trademark) is a trademark of Hormel Foods Corporation. Hormel says, "We do not object to use of this slang term [spam] to describe [unsolicited advertising email], although we do object to the use of our product image in association with that term. Also, if the term is to be used, it SHOULD be used in all lower-case letters to distinguish it from our trademark SPAM, which SHOULD be used with all uppercase letters." (See: metadata.)

Tutorial: In sufficient volume, spam can cause denial of service. (See: flooding.) According to Hormel, the term was adopted as a result of a Monty Python skit in which a group of Vikings sang a chorus of 'SPAM, SPAM, SPAM ...' in an increasing crescendo, drowning out other conversation. This lyric became a metaphor for the unsolicited advertising messages that threaten to overwhelm other discourse on the Internet.

SPD: See: Security Policy Database.

Special access program (SAP): (U.S. Government) "Sensitive program, [that is] approved in writing by a head of agency with [i.e., who has] original top secret classification authority, [and] that imposes need-to-know and access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program." (See: formal access approval, SCI. Compare: collateral information.)

SPI: See: Security Parameters Index.

SPKI: See: Simple Public Key Infrastructure.

Split key: A cryptographic key that is generated and distributed as two or more separate data items that individually convey no knowledge of the whole key that results from combining the items. (See: dual control, split knowledge.)

Split knowledge:

1. A security technique in which two or more entities separately hold data items that individually do not convey knowledge of the information that results from combining the items. (See: dual control, split key.)
2. "A condition under which two or more entities separately have key components [that] individually convey no knowledge of the plaintext key [that] will be produced when the key components are combined in the cryptographic module."

Spoof: (threat action) See: secondary definition under "masquerade".

Spoofing attack: Synonym for "masquerade attack".

Spread spectrum: A TRANSEC technique that transmits a signal in a bandwidth much greater than the transmitted information needs. Example: frequency hopping.

Tutorial: Usually uses a sequential, noise-like signal structure to spread the normally narrowband information signal over a relatively wide band of frequencies. The receiver correlates the signals to retrieve the original information signal. This technique decreases potential interference to other receivers, while achieving data confidentiality and increasing immunity of spread spectrum receivers to noise and interference.

Spyware: (slang) Software that an intruder has installed surreptitiously on a networked computer to gather data from that computer and send it through the network to the intruder or some other interested party. (See: malicious logic, Trojan horse.)

Deprecated Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term is used in many ways and could easily be misunderstood.

Tutorial: Some examples of the types of data that might be gathered by spyware are application files, passwords, email addresses, usage histories, and keystrokes. Some examples of motivations for gathering the data are blackmail, financial fraud, identity theft, industrial espionage, market research, and voyeurism.

SSH(trademark): See: Secure Shell(trademark).

SSL: See: Secure Sockets Layer.

SSO: See: system security officer.

SSO PIN: (MISSI) One of two PINs that control access to the functions and stored data of a FORTEZZA PC card. Knowledge of the SSO PIN enables a card user to perform the FORTEZZA functions intended for use by an end user and also the functions intended for use by a MISSI CA. (See: user PIN.)

SSO-PIN ORA (SORA): (MISSI) A MISSI organizational RA that operates in a mode in which the ORA performs all card management functions and, therefore, requires knowledge of the SSO PIN for FORTEZZA PC cards issued to end users. Standards for Interoperable LAN/MAN Security (SILS)

1. The IEEE 802.10 standards committee.
2. A set of IEEE standards, which has eight parts: (a) Model, including security management, (b) Secure Data Exchange protocol, (c) Key Management, (d) [has been incorporated in (a)], (e) SDE Over Ethernet 2.0, (f) SDE Sublayer Management, (g) SDE Security Labels, and (h) SDE PICS Conformance. Parts b, e, f, g, and h are incorporated in IEEE Standard 802.10-1998.

Star property: See: *-property.

Star Trek attack: (slang) An attack that penetrates your system where no attack has ever gone before. Deprecated Usage: DOCUMENTS SHOULD NOT use this term; it is a joke for Trekkies.

Static: (adjective) Refers to a cryptographic key or other parameter that is relatively long-lived. (Compare: ephemeral.)

Steganography: Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself.

Storage channel: See: covert storage channel.

Storage key: A cryptographic key used by a device for protecting information that is being maintained in the device, as opposed to protecting information that is being transmitted between devices.

Stream cipher: An encryption algorithm that breaks plain text into a stream of successive elements (usually, bits) and encrypts the n-th plaintext element with the n-th element of a parallel key stream, thus converting the plaintext stream into a ciphertext stream. (See: block cipher.)

Stream integrity service: A data integrity service that preserves integrity for a sequence of data packets, including both (a) bit-by-bit datagram integrity of each individual packet in the set and (b) packet-by-packet sequential integrity of the set as a whole. (See: data integrity. Compare: datagram integrity service.)

Tutorial: Some internetwork applications need only datagram integrity, but others require that an entire stream of packets be protected against insertion, reordering, deletion, and delay:

- "Insertion": The destination receives an additional packet that was not sent by the source.
- "Reordering": The destination receives packets in a different order than that in which they were sent by the source.
- "Deletion": A packet sent by the source is not ever delivered to the intended destination.
- "Delay": A packet is detained for some period of time at a relay, thus hampering and postponing the packet's normal timely delivery from source to destination.

Strength:

1. (I) (cryptography) A cryptographic mechanism's level of resistance to attacks. (See: entropy, strong, work factor.)
2. (Common Criteria) "Strength of function" is a "qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms": (See: strong.)
   - Basic: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential."
   - Medium: "... against straightforward or intentional breach ... by attackers possessing a moderate attack potential."
   - High: "... against deliberately planned or organized breach ... by attackers possessing a high attack potential."

Strong:

1. (cryptography) Used to describe a cryptographic algorithm that would require a large amount of computational power to defeat it. (See: strength, work factor, weak key.)
2. (COMPUSEC) Used to describe a security mechanism that would be difficult to defeat. (See: strength, work factor.)

Strong authentication:

1. An authentication process that uses a cryptographic security mechanism -- particularly public-key certificates – to verify the identity claimed for an entity. (Compare: simple authentication.)
2. "Authentication by means of cryptographically derived credentials."

Subject:

1. A process in a computer system that represents a principal and that executes with the privileges that have been granted to that principal. (Compare: principal, user.)
2. (formal model) A system entity that causes information to flow among objects or changes the system state; technically, a process-domain pair. A subject may itself be an object relative to some other subject; thus, the set of subjects in a system is a subset of the set of objects. (See: Bell-LaPadula model, object.)
3. (digital certificate) The name (of a system entity) that is bound to the data items in a digital certificate; e.g., a DN that is bound to a key in a public-key certificate. (See: X.509.)

Subject CA: The CA that is the subject of a cross-certificate issued by another CA. (See: cross-certification.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term because it is not widely known and could be misunderstood. Instead, say "the CA that is the subject of the cross-certificate".

Subnetwork: An OSI term for a system of packet relays and connecting links that implement OSI-RM layer 2 or 3 to provide a communication service that interconnects attached end systems. Usually, the relays are all of the same type (e.g., X.25 packet switches, or interface units in an IEEE 802.3 LAN). (See: gateway, internet, router.)

Subordinate CA (SCA):

1. A CA whose public-key certificate is issued by another (superior) CA. (See: certification hierarchy. Compare: crosscertification.)
2. (MISSI) The fourth-highest (i.e., bottom) level of a MISSI certification hierarchy; a MISSI CA whose public-key certificate is signed by a MISSI CA rather than by a MISSI PCA. A MISSI SCA is the administrative authority for a subunit of an organization, established when it is desirable to organizationally distribute or decentralize the CA service. The term refers both to that authoritative office or role, and to the person who fills that office. A MISSI SCA registers end users and issues their certificates and may also register ORAs, but may not register other CAs. An SCA periodically issues a CRL.

Subordinate DN: An X.500 DN is subordinate to another X.500 DN if it begins with a set of attributes that is the same as the entire second DN except for the terminal attribute of the second DN (which is usually the name of a CA). For example, the DN <C=FooLand, O=Gov, OU=Treasurer, CN=DukePinchpenny> is subordinate to the DN <C=FooLand, O=Gov, CN=KingFooCA>.

Subscriber: (PKI) A user that is registered in a PKI and, therefore, can be named in the "subject" field of a certificate issued by a CA in that PKI. (See: registration, user.)

Usage: This term is needed to distinguish registered users from two other kinds of PKI users:

- Users that access the PKI but are not identified to it: For example, a relying party may access a PKI repository to obtain the certificate of some other party. (See: access.)
- Users that do not access the PKI: For example, a relying party (see: certificate user) may use a digital certificate that was obtained from a database that is not part of the PKI that issued the certificate.

Substitution:

1. (cryptography) A method of encryption in which elements of the plain text retain their sequential position but are replaced by elements of cipher text. (Compare: transposition.)

2. (threat action) See: secondary definition under "falsification".

Subsystem: A collection of related system components that together perform a system function or deliver a system service.

Superencryption: An encryption operation for which the plaintext input to be transformed is the ciphertext output of a previous encryption operation. (Compare: hybrid encryption.)

Superuser: (UNIX) Synonym for "root".

Survivability: The ability of a system to remain in operation or existence despite adverse conditions, including natural occurrences, accidental actions, and attacks. (Compare: availability, reliability.)

SwIPe: An encryption protocol for IP that provides confidentiality, integrity, and authentication and can be used for both end-to-end and intermediate-hop security.

Tutorial: The swIPe protocol is an IP predecessor that is concerned only with encryption mechanisms; policy and key management are handled outside the protocol.

Syllabary: (encryption) A list of individual letters, combinations of letters, or syllables, with their equivalent code groups, used for spelling out proper names or other unusual words that are not present in the basic vocabulary (i.e., are not in the codebook) of a code used for encryption.

Symmetric cryptography: A branch of cryptography in which the algorithms use the same key for both of two counterpart cryptographic operations (e.g., encryption and decryption). (See: asymmetric cryptography. Compare: secret-key cryptography.)

Tutorial: Symmetric cryptography has been used for thousands of years. A modern example is AES. Symmetric cryptography has a disadvantage compared to asymmetric cryptography with regard to key distribution. For example, when Alice wants to ensure confidentiality for data she sends to Bob, she encrypts the data with a key, and Bob uses the same key to decrypt. However, keeping the shared key secret entails both cost and risk when the key is distributed to both Alice and Bob. (See: key distribution, key management.)

Symmetric key: A cryptographic key that is used in a symmetric cryptographic algorithm. (See: symmetric cryptography.)

SYN flood: A denial-of-service attack that sends a large number of TCP SYN (synchronize) packets to a host with the intent of disrupting the operation of that host. (See: blind attack, flooding.)

Tutorial: This attack seeks to exploit a vulnerability in the TCP specification or in a TCP implementation. Normally, two hosts use a three-way exchange of packets to establish a TCP connection: (a) host 1 requests a connection by sending a SYN packet to host 2; (b) host 2 replies by sending a SYN-ACK (acknowledgement) packet to host 1; and (c) host 1 completes the connection by sending an ACK packet to host 2. To attack host 2, host 1 can send a series of TCP SYNs, each with a different phony source address. discusses how to use packet filtering to prevent such attacks from being launched from behind an Internet service provider's aggregation point.) Host 2 treats each SYN as a request from a separate host, replies to each with a SYN-ACK, and waits to receive the matching ACKs. (The attacker can use random or unreachable sources addresses in the SYN packets, or can use source addresses that belong to third parties, that then become secondary victims.) For each SYN-ACK that is sent, the TCP process in host 2 needs some memory space to store state information while waiting for the matching ACK to be returned. If the matching ACK never arrives at host 2, a timer associated with the pending SYN-ACK will eventually expire and release the space. But if host 1 (or a cooperating group of hosts) can rapidly send many SYNs to host 2, host 2 will need to store state information for many pending SYNACKs and may run out of space. This can prevent host 2 from responding to legitimate connection requests from other hosts or even, if there are flaws in host 2's TCP implementation, crash when the available space is exhausted.

Synchronization: Any technique by which a receiving (decrypting) cryptographic process attains an internal state that matches the transmitting (encrypting) process, i.e., has the appropriate keying material to process the cipher text and is correctly initialized to do so.

System: Synonym for "information system".

Usage: This is a generic definition, and is the one with which the term is used in this Glossary. However, DOCUMENTS that use the term, especially DOCUMENTs that are protocol specifications, SHOULD state a more specific definition. Also, DOCUMENTS that specify security features, services, and assurances need to define which system components and system resources are inside the applicable security perimeter and which are outside. (See: security architecture.)

System architecture: The structure of system components, their relationships, and the principles and guidelines governing their design and evolution over time. (Compare: security architecture.)

System component:

1. A collection of system resources that

(a) forms a physical or logical part of the system,

(b) has specified functions and interfaces, and

(c) is treated (e.g., by policies or specifications) as existing independently of other parts of the system. (See: subsystem.)

2. (ITSEC) An identifiable and self-contained part of a TOE.

Usage: Component is a relative term because components may be nested; i.e., one component of a system may be a part of another component of that system.

Tutorial: Components can be characterized as follows:

- A "physical component" has mass and takes up space.
- A "logical component" is an abstraction used to manage and coordinate aspects of the physical environment, and typically represents a set of states or capabilities of the system. system entity

An active part of a system -- a person, a set of persons (e.g., some kind of organization), an automated process, or a set of processes (see: subsystem) -- that has a specific set of capabilities. (Compare: subject, user.)

System high: The highest security level at which a system operates, or is capable of operating, at a particular time or in a particular environment. (See: system-high security mode.)

System-high security mode: A mode of system operation wherein all users having Access to the system possess all necessary authorizations (both security clearance and formal access approval) for all data handled by the system, but some users might not have need-to-know for all the data. (See: (system operation(under "mode", formal access approval, protection level, security clearance.)

Usage: Usually abbreviated as "system-high mode". This mode was defined in U.S. DoD policy that applied to system accreditation, but the term is widely used outside the Government.

System integrity:

1. An attribute or quality "that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation." [C4009, NCS04] (See: recovery, system integrity service.)
2. "Quality of an [information system] reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data." [from an earlier version of C4009]

   Deprecated Definition: DOCUMENTS SHOULD NOT use definition 2 because it mixes several concepts in a potentially misleading way. Instead, DOCUMENTS should use the term with definition 1 and, depending on what is meant, couple the term with additional, more specifically descriptive and informative terms, such as "correctness", "reliability", and "data integrity".

System integrity service: A security service that protects system resources in a verifiable manner against unauthorized or accidental change, loss, or destruction. (See: system integrity.)

System low: The lowest security level supported by a system at a particular time or in a particular environment. (Compare: system high.)

System resource: Data contained in an information system; or a service provided by a system; or a system capacity, such as processing power or communication bandwidth; or an item of system equipment (i.e., hardware, firmware, software, or documentation); or a facility that houses system operations and equipment. (See: system component.)

System security officer (SSO): A person responsible for enforcement or administration of the security policy that applies to a system. (Compare: manager, operator.)

System user: A system entity that consumes a product or service provided by the system, or that accesses and employs system resources to produce a product or service of the system. (See: access, Compare: authorized user, manager, operator, principal, privileged user, subject, subscriber, system entity, unauthorized user.)

Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term is used in many ways and could easily be misunderstood:

- This term usually refers to an entity that has been authorized to access the system, but the term sometimes is used without regard for whether access is authorized.

- This term usually refers to a living human being acting either personally or in an organizational role. However, the term also may refer to an automated process in the form of hardware, software, or firmware; to a set of persons; or to a set of processes.
- DOCUMENTS SHOULD NOT use the term to refer to a mixed set containing both persons and processes. This exclusion is intended to prevent situations that might cause a security policy to be interpreted in two different and conflicting ways. A system user can be characterized as direct or indirect:
- "Passive user": A system entity that is (a) outside the system's security perimeter *and* (b) can receive output from the system but cannot provide input or otherwise interact with the system.
- "Active user": A system entity that is (a) inside the system's security perimeter *or* (b) can provide input or otherwise interact with the system.

TACACS: See: Terminal Access Controller (TAC) Access Control System.

TACACS+: A TCP-based protocol that improves on TACACS by separating the functions of authentication, authorization, and accounting and by encrypting all traffic between the network access server and authentication server. TACACS+ is extensible to allow any authentication mechanism to be used with TACACS+ clients.

Tamper: Make an unauthorized modification in a system that alters the system's functioning in a way that degrades the security services that the system was intended to provide. (See: QUADRANT. Compare: secondary definitions under "corruption" and "misuse".)

Tamper-evident: A characteristic of a system component that provides evidence that an attack has been attempted on that component or system.

Tamper-resistant: A characteristic of a system component that provides passive protection against an attack. (See: tamper.)

Tampering: (threat action) See: secondary definitions under "corruption" and "misuse".

Target of evaluation (TOE): (Common Criteria) An information technology product or system that is the subject of a security evaluation, together with the product's associated administrator and user documentation. (Compare: protection profile.)

Tutorial: The security characteristics of the target of evaluation (TOE) are described in specific terms by a corresponding security target, or in more general terms by a protection profile. In Common Criteria philosophy, it is important that a TOE be evaluated against the specific set of criteria expressed in the target. This evaluation consists of rigorous analysis and testing performed by an accredited, independent laboratory. The scope of a TOE evaluation is set by the EAL and other requirements specified in the target. Part of this process is an

evaluation of the target itself, to ensure that it is correct, complete, and internally consistent and can be used as the baseline for the TOE evaluation.

TCB: See: trusted computing base.

TCC field: See: Transmission Control Code field.

TCG: See: Trusted Computing Group.

TCP: See: Transmission Control Protocol.

TCP/IP: Synonym for "Internet Protocol Suite".

TCSEC: See: Trusted Computer System Evaluation Criteria. (Compare: TSEC.)

TDEA: See: Triple Data Encryption Algorithm.

Teardrop attack: (slang) A denial-of-service attack that sends improperly formed IP packet fragments with the intent of causing the destination system to fail.

Deprecated Term: DOCUMENTS that use this term SHOULD state a definition for it because the term is often used imprecisely and could easily be misunderstood. (See: Deprecated Usage under "Green Book".)

Technical non-repudiation: See: (secondary definition under) non-repudiation.

Technical security: Security mechanisms and procedures that are implemented in and executed by computer hardware, firmware, or software to provide automated protection for a system. (See: security architecture. Compare: administrative security.)

Telecommunications Security Word System (TSEC): (U.S. Government) A terminology for designating telecommunication security equipment. (Compare: TCSEC.)

Tutorial: A TSEC designator has the following parts: - Prefix "TSEC(" for items and systems, or suffix "(TSEC" for assemblies. (Often omitted when the context is clear.)

- First letter, for function: "C" COMSEC equipment system, "G" general purpose, "K" cryptographic, "H" crypto-ancillary, "M" manufacturing, "N" noncryptographic, "S" special purpose.
- Second letter, for type or purpose: "G" key generation, "I" data transmission, "L" literal conversion, "N" signal conversion, "O" multipurpose, "P" materials production, "S" special purpose, "T" testing or checking, "U" television, "W" teletypewriter, "X" facsimile, "Y" speech.
- Optional third letter, used only in designations of assemblies, for type or purpose: "A" advancing, "B" base or cabinet, "C" combining, "D" drawer or panel, "E" strip or chassis, "F" frame or rack, "G" key generator, "H" keyboard, "I" translator or reader, "J" speech processing, "K" keying or permuting, "L"

repeater, "M" memory or storage, "O" observation, "P" power supply or converter, "R" receiver, "S" synchronizing, "T" transmitter, "U" printer, "V" removable COMSEC component, "W" logic programmer(programming, "X" special purpose.

- Model number, usually two or three digits, assigned sequentially within each letter combination (e.g., KG-34, KG-84).
- Optional suffix letter, used to designate a version. First version has no letter, next version has "A" (e.g., KG-84, KG-84A), etc.

TELNET: A TCP-based, Application-Layer, Internet Standard protocol for remote login from one host to another.

TEMPEST:

1. Short name for technology and methods for protecting against data compromise due to electromagnetic emanations from electrical and electronic equipment
2. (U.S. Government) "Short name referring to investigation, study, and control of compromising emanations from IS equipment."

   Deprecated Usage: DOCUMENTS SHOULD NOT use this term as a synonym for "electromagnetic emanations security"; instead, use EMSEC. Also, the term is NOT an acronym for Transient Electromagnetic Pulse Surveillance Technology.

   Tutorial: The U.S. Federal Government issues security policies that (a) state specifications and standards for techniques to reduce the strength of emanations from systems and reduce the ability of unauthorized parties to receive and make use of emanations and (b) state rules for applying those techniques. Other nations presumably do the same.

TEMPEST zone: "Designated area [i.e., a physical volume] within a facility where equipment with appropriate TEMPEST characteristics ... may be operated."

Tutorial: The strength of an electromagnetic signal decreases in proportion to the square of the distance between the source and the receiver. Therefore, EMSEC for electromagnetic signals can be achieved by a combination of (a) reducing the strength of emanations to a defined level and (b) establishing around that equipment an appropriately sized physical buffer zone from which unauthorized entities are excluded. By making the zone large enough, it is possible to limit the signal strength available to entities outside the zone to a level lower than can be received and read with known, state-of-the-art methods. Typically, the need for and size of a TEMPEST zone established by a security policy depends not only on the measured level of signal emitted by equipment, but also on the perceived threat level in the equipment's environment.

Terminal Access Controller (TAC): Access Control System (TACACS) A UDP-based authentication and access control protocol in which a network access server receives an identifier and password from a remote terminal and passes them to a separate authentication server for verification. (See: TACACS+.)

Tutorial: TACACS can provide service not only for network access servers but also routers and other networked computing devices via one or more centralized authentication servers. TACACS was originally developed for ARPANET and has evolved for use in commercial equipment.

TESS: See: The Exponential Encryption System.

The Exponential Encryption System (TESS): A system of separate but cooperating cryptographic mechanisms and functions for the secure authenticated exchange of cryptographic keys, the generation of digital signatures, and the distribution of public keys. TESS uses asymmetric cryptography, based on discrete exponentiation, and a structure of self-certified public keys.

Theft: (threat action) See: secondary definitions under "interception" and "misappropriation".

Threat:

1. A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. (See: dangling threat, INFOCON level, threat action, threat agent, threat consequence. Compare: attack, vulnerability.)
2. Any circumstance or event with the potential to adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service. (See: sensitive information.)

   Usage:

   (a) Frequently misused with the meaning of either "threat action" or "vulnerability".

   (b) In some contexts, "threat" is used more narrowly to refer only to intelligent threats; for example, see definition 2 below.

   (c) In some contexts, "threat" is used more broadly to cover both definition 1 and other concepts, such as in definition 3 below.

   Tutorial: A threat is a possible danger that might exploit a vulnerability. Thus, a threat may be intentional or not:

   - "Intentional threat": A possibility of an attack by an intelligent entity (e.g., an individual cracker or a criminal organization).
   - "Accidental threat": A possibility of human error or omission, unintended equipment malfunction, or natural disaster (e.g., fire, flood, earthquake, windstorm, and other causes listed in).

The Common Criteria characterizes a threat in terms of (a) a threat agent, (b) a presumed method of attack, (c) any vulnerabilities that are the foundation for the attack, and (d) the system resource that is attacked. That characterization agrees with the definitions in this Glossary (see: diagram under "attack").

3. The technical and operational ability of a hostile entity to detect, exploit, or subvert a friendly system and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

Tutorial: To be likely to launch an attack, an adversary must have (a) a motive to attack, (b) a method or technical ability to make the attack, and (c) an opportunity to appropriately access the targeted system.

4. "An indication of an impending undesirable event."

Threat action: A realization of a threat, i.e., an occurrence in which system security is assaulted as the result of either an accidental event or an intentional act. (See: attack, threat, threat consequence.)

Tutorial: A complete security architecture deals with both intentional acts (i.e., attacks) and accidental events. (See: various kinds of threat actions defined under the four kinds of "threat consequence".)

Threat agent: A system entity that performs a threat action, or an event that results in a threat action.

Threat analysis: An analysis of the threat actions that might affect a system, primarily emphasizing their probability of occurrence but also considering their resulting threat consequences.

Threat consequence: A security violation that results from a threat action.

Tutorial: The four basic types of threat consequence are "unauthorized disclosure", "deception", "disruption", and "usurpation". (See main Glossary entries of each of these four terms for lists of the types of threat actions that can result in these consequences.)

Thumbprint:

1. A pattern of curves formed by the ridges on the tip of a **thumb.** (See: biometric authentication, fingerprint.)

2. Synonym for some type of "hash result". (See: biometric authentication. Compare: fingerprint.)

Ticket : Synonym for "capability token".

Tutorial: A ticket is usually granted by a centralized access control server (ticket-granting agent) to authorize access to a system resource for a limited time. Tickets can be implemented with either symmetric cryptography (see: Kerberos) or asymmetric cryptography (see: attribute certificate).

Tiger team: A group of evaluators employed by a system's managers to perform penetration tests on the system.

Time stamp:

1. (noun) With respect to a data object, a label or marking in which is recorded the time (time of day or other instant of elapsed time) at which the label or marking was affixed to the data object. (See: Time-Stamp Protocol.)

2. (noun) "With respect to a recorded network event, a data field in which is recorded the time (time of day or other instant of elapsed time) at which the event took place."

   Tutorial: A time stamp can be used as evidence to prove that a data object existed (or that an event occurred) at or before a particular time. For example, a time stamp might be used to prove that a digital signature based on a private key was created while the corresponding public-key certificate was valid, i.e., before the certificate either expired or was revoked. Establishing this proof would enable the certificate to be used after its expiration or revocation, to verify a signature that was created earlier. This kind of proof is required as part of implementing PKI services, such as non-repudiation service, and long-term security services, such as audit.

Time-Stamp Protocol: An Internet protocol that specifies how a client requests and receives a time stamp from a server for a data object held by the client.

Tutorial: The protocol describes the format of (a) a request sent to a time-stamp authority and (b) the response that is returned containing a time stamp. The authority creates the stamp by concatenating (a) a hash value of the input data object with (c) a UTC time value and other parameters (policy OID, serial number, indication of time accuracy, nonce, DN of the authority, and various extensions), and then signing that dataset with the authority's private key as specified in CMS. Such an authority typically would operate as a trusted third-party service, but other operational models might be used.

Timing channel: See: covert timing channel.

TKEY: A mnemonic referring to an Internet protocol for establishing a shared secret key between a DNS resolver and a DNS name server. (See: TSIG.)

TLS: See: Transport Layer Security.

TLSP: See: Transport Layer Security Protocol.

TOE: See: target of evaluation.

Token:

1. (cryptography) See: cryptographic token. (Compare: dongle.)

2. (access control) An object that is used to control access and is passed between cooperating entities in a protocol that synchronizes use of a shared resource. Usually, the entity that currently holds the token has exclusive access to the resource. (See: capability token.)

Token backup: A token management operation that stores sufficient information in a database (e.g., in a CAW) to recreate or restore a security token (e.g., a smart card) if it is lost or damaged.

Token copy: A token management operation that copies all the personality information from one security token to another. However, unlike in a token restore operation, the second token is initialized with its own, different local security values such as PINs and storage keys.

Token management: The process that includes initializing security tokens (e.g., "smart card"), loading data into the tokens, and controlling the tokens during their lifecycle. May include performing key management and certificate management functions; generating and installing PINs; loading user personality data; performing card backup, card copy, and card restore operations; and updating firmware.

Token restore: A token management operation that loads a security token with data for the purpose of recreating (duplicating) the contents previously held by that or another token. (See: recovery.)

Token storage key: A cryptographic key used to protect data that is stored on a security token.

Top CA: Synonym for "root" in a certification hierarchy. (See: apex trust anchor.)

Top-level specification: "A non-procedural description of system behavior at the most abstract level; typically a functional specification that omits all implementation details." (See: formal top-level specification, Tutorial under "security policy".)

Tutorial: A top-level specification is at a level of abstraction below "security model" and above "security architecture" (see: Tutorial under "security policy").

A top-level specification may be descriptive or formal:

- "Descriptive top-level specification": One that is written in a natural language like English or an informal design notation.
- "Formal top-level specification": One that is written in a formal mathematical language to enable theorems to be proven that show that the specification correctly implements a set of formal requirements or a formal security model. (See: correctness proof.)

TPM: See: Trusted Platform Module.

Traceback: Identification of the source of a data packet. (See: masquerade, network weaving.)

Tracker: An attack technique for achieving unauthorized disclosure from a statistical database. (See: Tutorial under "inference control".)

Traffic analysis:

1. Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. The object of the analysis might be information in SDUs, information in the PCI, or both. (See: inference, traffic-flow confidentiality, wiretapping. Compare: signal analysis.)

2. "The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency)."

Traffic-flow analysis: Synonym for "traffic analysis".

Traffic-flow confidentiality (TFC):

1. A data confidentiality service to protect against traffic analysis. (See: communications cover.)

2. "A confidentiality service to protect against traffic analysis."

Tutorial: Confidentiality concerns involve both direct and indirect disclosure of data, and the latter includes traffic analysis. However, operational considerations can make TFC difficult to achieve. For example, if Alice sends a product idea to Bob in an email message, she wants data confidentiality for the message's content, and she might also want to conceal the destination of the message to hide Bob's identity from her competitors. However, the identity of the intended recipient, or at least a network address for that recipient, needs to be made available to the mail system. Thus, complex forwarding schemes may be needed to conceal the ultimate destination as the message travels through the open Internet (see: onion routing).Later, if Alice uses an ATM during a clandestine visit to negotiate with Bob, she might prefer that her bank conceal the origin of her transaction, because knowledge of the ATM's location might allow a competitor to infer Bob's identity. The bank, on the other hand, might prefer to protect only Alice's PIN (see: selective-field confidentiality).

A TFC service can be either full or partial:

- "Full TFC": This type of service conceals all traffic characteristics.
- "Partial TFC": This type of service either

  (a) conceals some but not all of the characteristics or

(b) does not completely conceal some characteristic.

On point-to-point data links, full TFC can be provided by enciphering all PDUs and also generating a continuous, random data stream to seamlessly fill all gaps between PDUs. To a wiretapper, the link then appears to be carrying an unbroken stream of enciphered data. In other cases -- including on a shared or broadcast medium, or end-to-end in a network -- only partial TFC is possible, and that may require a combination of techniques. For example, a LAN that uses "carrier sense multiple access with collision detection" (CSMA) CD; a.k.a. "listen while talk") to control access to the medium, relies on detecting intervals of silence, which prevents using full TFC. Partial TFC can be provided on that LAN by measures such as adding spurious PDUs, padding PDUs to a constant size, or enciphering addresses just above the Physical Layer; but these measures reduce the efficiency with which the LAN can carry traffic. At higher protocol layers, SDUs can be protected, but addresses and other items of PCI must be visible at the layers below.

Traffic key: A cryptographic key used by a device for protecting information that is being transmitted between devices, as opposed to protecting information that being is maintained in the device. (Compare: storage key.)

Traffic padding: "The generation of spurious instances of communication, spurious data units, and-or spurious data within data units."

Tranquility property: (formal model) Property of a system whereby the security level of an object cannot change while the object is being processed by the system. (See: Bell-LaPadula model.)

Transaction:

1. A unit of interaction between an external entity and a system, or between components within a system, that involves a series of system actions or events.
2. "A discrete event between user and systems that supports a business or programmatic purpose."

   Tutorial: To maintain secure state, transactions need to be processed coherently and reliably. Usually, they need to be designed to be atomic, consistent, isolated, and durable:

   - "Atomic": All actions and events that comprise the transaction are guaranteed to be completed successfully, or else the result is as if none at all were executed.
   - "Consistent": The transaction satisfies correctness constraints defined for the data that is being processed.
   - "Isolated": If two transactions are performed concurrently, they do not interfere with each other, and it appears as though the system performs one at a time.

- "Durable": System state and transaction semantics survive system failures.

TRANSEC: See: transmission security.

Transmission Control Code field (TCC field): A data field that provides a means to segregate traffic and define controlled communities of interest in the security option (option type = 130) of IPv4's datagram header format. The TCC values are alphanumeric trigraphs assigned by the U.S. Government as specified in RFC 791.

Transmission Control Protocol (TCP): An Internet Standard, Transport-Layer protocol that reliably delivers a sequence of datagrams from one computer to another in a computer network. (See: TCP(IP.)

Tutorial: TCP is designed to fit into a layered suite of protocols that support internetwork applications. TCP assumes it can obtain a simple but potentially unreliable end-to-end datagram service (such as IP) from the lower-layer protocols.

Transmission security (TRANSEC): COMSEC measures that protect communications from interception and exploitation by means other than cryptanalysis. Example: frequency hopping. (Compare: anti-jam, traffic flow confidentiality.)

Transport Layer: See: Internet Protocol Suite, OSI-RM.

Transport Layer Security (TLS): TLS is an Internet protocol that is based on, and very similar to, SSL Version 3.0. (Compare: TLSP.)

Tutorial: The TLS protocol is misnamed. The name misleadingly suggests that TLS is situated in the IPS Transport Layer, but TLS is always layered above a reliable Transport-Layer protocol (usually TCP) and either layered immediately below or integrated with an Application-Layer protocol (often HTTP).

Transport Layer Security Protocol (TLSP): An end-to-end encryption protocol (ISO 10736) that provides security services at the bottom of OSI-RM Layer 4, i.e., directly above Layer 3. (Compare: TLS.) TLSP evolved directly from SP4.

Transport mode: One of two ways to apply AH or ESP to protect data packets; in this mode, the IPsec protocol encapsulates (i.e., the protection applies to) the packets of an IPS Transport-Layer protocol (e.g., TCP, UDP), which normally is carried directly above IP in an IPS protocol stack. (Compare: tunnel mode.)

Tutorial: An IPsec transport-mode security association is always between two hosts; neither end has the role of a security gateway. Whenever either end of an IPsec security association is a security gateway, the association is required to be in tunnel mode.

Transposition: (cryptography) A method of encryption in which elements of the plain text retain their original form but undergo some change in their sequential position. (Compare: substitution.)

Trap door: Synonym for "back door".

Trespass: (threat action) See: secondary definition under "intrusion".

Triple Data Encryption Algorithm: A block cipher that transforms each 64-bit plaintext block by applying the DEA three successive times, using either two or three different keys for an effective key length of 112 or 168 bits.

Example: A variation proposed for IPsec's ESP uses a 168-bit key, consisting of three independent 56-bit values used by the DEA, and a 64-bit initialization vector. Each datagram contains an IV to ensure that each received datagram can be decrypted even when other datagrams are dropped or a sequence of datagrams is reordered in transit.

Triple-wrapped: (S-MIME) Data that has been signed with a digital signature, then encrypted, and then signed again.

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (See: malware, spyware. Compare: logic bomb, virus, worm.)

Trust:

1. (information system) A feeling of certainty (sometimes based on inconclusive evidence) either (a) that the system will not fail or (b) that the system meets its specifications (i.e., the system does what it claims to do and does not perform unwanted functions). (See: trust level, trusted system, trustworthy system. Compare: assurance.)

   Tutorial: Components of a system can be grouped into three classes of trust:

   - "Trusted": The component is responsible for enforcing security policy on other components; the system's security depends on flawless operation of the component. (See: trusted process.)
   - "Benign": The component is not responsible for enforcing security policy, but it has sensitive authorizations. It must be trusted not to intentionally violate security policy, but security violations are assumed to be accidental and not likely to affect overall system security.
   - "Untrusted": The component is of unknown or suspicious provenance and must be treated as deliberately malicious. (See: malicious logic.)

2. (PKI) A relationship between a certificate user and a CA in which the user acts according to the assumption that the CA creates only valid digital certificates.

   Tutorial: "Generally, an entity is said to 'trust' a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects. This trust may apply only for some specific function. The key role of trust

in [X.509] is to describe the relationship between an entity [i.e., a certificate user] and a [CA]; an entity shall be certain that it can trust the CA to create only valid and reliable certificates."

Trust anchor: (PKI) An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. (See: apex trust anchor, path validation, trust anchor CA, trust anchor certificate, trust anchor key.)

Usage: DOCUMENTS that use this term SHOULD state a definition for it because it is used in various ways in existing DOCUMENTS and other PKI literature. The literature almost always uses this term in a sense that is equivalent to this definition, but usage often differs with regard to what constitutes the point of trust.

Tutorial: A trust anchor may be defined as being based on a public key, a CA, a public-key certificate, or some combination or variation of those:

1. A public key as a point of trust: Although a certification path is defined as beginning with a "sequence of public-key certificates", an implementation of a path validation process might not explicitly handle a root certificate as part of the path, but instead begin the process by using a trusted root key to verify the signature on a certificate that was issued by the **root.** Therefore, "trust anchor" is sometimes defined as just a public key. (See: root key, trust anchor key, trusted key.)
2. A CA as a point of trust: A trusted public key is just one of the data elements needed for path validation; the IPS path validation algorithm also needs the name of the CA to which that key belongs, i.e., the DN of the issuer of the first X.509 certificate to be validated on the path. (See: issue.) Therefore, "trust anchor" is sometimes defined as either just a CA (where some public key is implied) or as a CA together with a specified public key belonging to that CA. (See: root, trust anchor CA, trusted CA.) Example: "A public key and the name of a [CA] that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor [CA]."
3. A public-key certificate as a point of trust: Besides the trusted CA's public key and name, the path validation algorithm needs to know the digital signature algorithm and any associated parameters with which the public key is used, and also any constraints that have been placed on the set of paths that may be validated using the key. All of this information is available from a CA's public-key certificate. Therefore, "trust anchor" is sometimes defined as a public-key certificate of a CA. (See: root certificate, trust anchor certificate, trusted certificate.)
4. Combinations: Combinations and variations of the first three definitions are also used in the PKI literature.

Example: "trust anchor information". The IPS standard for path validation specifies the information that describes "a CA that serves as a trust anchor for the certification path. The trust anchor information includes:

(a) the trusted issuer name,

(b) the trusted public key algorithm,

(c) the trusted public key, and

(d) optionally, the trusted public key parameters associated with the public key.

The trust anchor information may be provided to the path processing procedure in the form of a self-signed certificate. The trusted anchor information is trusted because it was delivered to the path processing procedure by some trustworthy out-of-band procedure. If the trusted public key algorithm requires parameters, then the parameters are provided along with the trusted public key."

Trust anchor CA: A CA that is the subject of a trust anchor certificate or otherwise establishes a trust anchor key. (See: root, trusted CA.)

Tutorial: The selection of a CA to be a trust anchor is a matter of policy. Some of the possible choices include (a) the top CA in a hierarchical PKI, (b) the CA that issued the verifier's own certificate, or (c) any other CA in a network PKI. Different applications may rely on different trust anchors, or may accept paths that begin with any of a set of trust anchors. The IPS path validation algorithm is the same, regardless of the choice.

Trust anchor certificate: A public-key certificate that is used to provide the first public key in a certification path. (See: root certificate, trust anchor, trusted certificate.)

Trust anchor key: A public key that is used as the first public key in a certification path. (See: root key, trust anchor, trusted public key.)

Trust anchor information: See: secondary definition under "trust anchor".

Trust chain: Synonym for "certification path". (See: trust anchor, trusted certificate.)

Deprecated Term: DOCUMENTS SHOULD NOT use this term, because it unnecessarily duplicates the meaning of the internationally standardized term. Also, the term mixes concepts in a potentially misleading way. Having "trust" involves factors unrelated to simply verifying signatures and performing other tests as specified by a standard algorithm for path validation. Thus, even if a user is able to validate a certification path algorithmically, the user still might distrust one of the CAs that issued certificates in that path or distrust some other aspects of the PKI.

Trust-file PKI: A non-hierarchical PKI in which each certificate user has its own local file (which is used by application software) of trust anchors, i.e., either public keys or

public-key certificates that the user trusts as starting points for certification paths. (See: trust anchor, web of trust. Compare: hierarchical PKI, mesh PKI.)

Example: Popular browsers are distributed with an initial file of trust anchor certificates, which often are self-signed certificates. Users can add certificates to the file or delete from it. The file may be directly managed by the user, or the user's organization may manage it from a centralized server.

Trust hierarchy: Synonym for "certification hierarchy".

Deprecated Usage: DOCUMENTS SHOULD NOT use this term because it mixes concepts in a potentially misleading way, and because a trust hierarchy could be implemented in other ways. (See: trust, trust chain, web of trust.)

Trust level: A characterization of a standard of security protection to be met by an information system. (See: Common Criteria, TCSEC.)

Tutorial: A trust level is based not only on (a) the presence of security mechanisms, but also on the use of (b) systems engineering discipline to properly structure the system and (c) implementation analysis to ensure that the system provides an appropriate degree of trust.

Trusted: See: secondary definition under "trust".

Trusted CA: A CA upon which a certificate user relies as issuing valid certificates; especially a CA that is used as a trust anchor CA. (See: certification path, root, trust anchor CA, validation.)

Tutorial. This trust is transitive to the extent that the X.509 certificate extensions permit; that is, if a trusted CA issues a certificate to another CA, a user that trusts the first CA also trusts the second CA if the user succeeds in validating the certificate path (see: path validation).

Trusted certificate: A digital certificate that a certificate user accepts as being valid "a priori", i.e., without testing the certificate to validate it as the final certificate on a certification path; especially a certificate that is used as a trust anchor certificate. (See: certification path, root certificate, trust anchor certificate, trust-file PKI, validation.)

Tutorial: The acceptance of a certificate as trusted is a matter of policy and choice. Usually, a certificate is accepted as trusted because the user obtained it by reliable, out-of-band means that cause the user to believe the certificate accurately binds its subject's name to the subject's public key or other attribute values. Many choices are possible; e.g., a trusted public-key certificate might be (a) the root certificate in a hierarchical PKI, (b) the certificate of the CA that issued the user's own certificate in a mesh PKI, or (c) a certificate provided with an application that uses a trust-file PKI.

Trusted Computer System Evaluation Criteria (TCSEC): A standard for evaluating the security provided by operating systems. Known as the "Orange Book" because of the color of its cover; first document in the Rainbow Series. (See: Common Criteria, Deprecated Usage under "Green Book", Orange Book, trust level, trusted system. Compare: TSEC.)

Tutorial: The TCSEC defines classes of hierarchically ordered assurance levels for rating computer systems. From highest to lowest, the classes are as follows:

- Division A: Verified protection. Beyond A1 Beyond current technology. (See: beyond A1.) Class A1 Verified design. (See: SCOMP.)
- Division B: Mandatory protection. Class B3 Security domains. Class B2 Structured protection. (See: Multics.) Class B1 Labeled security protection.
- Division C: Discretionary protection. Class C2 Controlled access protection. Class C1 Discretionary security protection.
- Division D: Minimal protection, i.e., has been evaluated but does not meet the requirements for a higher evaluation class.

Trusted computing base (TCB): "The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy." (See: "trusted" under "trust". Compare: TPM.)

Trusted Computing Group (TCG): A not-for-profit, industry standards organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. (See: TPM, trusted system. Compare: TSIG.)

Trusted distribution: (COMPUSEC) "A trusted method for distributing the TCB hardware, software, and firmware components, both originals and updates, that provides methods for protecting the TCB from modification during distribution and for detection of any changes to the TCB that may occur." (See: code signing, configuration control.)

Trusted key: Abbreviation for "trusted public key" and also for other types of keys. (See: root key, trust anchor key.)

Deprecated Usage: DOCUMENTS SHOULD either (a) state a definition for this term or (b) use a different, less ambiguous term. This term is ambiguous when it stands alone; e.g., it could refer to a trusted public key or to a private key or symmetric key that is believed to be secure (i.e., not compromised).

Trusted path:

1a. (COMPUSEC) A mechanism by which a computer system user can communicate directly and reliably with the TCB and that can only be activated by the user or the TCB and cannot be imitated by untrusted software within the computer.

1b. (COMSEC) A mechanism by which a person or process can communicate directly with a cryptographic module and that can only be activated by the person, process, or module, and cannot be imitated by untrusted software within the module.

Trusted Platform Module (TPM): The name of a specification, published by the TCG, for a microcontroller that can store secured information; and also the general name of implementations of that specification. (Compare: TCB.)

Trusted process: A system component that has privileges that enable it to affect the state of system security and that can, therefore, through incorrect or malicious execution, violate the system's security policy. (See: privileged process, trusted system.)

Trusted public key: A public key upon which a user relies; especially a public key that is used as a trust anchor key. (See: certification path, root key, trust anchor key, validation.)

Tutorial: A trusted public key could be (a) the root key in a hierarchical PKI, (b) the key of the CA that issued the user's own certificate in a mesh PKI, or (c) any key accepted by the user in a trust-file PKI.

Trusted recovery: A process that, after a system has experienced a failure or an attack, restores the system to normal operation (or to a secure state) without causing a security compromise. (See: recovery.)

Trusted subnetwork: A subnetwork containing hosts and routers that trust each other not to engage in active or passive attacks. (There also is an assumption that the underlying communication channels, such as telephone lines or a LAN, are protected from attack.)

Trusted system:

1. (information system) A system that operates as expected, according to design and policy, doing what is required – despite environmental disruption, human user and operator errors, and attacks by hostile parties -- and not doing other things. (See: trust level, trusted process. Compare: trustworthy.)

2. (multilevel secure) "A [trusted system is a] system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information." (See: multilevel security mode.)

Trusted Systems Interoperability Group (TSIG): A forum of computer vendors, system integrators, and users devoted to promoting interoperability of trusted computer systems. (See: trusted system. Compare: TCG.)

Trustworthy system:

1. A system that not only is trusted, but also warrants that trust because the system's behavior can be validated in some convincing way, such as through formal analysis or code review. (See: trust. Compare: trusted.)
2. (Digital Signature Guidelines) "Computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonably reliable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions; and (d) adhere to generally accepted security principles."

TSEC: See: Telecommunications Security Nomenclature System. (Compare: TCSEC.)

TSIG:

1. See: Trusted System Interoperability Group.
2. A mnemonic (presumed to be derived from "Transaction signature") referring to an Internet protocol for data origin authentication and data integrity for certain DNS operations. (See: TKEY.)

Tunnel:

1. A communication channel created in a computer network by encapsulating (i.e., layering) a communication protocol's data packets in (i.e., above) a second protocol that normally would be carried above, or at the same layer as, the first one. (See: L2TP, tunnel mode, VPN. Compare: covert channel.)

   Tutorial: Tunneling can involve almost any two IPS protocol layers. For example, a TCP connection between two hosts could conceivably be carried above SMTP (i.e., in SMTP messages) as a covert channel to evade access controls that a security gateway applies to the normal TCP layer that is below SMTP. Usually, however, a tunnel is a logical point-to-point link -- i.e., an OSI-RM Layer 2 connection -- created by encapsulating the Layer 2 protocol in one of the following three types of IPS protocols: (a) an IPS Transport-Layer protocol (such as TCP), (b) an IPS Network-Layer or Internet-Layer protocol (such as IP), or (c) another Layer 2 protocol. In many cases, the encapsulation is accomplished with an extra, intermediate that is layered below the tunneled Layer 2 protocol.

   Tunneling can be used to move data between computers that use a protocol not supported by the network connecting them. Tunneling also can enable a computer network to use the services of a second network as though the second network were a set of point-to-point links between the first network's nodes. (See: VPN.)

2. (SET) The name of a SET private extension that indicates whether the CA or the payment gateway supports passing encrypted messages to the cardholder through the merchant. If so, the extension lists OIDs of symmetric encryption algorithms that are supported.

Tunnel mode: One of two ways to apply the IPsec protocols (AH and ESP) to protect data packets; in this mode, the IPsec protocol encapsulates (i.e., the protection applies to) IP packets, rather than the packets of higher-layer protocols. (See: tunnel. Compare: transport mode.)

Tutorial: Each end of a tunnel-mode security association may be either a host or a security gateway. Whenever either end of an IPsec security association is a security gateway, the association is required to be in tunnel mode.

Two-person control: The close surveillance and control of a system, a process, or materials (especially with regard to cryptography) at all times by a minimum of two appropriately authorized persons, each capable of detecting incorrect and unauthorized procedures with respect to the tasks to be performed and each familiar with established security requirements. (See: dual control, no-lone zone.)

Twofish: A symmetric, 128-bit block cipher with variable key length (128, 192, or 256 bits), developed by Counterpane Labs as a candidate for the AES. (See: Blowfish.)

Type 0 product: (cryptography, U.S. Government) Classified cryptographic equipment endorsed by NSA for use (when appropriately keyed) in electronically distributing bulk keying material.

Type 1 key: (cryptography, U.S. Government) "Generated and distributed under the auspices of NSA for use in a cryptographic device for the protection of classified and sensitive national security information."

Type 1 product: (cryptography, U.S. Government) "Cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. Used to protect systems requiring the most stringent protection mechanisms."

Tutorial: The current definition of this term is less specific than an earlier version: "Classified or controlled cryptographic item endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. Type 1 products contain classified NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions.

Type 2 key: (cryptography, U.S. Government) "Generated and distributed under the auspices of NSA for use in a cryptographic device for the protection of unclassified national security information."

Type 2 product: (cryptography, U.S. Government) "Cryptographic equipment, assembly, or component certified by NSA for encrypting or decrypting sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. Used to protect systems requiring protection mechanisms exceeding best commercial practices including systems used for the protection of unclassified national security information."

Tutorial: The current definition of this term is less specific than an earlier version: "Unclassified cryptographic equipment, assembly, or component, endorsed by the NSA, for use in national security systems as defined in Title 40 U.S.C."

Type 3 key: (cryptography, U.S. Government) "Used in a cryptographic device for the protection of unclassified sensitive information, even if used in a Type 1 or Type 2 product."

Type 3 product: (cryptography, U.S. Government) "Unclassified cryptographic equipment, assembly, or component used, when appropriately keyed, for encrypting or decrypting unclassified sensitive U.S. Government or commercial information, and to protect systems requiring protection mechanisms consistent with standard commercial practices. Developed using established commercial standards and containing NIST approved cryptographic algorithms (modules or successfully evaluated by the National Information Assurance Partnership (NIAP)."

Type 4 key: (cryptography, U.S. Government) "Used by a cryptographic device in support of its Type 4 functionality; i.e., any provision of key that lacks U.S. Government endorsement or oversight."

Type 4 product: (cryptography, U.S. Government) "Unevaluated commercial cryptographic equipment, assemblies, or components that neither NSA nor NIST certify for any Government usage. These products are typically delivered as part of commercial offerings and are commensurate with the vendor's commercial practices. These products may contain either vendor proprietary algorithms, algorithms registered by NIST, or algorithms registered by NIST and published in a FIPS."

UDP: See: User Datagram Protocol.

UDP flood: A denial-of-service attack that takes advantage of (a) one system's UDP test function that generates a series of characters for each packet it receives and (b) another system's UPD test function that echoes any character it receives.

Unauthorized disclosure: A circumstance or event whereby an entity gains access to information for which the entity is not authorized.

Tutorial: This type of threat consequence can be caused by the following types of threat actions: exposure, interception, inference, and intrusion. Some methods of protecting against this consequence include access control, flow control, and inference control. (See: data confidentiality.)

Unauthorized user: (access control) A system entity that accesses a system resource for which the entity has not received an authorization. (See: user. Compare: authorized user, insider, outsider.) Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term is used in many ways and could easily be misunderstood.

Uncertainty: An information-theoretic measure (usually stated as a number of bits) of the minimum amount of plaintext information that needs to be recovered from cipher text to learn the entire plain text that was encrypted. (See: entropy.)

Unclassified: Not classified.

Unencrypted: Not encrypted.

Unforgeable: (cryptography) The property of a cryptographic data structure (i.e., a data structure that is defined using one or more cryptographic functions, e.g., "digital certificate") that makes it computationally infeasible to construct (i.e., compute) an unauthorized but correct value of the structure without having knowledge of one of more keys.

Tutorial: This definition is narrower than general English usage, where "unforgeable" means unable to be fraudulently created or duplicated. In that broader sense, anyone can forge a digital certificate containing any set of data items whatsoever by generating the to-be-signed certificate and signing it with any private key whatsoever. But for PKI purposes, the forged data structure is invalid if it is not signed with the true private key of the claimed issuer; thus, the forgery will be detected when a certificate user uses the true public key of the claimed issuer to verify the signature.

Uniform resource identifier (URI): A type of formatted identifier that encapsulates the name of an Internet object, and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces. Example: HTML uses URIs to identify the target of hyperlinks.

Usage: "A URI can be classified as a locator (see: URL), a name (see: URN), or both. ... Instances of URIs from any given scheme may have the characteristics of names or locators or both, often depending on the persistence and care in the assignment of identifiers by the naming authority.

Uniform resource locator (URL): A URI that describes the access method and location of an information resource object on the Internet. (See: Usage under

"URI". Compare: URN.):

Tutorial: The term URL "refers to the subset of URIs that, besides identifying a resource, provide a means of locating the resource by describing its primary access mechanism (e.g., its network 'location')."

A URL provides explicit instructions on how to access the named object. The part before the colon specifies the access scheme or protocol, and the part after the colon is interpreted according to that access method. Usually, two slashes after the colon indicate the host name of a server (written as a domain name). In an FTP or HTTP URL, the host name is followed by the path name of a file on the server. The last (optional) part of a URL may be either a fragment identifier that indicates a position in the file, or a query string.

Uniform resource name (URN): A URI with the properties of a name. (See: Usage under "URI". Compare: URL.)

Tutorial: The term URN "has been used historically to refer to both URIs under the "urn" scheme, which are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable, and to any other URI with the properties of a name."

Untrusted: See: secondary definition under "trust".

Untrusted process:

1. A system component that is not able to affect the state of system security through incorrect or malicious operation. Example: A component that has its operations confined by a security kernel. (See: trusted process.)
2. A system component that (a) has not been evaluated or examined for adherence to a specified security policy and, therefore, (b) must be assumed to contain logic that might attempt to circumvent system security.

UORA: See: user-PIN ORA.

Update: See: "certificate update" and "key update".

Upgrade: (data security) Increase the classification level of data without changing the information content of the data. (See: classify, downgrade, regrade.)

URI: See: uniform resource identifier.

URL: See: uniform resource locator**.**

URN: See: uniform resource name.

User: See: system user.

Usage: DOCUMENTS that use this term SHOULD state a definition for it because the term is used in many ways and could easily be misunderstood.

User authentication service: A security service that verifies the identity claimed by an entity that attempts to access the system. (See: authentication, user.)

User Datagram Protocol (UDP): An Internet Standard, Transport-Layer protocol that delivers a sequence of datagrams from one computer to another in a computer network. (See: UPD flood.)

Tutorial: UDP assumes that IP is the underlying protocol. UDP enables application programs to send transaction-oriented data to other programs with minimal protocol mechanism. UDP does not provide reliable delivery, flow control, sequencing, or other endto-end service guarantees that TCP does.

User identifier: See: identifier.

User identity: See: identity.

User PIN: (MISSI) One of two PINs that control access to the functions and stored data of a FORTEZZA PC card. Knowledge of the user PIN enables a card user to perform the FORTEZZA functions that are intended for use by an end user. (See: PIN. Compare: SSO PIN.)

User-PIN ORA (UORA): (MISSI) A MISSI organizational RA that operates in a mode in which the ORA performs only the subset of card management functions that are possible with knowledge of the user PIN for a FORTEZZA PC card. (See: no-PIN ORA, SSO-PIN ORA.)

Usurpation: A circumstance or event that results in control of system services or functions by an unauthorized entity. This type of threat consequence can be caused by the following types of threat actions: misappropriation, misuse. (See: access control.)

UTCTime: The ASN.1 data type "UTCTime" contains a calendar date (YYMMDD) and a time to a precision of either one minute (HHMM) or one second (HHMMSS), where the time is either (a) Coordinated Universal Time or (b) the local time followed by an offset that enables Coordinated Universal Time to be calculated. (See: Coordinated Universal Time. Compare: GeneralizedTime.)

Usage: If you care about centuries or millennia, you probably need to use the Generalized-Time data type instead of UTCTime.

V1 certificate: An abbreviation that ambiguously refers to either an "X.509 public-key certificate in version 1 format" or an "X.509 attribute certificate in version 1 format".

Deprecated Usage: DOCUMENTS MAY use this term as an abbreviation of "version 1 X.509 public-key certificate", but only after using the full term at the first instance. Otherwise, the term is ambiguous, because X.509 specifies both v1 public-key certificates and v1 attribute certificates. (See: X.509 attribute certificate, X.509 public-key certificate.)

V1 CRL: Abbreviation of "X.509 CRL in version 1 format".

Usage: DOCUMENTS MAY use this abbreviation, but SHOULD use the full term at its first occurrence and define the abbreviation there.

V2 certificate: Abbreviation of "X.509 public-key certificate in version 2 format".

Usage: DOCUMENTS MAY use this abbreviation, but SHOULD use the full term at its first occurrence and define the abbreviation there.

V2 CRL: Abbreviation of "X.509 CRL in version 2 format".

Usage: DOCUMENTS MAY use this abbreviation, but SHOULD use the full term at its first occurrence and define the abbreviation there.

V3 certificate: Abbreviation of "X.509 public-key certificate in version 3 format".

Usage: DOCUMENTS MAY use this abbreviation, but SHOULD use the full term at its first occurrence and define the abbreviation there.

Valid certificate:

1. A digital certificate that can be validated successfully. (See: validate, verify.)

2. A digital certificate for which the binding of the data items can be trusted.

Valid signature: Synonym for "verified signature".

Deprecated Term: DOCUMENTS SHOULD NOT use this synonym. This Glossary recommends saying "validate the certificate" and "verify the signature"; therefore, it would be inconsistent to say that a signature is "valid". (See: validate, verify.)

Validate:

1. Establish the soundness or correctness of a construct. Example: certificate validation. (See: validate vs. verify.)

2. To officially approve something, sometimes in relation to a standard.

Validate vs. verify:

Usage: To ensure consistency and align with ordinary English usage, DOCUMENTS SHOULD comply with the following two rules:

- Rule 1: Use "validate" when referring to a process intended to establish the soundness or correctness of a construct (e.g., "certificate validation"). (See: validate.)

- Rule 2: Use "verify" when referring to a process intended to test or prove the truth or accuracy of a fact or value (e.g., "authenticate"). (See: verify.)

Tutorial: The Internet security community sometimes uses these two terms inconsistently, especially in a PKI context. Most often, however, we say "verify the signature" but say "validate the certificate". That is, we "verify" atomic truths but "validate" data structures, relationships, and systems that are composed of or depend on verified items. This usage has a basis in Latin: The word "valid" derives from a Latin word that means "strong". Thus, to validate means to check that a construct is sound. For example, a certificate user validates a public-key certificate to establish trust in the binding that the certificate asserts between an identity and a key. This can include checking various aspects of the certificate's construction, such as verifying the digital signature on the certificate by performing calculations, verifying that the current time is within the certificate's validity period, and validating a certification path involving additional certificates. The word "verify" derives from a Latin word that means "true". Thus, to verify means to check the truth of an assertion by examining evidence or performing tests. For example, to verify an identity, an authentication process examines identification information that is presented or generated. To validate a certificate, a certificate user verifies the digital signature on the certificate by performing calculations, verifies that the current time is within the certificate's validity period, and may need to validate a certification path involving additional certificates.

Validation: See: validate vs. verify.

Validity period: (PKI) A data item in a digital certificate that specifies the time period for which the binding between data items (especially between the subject name and the public key value in a public-key certificate) is valid, except if the certificate appears on a CRL or the key appears on a CKL. (See: cryptoperiod, key lifetime.)

Value-added network: A computer network or subnetwork (usually a commercial enterprise) that transmits, receives, and stores EDI transactions on behalf of its users.

Tutorial: A VAN may also provide additional services, ranging from EDI format translation, to EDI-to-FAX conversion, to integrated business systems.

VAN: See: value-added network.

Verification:

1. (authentication) The process of examining information to establish the truth of a claimed fact or value. (See: validate vs. verify, verify. Compare: authentication.)
2. (COMPUSEC) The process of comparing two levels of system specification for proper correspondence, such as comparing a security model with a top-level specification, a top-level specification with source code, or source code with object code.

Verified design: See: TCSEC Class A1.

Verify: To test or prove the truth or accuracy of a fact or value. (See: validate vs. verify, verification. Compare: authenticate.)

Vet: (verb) To examine or evaluate thoroughly. (Compare: authenticate, identity proofing, validate, verify.) See: security violation.

Virtual private network (VPN): A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (e.g., the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. (See: tunnel.)

Tutorial: A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the underlying real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by using encrypted tunnels to connect from firewall to firewall across the Internet.

Virus: A self-replicating (and usually hidden) section of computer software (usually malicious logic) that propagates by infecting --i.e., inserting a copy of itself into and becoming part of --another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Visa Cash: A smartcard-based electronic money system that incorporates cryptography and can be used to make payments via the Internet. (See: IOTP.)

Volatile media: Storage media that require an external power supply to maintain stored information. (Compare: non-volatile media, permanent storage.)

VPN: See: virtual private network.

Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. (See: harden.)

Tutorial: A system can have three types of vulnerabilities: (a) vulnerabilities in design or specification; (b) vulnerabilities in implementation; and (c) vulnerabilities in operation and management. Most systems have one or more vulnerabilities, but this does not mean that the systems are too flawed to use. Not every threat results in an attack, and not every attack succeeds. Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use. If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable.

W3: Synonym for WWW.

Deprecated Abbreviation: This abbreviation could be confused with W3C; use "WWW" instead.

W3C: See: World Wide Web Consortium.

War dialer: (slang) A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break the systems.

Deprecated Usage: DOCUMENTs that use this term SHOULD state a definition for it because the term could confuse international readers.

Wassenaar Arrangement: The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a global, multilateral agreement approved by 33 countries in July 1996 to contribute to regional and international security and stability, by promoting information exchange concerning, and greater responsibility in, transfers of arms and dual-use items, thus preventing destabilizing accumulations. (See: International Traffic in Arms Regulations.)

Tutorial: The Arrangement began operations in September 1996 with headquarters in Vienna. The participating countries were Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and United States. Participating countries seek through their national policies to ensure that transfers do not contribute to the development or enhancement of military capabilities that undermine the goals of the arrangement, and are not diverted to support such capabilities. The countries maintain effective export controls for items on the agreed lists, which are reviewed periodically to account for technological developments and experience gained. Through transparency and exchange of views and information, suppliers of arms and dual-use items can develop common understandings of the risks associated with their transfer and assess the scope for coordinating national control policies to combat these risks. Members provide semi-annual notification of arms transfers, covering seven categories derived from the UN Register of Conventional Arms. Members also report transfers or denials of transfers of certain controlled dual-use items. However, the decision to transfer or deny transfer of any item is the sole responsibility of each participating country. All measures undertaken with respect to the arrangement are in accordance with national legislation and policies and are implemented on the basis of national discretion.

Watermarking: See: digital watermarking.

Weak key: In the context of a particular cryptographic algorithm, a key value that provides poor security. (See: strong.)

Example: The DEA has four "weak keys" for which encryption produces the same result as decryption. It also has ten pairs of "semi-weak keys" (a.k.a. "dual keys") for which encryption with one key in the pair produces the same result as decryption with the other key.

Web, Web:

1. (not capitalized) DOCUMENTS SHOULD NOT capitalize "web" when using the term (usually as an adjective) to refer generically to technology -- such as web browsers, web servers, HTTP, and HTML -- that is used in the Web or similar networks.
2. (capitalized) DOCUMENTS SHOULD capitalize "Web" when using the term (as either a noun or an adjective) to refer specifically to the World Wide Web. (Similarly, see: internet.)

   Usage: DOCUMENTS SHOULD NOT use "web" or "Web" in a way that might confuse these definitions with the PGP "web of trust". When using Web as an abbreviation for "World Wide Web", DOCUMENTs SHOULD fully spell out the term at the first instance of usage.

Web of trust: (PGP) A PKI architecture in which each certificate user defines their own trust anchor(s) by depending on personal relationships. (See: trust anchor. Compare: hierarchical PKI, mesh PKI.)

Deprecated Usage: DOCUMENTS SHOULD NOT use this term except with reference to PGP. This term mixes concepts in potentially misleading ways; e.g., this architecture does not depend on World Wide Web technology. Instead of this term, DOCUMENTS MAY use "trustfile PKI". (See: web, Web).

Tutorial: This type of architecture does not usually include public repositories of certificates. Instead, each certificate user builds their own, private repository of trusted public keys by making personal judgments about being able to trust certain people to be holding properly certified keys of other people. It is this set of person-to-person relationships from which the architecture gets its name.

Web server: A software process that runs on a host computer connected to a network and responds to HTTP requests made by client web browsers.

WEP: See: Wired Equivalency Protocol.

Wired Equivalent Privacy (WEP): A cryptographic protocol that is defined in the IEEE 802.11 standard and encapsulates the packets on wireless LANs. Usage: a.k.a. "Wired Equivalency Protocol".

Tutorial: The WEP design, which uses RC4 to encrypt both the plain text and a CRC, has been shown to be flawed in multiple ways; and it also has often suffered from flawed implementation and management.

Wiretapping: An attack that intercepts and accesses information contained in a data flow in a communication system. (See: active wiretapping, end-to-end encryption, passive wiretapping, secondary definition under "interception".)

Usage: Although the term originally referred to making a mechanical connection to an electrical conductor that links two nodes, it is now used to refer to accessing information from any sort of medium used for a link or even from a node, such as a gateway or subnetwork switch.

Tutorial: Wiretapping can be characterized according to intent:

- "Active wiretapping" attempts to alter the data or otherwise affect the flow.
- "Passive wiretapping" only attempts to observe the data flow and gain knowledge of information contained in it.

Work factor:

1a. (COMPUSEC) The estimated amount of effort or time that can be expected to be expended by a potential intruder to penetrate a system, or defeat a particular countermeasure, when using specified amounts of expertise and resources. (See: brute force, impossible, strength.)

1b. (cryptography) The estimated amount of computing power and time needed to break a cryptographic system. (See: brute force, impossible, strength.)

World Wide Web ("the Web", WWW): The global, hypermedia-based collection of information and services that is available on Internet servers and is accessed by browsers using Hypertext Transfer Protocol and other information retrieval mechanisms.

World Wide Web Consortium (W3C): Created in October 1994 to develop and standardize protocols to promote the evolution and interoperability of the Web, and now consisting of hundreds of member organizations (commercial firms, governmental agencies, schools, and others).

Tutorial: W3C Recommendations are developed through a process similar to that of the standards published by other organizations, such as the IETF. The W3 Recommendation Track (i.e., standards track) has four levels of increasing maturity: Working, Candidate Recommendation, Proposed Recommendation, and W3C Recommendation. W3C Recommendations are similar to the standards published by other organizations. (Compare: Internet Standard, ISO.)

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume system resources destructively. (See: mobile code, Morris Worm, virus.)

Wrap:

1. To use cryptography to provide data confidentiality service for keying material. (See: encrypt, wrapping algorithm, wrapping key. Compare: seal, shroud.)
2. To use cryptography to provide data confidentiality service for data in general.

   Deprecated Usage: DOCUMENTS SHOULD NOT use this term with definition 2 because that duplicates the meaning of the more widely understood "encrypt".

Wrapping algorithm: An encryption algorithm that is specifically intended for use in encrypting keys. (See: KEK, wrap.)

Wrapping key: Synonym for "KEK". (See: encrypt. Compare: seal, shroud.)

Write: (security model) A system operation that causes a flow of information from a subject to an object. (See: access mode. Compare: read.)

WWW: See: World Wide Web.

X.400: An ITU-T Recommendation that is one part of a joint ITU-T/ISO multi-part standard (X.400-X.421) that defines the Message Handling Systems

X.500: An ITU-T Recommendation that is one part of a joint ITU-T(ISO multi-part standard (X.500-X.525) that defines the X.500 Directory, a conceptual collection of systems that provide distributed directory capabilities for OSI entities, processes, applications, and services.

Tutorial: The X.500 Directory is structured as a tree (the Directory Information Tree), and information is stored in directory entries. Each entry is a collection of information about one object, and each object has a DN. A directory entry is composed of attributes, each with a type and one or more values. For example, if a PKI uses the Directory to distribute certificates, then the X.509 public-key certificate of an end user is normally stored as a value of an attribute of type "user-Certificate" in the Directory entry that has the DN that is the subject of the certificate.

X.509: An ITU-T Recommendation that defines a framework to provide and support data origin authentication and peer entity authentication, including formats for X.509 public-key certificates, X.509 attribute certificates, and X.509 CRLs. (The ISO equivalent is IS 9498-4.) (See: X.500.)

Tutorial: X.509 describes two "levels" of authentication: "simple authentication" and "strong authentication". It recommends, "While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services.

X.509 attribute certificate: An attribute certificate in the version 1 (v1) format defined by X.509. (The v1 designation for an X.509 attribute certificate is disjoint from the v1

designation for an X.509 public-key certificate, and from the v1 designation for an X.509 CRL.)

Tutorial: An X.509 attribute certificate has a "subject" field, but the attribute certificate is a separate data structure from that subject's public-key certificate. A subject may have multiple attribute certificates associated with each of its public-key certificates, and an attribute certificate may be issued by a Different CA than the one that issued the associated public-key certificate. An X.509 attribute certificate contains a sequence of data items and has a digital signature that is computed from that sequence. Besides the signature, an attribute certificate contains items 1 through 9 listed below:

X.509 certificate: Synonym for "X.509 public-key certificate". Usage: DOCUMENTS MAY use this term as an abbreviation of "X.509 public-key certificate", but only after using the full term at the first instance. Otherwise, the term is ambiguous, because X.509 specifies both public-key certificates and attribute certificates. (See: X.509 attribute certificate, X.509 public-key certificate.)

Deprecated Usage: DOCUMENTs SHOULD NOT use this term as an abbreviation of "X.509 attribute certificate", because the term is much more commonly used to mean "X.509 public-key certificate" and, therefore, is likely to be misunderstood.

X.509 certificate revocation list (CRL): A CRL in one of the formats defined by X.509 -- version 1 (v1) or version 2 (v2). (The v1 and v2 designations for an X.509 CRL are disjoint from the v1 and v2 designations for an X.509 public-key certificate, and from the v1 designation for an X.509 attribute certificate.) (See: certificate revocation.)

Usage: DOCUMENTS SHOULD NOT refer to an X.509 CRL as a digital certificate; however, note that an X.509 CRL does meet this Glossary's definition of "digital certificate". That is, like a digital certificate, an X.509 CRL makes an assertion and is signed by a CA. But instead of binding a key or other attributes to a subject, an X.509 CRL asserts that certain previously issued, X.509 certificates have been revoked.

X.509 public-key certificate: A public-key certificate in one of the formats defined by X.509 -- version 1 (v1), version 2 (v2), or version 3 (v3). (The v1 and v2 designations for an X.509 public-key certificate are disjoint from the v1 and v2 designations for an X.509 CRL, and from the v1 designation for an X.509 attribute certificate.)

X9: See: "Accredited Standards Committee X9" under "ANSI".

XML: See: Extensible Markup Language.

XML-Signature: A W3C Recommendation (i.e., approved standard) that specifies XML syntax and processing rules for creating and representing digital signatures (based on asymmetric cryptography) that can be applied to any digital content (i.e., any data object) including other XML material.

Yellow Book: (slang) Synonym for "Computer Security Requirements: Guidance for Applying the [U.S.] Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments" (See:"first law" under "Courtney's laws".)

Deprecated Term: DOCUMENTs SHOULD NOT use this term as a synonym for that or any other document. Instead, use the full proper name of the document or, in subsequent references, a conventional abbreviation. (See: Deprecated Usage under "Green Book", Rainbow Series.)

Zero-knowledge proof: (cryptography) A proof-of-possession protocol whereby a system entity can prove possession of some information to another entity, without revealing any of that information. (See: proof-of-possession protocol.)

Zeroize:

1. Synonym for "erase". (See: sanitize.) Usage: Particularly with regard to erasing keys that are stored in a cryptographic module.
2. Erase electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.
3. "To remove or eliminate the key from a crypto-equipment or fill device."

Usage: The phrase "zeroize the device" normally is used to mean erasing all keys stored in the device, but sometimes means erasing all keying material in the device, or all cryptographic information in the device, or even all sensitive information in the device.

Zombie: (slang) An Internet host computer that has been surreptitiously penetrated by an intruder that installed malicious daemon software to cause the host to operate as an accomplice in attacking other hosts, particularly in distributed attacks that attempt denial of service through flooding.

Deprecated Usage: Other cultures likely use different metaphorical terms (such as "robot") for this concept, and some use this term for different concepts. Therefore, to avoid international misunderstanding, DOCUMENTS SHOULD NOT use this term. Instead, use "compromised, coopted computer" or other explicitly descriptive terminology. (See: Deprecated Usage under "Green Book".)

Zone of control: (EMSEC) Synonym for "inspectable space". (See: TEMPEST.)