Network Working Group
Request for Comments: 2828
FYI: 36
Category: Informational

R. Shirey
GTE / BBN Technologies

May 2000

Internet Security Glossary

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This Glossary (191 pages of definitions and 13 pages of references) provides abbreviations, explanations, and recommendations for use of information system security terminology. The intent is to improve the comprehensibility of writing that deals with Internet security, particularly Internet Standards documents (ISDs). To avoid confusion, ISDs should use the same term or definition whenever the same concept is mentioned. To improve international understanding, ISDs should use terms in their plainest, dictionary sense. ISDs should use terms established in standards documents and other well-founded publications and should avoid substituting private or newly made-up terms. ISDs should avoid terms that are proprietary or otherwise favor a particular vendor, or that create a bias toward a particular security technology or mechanism versus other, competing techniques that already exist or might be developed in the future.

Table of Contents

1. Introduction

This Glossary provides an internally consistent, complementary set of abbreviations, definitions, explanations, and recommendations for use of terminology related to information system security. The intent of this Glossary is to improve the comprehensibility of Internet Standards documents (ISDs)--i.e., RFCs, Internet-Drafts, and other material produced as part of the Internet Standards Process [R2026]--and of all other Internet material, too. Some non-security terms are included to make the Glossary self-contained, but more complete lists of networking terms are available elsewhere [R1208, R1983].

Some glossaries (e.g., [Raym]) list terms that are not listed here but could be applied to Internet security. However, those terms have not been included in this Glossary because they are not appropriate for ISDs.

This Glossary marks terms and definitions as being either endorsed or deprecated for use in ISDs, but this Glossary is not an Internet standard. The key words "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are intended to be interpreted the same way as in an Internet Standard [R2119], but this guidance represents only the recommendations of this author. However, this Glossary includes reasons for the recommendations--particularly for the SHOULD NOTs--so that readers can judge for themselves whether to follow the recommendations.

This Glossary supports the goals of the Internet Standards Process:

o Clear, Concise, and Easily Understood Documentation

This Glossary seeks to improve comprehensibility of security-related content of ISDs. That requires wording to be clear and understandable, and requires the set of security-related terms and definitions to be consistent and self-supporting. Also, the terminology needs to be uniform across all ISDs; i.e., the same term or definition needs to be used whenever and wherever the same concept is mentioned. Harmonization of existing ISDs need not be done immediately, but it is desirable to correct and standardize the terminology when new versions are issued in the normal course of standards development and evolution.

o Technical Excellence

Just as Internet Standard (STD) protocols should operate effectively, ISDs should use terminology accurately, precisely, and unambiguously to enable Internet Standards to be implemented correctly.

o Prior Implementation and Testing

Just as STD protocols require demonstrated experience and stability before adoption, ISDs need to use well-established language. Using terms in their plainest, dictionary sense (when appropriate) helps to ensure international understanding. ISDs need to avoid using private, made-up terms in place of generally-accepted terms from standards and other publications. ISDs need to avoid substituting new definitions that conflict with established ones. ISDs need to avoid using "cute" synonyms (e.g., see: Green Book); no matter how popular a nickname may be in one community, it is likely to cause confusion in another.

o Openness, Fairness, and Timeliness

ISDs need to avoid terms that are proprietary or otherwise favor a particular vendor, or that create a bias toward a particular security technology or mechanism over other, competing techniques that already exist or might be developed in the future. The set of terminology used across the set of ISDs needs to be flexible and adaptable as the state of Internet security art evolves.

2. Explanation of Paragraph Markings

Section 3 marks terms and definitions as follows:

o Capitalization: Only terms that are proper nouns are capitalized.

o Paragraph Marking: Definitions and explanations are stated in paragraphs that are marked as follows:

- "I" identifies a RECOMMENDED Internet definition.
- "N" identifies a RECOMMENDED non-Internet definition.
- "O" identifies a definition that is not recommended as the first choice for Internet documents but is something that authors of Internet documents need to know.
- "D" identifies a term or definition that SHOULD NOT be used in Internet documents.
- "C" identifies commentary or additional usage guidance.

The rest of Section 2 further explains these five markings.

2.1 Recommended Terms with an Internet Basis ("I")

The paragraph marking "I" (as opposed to "O") indicates a definition that SHOULD be the first choice for use in ISDs. Most terms and definitions of this type MAY be used in ISDs; however, some "I" definitions are accompanied by a "D" paragraph that recommends against using the term. Also, some "I" definitions are preceded by an indication of a contextual usage limitation (e.g., see: certification), and ISDs should not the term and definition outside that context

An "I" (as opposed to an "N") also indicates that the definition has an Internet basis. That is, either the Internet Standards Process is authoritative for the term, or the term is sufficiently generic that this Glossary can freely state a definition without contradicting a non-Internet authority (e.g., see: attack).

Many terms with "I" definitions are proper nouns (e.g., see: Internet Protocol). For such terms, the "I" definition is intended only to provide basic information; the authoritative definition is found elsewhere.

For a proper noun identified as an "Internet protocol", please refer to the current edition of "Internet Official Protocol Standards" (STD 1) for the standardization state and status of the protocol.

2.2 Recommended Terms with a Non-Internet Basis ("N")

The paragraph marking "N" (as opposed to "O") indicates a definition that SHOULD be the first choice for the term, if the term is used at all in Internet documents. Terms and definitions of this type MAY be used in Internet documents (e.g., see: X.509 public-key certificate).

However, an "N" (as opposed to an "I") also indicates a definition that has a non-Internet basis or origin. Many such definitions are preceded by an indication of a contextual usage limitation, and this Glossary's endorsement does not apply outside that context. Also, some contexts are rarely if ever expected to occur in a Internet document (e.g., see: baggage). In those cases, the listing exists to make Internet authors aware of the non-Internet usage so that they can avoid conflicts with non-Internet documents.

Many terms with "N" definitions are proper nouns (e.g., see: Computer Security Objects Register). For such terms, the "N" definition is intended only to provide basic information; the authoritative definition is found elsewhere.

2.3 Other Definitions ("O")

The paragraph marking "O" indicates a definition that has a non-Internet basis, but indicates that the definition SHOULD NOT be used in ISDs *except* in cases where the term is specifically identified as non-Internet.

For example, an ISD might mention "BCA" (see: brand certification authority) or "baggage" as an example to illustrate some concept; in that case, the document should specifically say "SET(trademark) BCA" or "SET(trademark) baggage" and include the definition of the term.

For some terms that have a definition published by a non-Internet authority--government (see: object reuse), industry (see: Secure Data Exchange), national (see: Data Encryption Standard), or international (see: data confidentiality)--this Glossary marks the definition "N", recommending its use in Internet documents. In other cases, the non-Internet definition of a term is inadequate or inappropriate for ISDs. For example, it may be narrow or outdated, or it may need clarification by substituting more careful or more explanatory wording using other terms that are defined in this Glossary. In those cases, this Glossary marks the tern "O" and provides an "I" definition (or sometimes a different "N" definition), which precedes and supersedes the definition marked "O".

In most of the cases where this Glossary provides a definition to supersede one from a non-Internet standard, the substitute is intended to subsume the meaning of the superseded "O" definition and not conflict with it. For the term "security service", for example, the "O" definition deals narrowly with only communication services provided by layers in the OSI model and is inadequate for the full range of ISD usage; the "I" definition can be used in more situations and for more kinds of service. However, the "O" definition is also provided here so that ISD authors will be aware of the context in which the term is used more narrowly.

When making substitutions, this Glossary attempts to use understandable English that does not contradict any non-Internet authority. Still, terminology differs between the standards of the American Bar Association, OSI, SET, the U.S. Department of Defense, and other authorities, and this Glossary probably is not exactly aligned with all of them.

2.4 Deprecated Terms, Definitions, and Uses ("D")

If this Glossary recommends that a term or definition SHOULD NOT be used in ISDs, then either the definition has the paragraph marking "D", or the restriction is stated in a "D" paragraph that immediately follows the term or definition.

2.5 Commentary and Additional Guidance ("C")

The paragraph marking "C" identifies text that is advisory or tutorial. This text MAY be reused in other Internet documents. This text is not intended to be authoritative, but is provided to clarify the definitions and to enhance this Glossary so that Internet security novices can use it as a tutorial.

3. Definitions

Note: Each acronym or other abbreviation (except items of common English usage, such as "e.g.", "etc.", "i.e.", "vol.", "pp.", "U.S.") that is used in this Glossary, either in a definition or as a subpart of a defined term, is also defined in this Glossary.

$ 3DES
See: triple DES.

$ *-property
(N) (Pronounced "star property".) See: "confinement property" under Bell-LaPadula Model.

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

$ Abstract Syntax Notation One (ASN.1)
(N) A standard for describing data objects. [X680]

(C) OSI standards use ASN.1 to specify data formats for protocols. OSI defines functionality in layers. Information objects at higher layers are abstractly defined to be implemented with objects at lower layers. A higher layer may define transfers of abstract objects between computers, and a lower layer may define transfers concretely as strings of bits. Syntax is needed to define abstract objects, and encoding rules are needed to transform between abstract objects and bit strings. (See: Basic Encoding Rules.)

(C) In ASN.1, formal names are written without spaces, and separate words in a name are indicated by capitalizing the first letter of each word except the first word. For example, the name of a CRL is "certificateRevocationList".

$ ACC
See: access control center.

$ access
(I) The ability and means to communicate with or otherwise interact with a system in order to use system resources to either handle information or gain knowledge of the information the system contains.

(O) "A specific type of interaction between a subject and an object that results in the flow of information from one to the other." [NCS04]

(C) In this Glossary, "access" is intended to cover any ability to communicate with a system, including one-way communication in either direction. In actual practice, however, entities outside a security perimeter that can receive output from the system but cannot provide input or otherwise directly interact with the system, might be treated as not having "access" and, therefore, be exempt from security policy requirements, such as the need for a security clearance.

$ access control
(I) Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities

(users, programs, processes, or other systems) according to that policy. (See: access, access control service.)

(O) "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner." [I7498 Part 2]

$ access control center (ACC)
(I) A computer containing a database with entries that define a security policy for an access control service.

(C) An ACC is sometimes used in conjunction with a key center to implement access control in a key distribution system for symmetric cryptography.

$ access control list (ACL)
(I) A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resource. (See: capability.)

$ access control service
(I) A security service that protects against a system entity using a system resource in a way not authorized by the system's security policy; in short, protection of system resources against unauthorized access. (See: access control, discretionary access control, identity-based security policy, mandatory access control, rule-based security policy.)

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

$ access mode
(I) A distinct type of data processing operation--e.g., read, write, append, or execute--that a subject can potentially perform on an object in a computer system.

$ accountability
(I) The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions. (See: audit service.)

(C) Accountability permits detection and subsequent investigation of security breaches.

$ accredit
$ accreditation
(I) An administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. [FP102] (See: certification.)

(C) An accreditation is usually based on a technical certification of the system's security mechanisms. The terms "certification" and "accreditation" are used more in the U.S. Department of Defense and other government agencies than in commercial organizations. However, the concepts apply any place where managers are required to deal with and accept responsibility for security risks. The American Bar Association is developing accreditation criteria for CAs.

$ ACL
See: access control list.

$ acquirer
(N) SET usage: "The financial institution that establishes an account with a merchant and processes payment card authorizations and payments." [SET1]

(O) "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." [SET2]

$ active attack
See: (secondary definition under) attack.

$ active wiretapping
See: (secondary definition under) wiretapping.

$ add-on security
(I) "The retrofitting of protection mechanisms, implemented by hardware or software, after the [automatic data processing] system has become operational." [FP039]

$ administrative security
(I) Management procedures and constraints to prevent unauthorized access to a system. (See: security architecture.)

(O) "The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data." [FP039]

(C) Examples include clear delineation and separation of duties, and configuration control.

$ Advanced Encryption Standard (AES)
(N) A future FIPS publication being developed by NIST to succeed DES. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm, available royalty-free worldwide.

$ adversary
(I) An entity that attacks, or is a threat to, a system.

$ aggregation
(I) A circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it.

$ AH
See: Authentication Header

$ algorithm
(I) 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
(I) A name that an entity uses in place of its real name, usually for the purpose of either anonymity or deception.

$ American National Standards Institute (ANSI)
(N) A private, not-for-profit association of users, manufacturers, and other organizations, that administers U.S. private sector voluntary standards.

(C) ANSI is the sole U.S. representative to the two major non-treaty international standards organizations, ISO and, via the U.S. National Committee (USNC), the International Electrotechnical Commission (IEC).

$ anonymous
(I) The condition of having a name that is unknown or concealed. (See: anonymous login.)

(C) 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 an account number. Parties to a transaction can thus remain relatively anonymous, but can also accept the transaction

as legitimate. Real names of the parties cannot be easily determined by observers of the transaction, 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.

$ anonymous login
(I) An access control feature (or, rather, an access control weakness) in many Internet hosts that enables users to gain access to general-purpose or public services and resources on a host (such as allowing any user to transfer data using File Transfer Protocol) without having a pre-established, user-specific account (i.e., user name and secret password).

(C) 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.

$ APOP
See: POP3 APOP.

$ archive
(I) (1.) 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. (See: backup.) (2.) Verb: To store data in such a way. (See: back up.)

(C) 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
(N) Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the U.S. Government, led to the development of today’s Internet, and was decommissioned in June 1990.

$ ASN.1
See: Abstract Syntax Notation One.

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

$ assurance
(I) (1.) An attribute of an information system that provides grounds for having confidence that the system operates such that the system security policy is enforced. (2.) A procedure that ensures a system is developed and operated as intended by the system's security policy.

$ assurance level
(I) Evaluation usage: A specific level on a hierarchical scale representing successively increased confidence that a target of evaluation adequately fulfills the requirements. (E.g., see: TCSEC.)

$ asymmetric cryptography
(I) A modern branch of cryptography (popularly known as "public-key cryptography") in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm. (See: key pair.)

(C) Asymmetric algorithms have key management advantages over equivalently strong symmetric ones. First, one key of the pair does not need to be known by anyone but its owner; so it can more easily be kept secret. Second, although the other key of the pair is shared by all entities that use the algorithm, that key does not need to be kept secret from other, non-using entities; so the key distribution part of key management can be done more easily.

(C) For encryption: In an asymmetric encryption algorithm (e.g., see: 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.

(C) For signature: In an asymmetric digital signature algorithm (e.g., see: 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.

(C) For key agreement: In an asymmetric key agreement algorithm (e.g., see: Diffie-Hellman), Alice and Bob each send their own public key to the other person. Then each uses their own private key and the other's public key to compute the new key value.

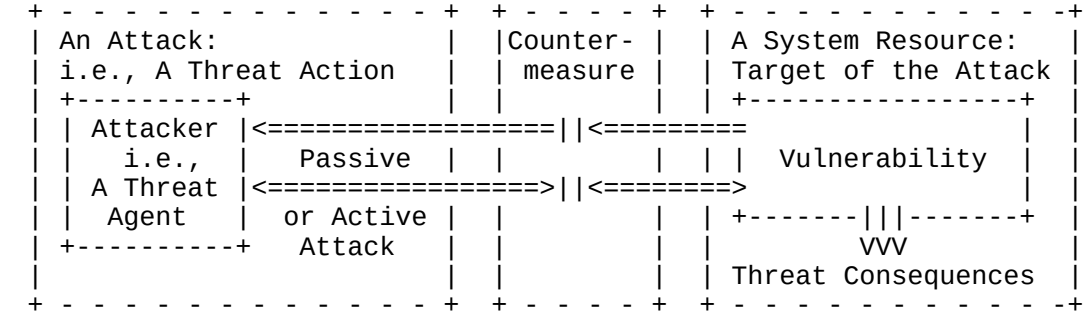
$ attack

(I) An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. (See: penetration, violation, vulnerability.)

- Active vs. passive: An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.)

- Insider vs. outsider: An "inside attack" is an attack 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 those who granted the authorization. An "outside attack" is initiated from outside the 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.

(C) The term "attack" relates to some other basic security terms as shown in the following diagram:



$ attribute authority

(I) A CA that issues attribute certificates.

(O) "An authority, trusted by the verifier to delegate privilege, which issues attribute certificates." [FPDAM]

$ attribute certificate
(I) 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. [X509]

(O) "A set of attributes of a user together with some other information, rendered unforgeable by the digital signature created using the private key of the CA which issued it." [X509]

(O) "A data structure that includes some attribute values and identification information about the owner of the attribute certificate, all digitally signed by an Attribute Authority. This authority's signature serves as the guarantee of the binding between the attributes and their owner." [FPDAM]

(C) A public-key certificate binds a subject name to a public key value, along with information needed to perform certain cryptographic functions. 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.

(C) 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 service
(I) 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.

$ authentic signature
(I) A signature (particularly a digital signature) that can be trusted because it can be verified. (See: validate vs. verify.)

$ authenticate
(I) Verify (i.e., establish the truth of) an identity claimed by or for a system entity. (See: authentication.)

(D) In general English usage, this term usually means "to prove genuine" (e.g., an art expert authenticates a Michelangelo painting). But the recommended definition carries a much narrower meaning. For example, to be precise, an ISD SHOULD NOT say "the host authenticates each received datagram". Instead, the ISD SHOULD say "the host authenticates the origin of each received datagram". In most cases, we also can say "and verifies the datagram's integrity", because that is usually implied. (See: ("relationship between data integrity service and authentication services" under) data integrity service.)

(D) ISDs SHOULD NOT talk about authenticating a digital signature or digital certificate. Instead, we "sign" and then "verify" digital signatures, and we "issue" and then "validate" digital certificates. (See: validate vs. verify.)

$ authentication
(I) The process of verifying an identity claimed by or for a system entity. (See: authenticate, authentication exchange, authentication information, credential, data origin authentication, peer entity authentication.)

(C) An authentication process consists of two steps:

1. Identification step: Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)

2. Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier. (See: verification.)

(C) See: ("relationship between data integrity service and authentication services" under) data integrity service.

$ authentication code
(D) ISDs SHOULD NOT use this term as a synonym for any form of checksum, whether cryptographic or not. The word "authentication" is misleading because the mechanism involved usually serves a data integrity function rather than an authentication function, and the word "code" is misleading because it implies that either encoding or encryption is involved or that the term refers to computer software. (See: message authentication code.)

$ authentication exchange
(I) A mechanism to verify the identity of an entity by means of information exchange.

(O) "A mechanism intended to ensure the identity of an entity by means of information exchange." [I7498 Part 2]

$ Authentication Header (AH)
(I) An Internet IPsec protocol [R2402] designed to provide connectionless data integrity service and data origin authentication service for IP datagrams, and (optionally) to provide protection against replay attacks.

(C) Replay protection may be selected by the receiver when a security association is established. AH authenticates upper-layer protocol data units and as much of 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.

(C) AH may be used alone, or in combination with the IPsec ESP protocol, 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 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
(I) Information used to verify an identity claimed by or for an entity. (See: authentication, credential.)

(C) Authentication information may exist as, or be derived from, one of the following:

- Something the entity knows. (See: password).
- Something the entity possesses. (See: token.)
- Something the entity is. (See: biometric authentication.)

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

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

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

$ authority
(D) "An entity, responsible for the issuance of certificates." [FPDAM]

(C) ISDs SHOULD NOT use this term as a synonym for AA, CA, RA, ORA, or similar terms, because it may cause confusion. Instead, use the full term at the first instance of usage and then, if it is necessary to shorten text, use the style of abbreviation defined in this Glossary.

(C) ISDs SHOULD NOT use this definition for any PKI entity, because the definition is ambiguous with regard to whether the entity actually issues certificates (e.g., attribute authority or certification authority) or just has accountability for processes that precede or follow signing (e.g., registration authority). (See: issue.)

$ authority certificate
(D) "A certificate issued to an authority (e.g. either to a certification authority or to an attribute authority)." [FPDAM] (See: authority.)

(C) ISDs SHOULD NOT use this term or definition because they are ambiguous with regard to which specific types of PKI entities they address.

$ authority revocation list (ARL)
(I) A data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, X.509 authority revocation list.)

(O) "A revocation list containing a list of public-key certificates issued to authorities, which are no longer considered valid by the certificate issuer." [FPDAM]

$ authorization
$ authorize
(I) (1.) An "authorization" is a right or a permission that is granted to a system entity to access a system resource. (2.) An "authorization process" is a procedure for granting such rights. (3.) To "authorize" means to grant such a right or permission. (See: privilege.)

(O) SET usage: "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.)" [SET2]

$ automated information system
(I) An organized assembly of resources and procedures--i.e., computing and communications equipment and services, with their supporting facilities and personnel--that collect, record, process, store, transport, retrieve, or display information to accomplish a specified set of functions.

$ availability
(I) The property of a system or a system resource being accessible and usable 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, reliability, survivability.)

(O) "The property of being accessible and usable upon demand by an authorized entity." [I7498 Part 2]

$ availability service
(I) A security service that protects a system to ensure its availability.

(C) 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.

$ back door
(I) A hardware or software mechanism that (a) provides access to a system and its resources by other than the usual procedure, (b) was deliberately left in place by the system's designers or maintainers, and (c) usually is not publicly known. (See: trap door.)

(C) For example, a way to access a computer other than through a normal login. Such access paths do not necessarily have malicious intent; e.g., operating systems sometimes are shipped by the manufacturer with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers. (See: trap door.)

$ back up vs. backup
(I) Verb "back up": To store data for the purpose of creating a backup copy. (See: archive.)

(I) Noun/adjective "backup": (1.) A reserve copy of data that is stored separately from the original, for use if the original becomes lost or damaged. (See: archive.) (2.) Alternate means to permit performance of system functions despite a disaster to system resources. (See: contingency plan.)

$ baggage
(D) ISDs SHOULD NOT use this term to describe a data element except when stated as "SET(trademark) baggage" with the following meaning:

(O) SET usage: An "opaque encrypted tuple, which is included in a SET message but appended as external data to the PKCS encapsulated data. This avoids superencryption of the previously encrypted tuple, but guarantees linkage with the PKCS portion of the message." [SET2]

$ bandwidth
(I) Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

$ bank identification number (BIN)
(N) The digits of a credit card number that identify the issuing bank. (See: primary account number.)

(O) SET usage: The first six digits of a primary account number.

$ Basic Encoding Rules (BER)
(I) A standard for representing ASN.1 data types as strings of octets. [X690] (See: Distinguished Encoding Rules.)

$ bastion host
(I) 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 hosts) in the network that can be directly accessed from networks on the other side of the firewall.

(C) 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.

$ BCA
See: brand certification authority.

$ BCI
See: brand CRL identifier.

$ Bell-LaPadula Model
(N) A formal, mathematical, state-transition model of security policy for multilevel-secure computer systems. [Bell]

(C) The model separates computer system elements into a set of subjects and a set of 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.

(C) In this model, a multilevel-secure system satisfies several rules, including the following:

- "Confinement property" (also called "*-property", pronounced "star property"): A subject has write access to an object only if classification of the object dominates the clearance of the subject.

- "Simple security property": A subject has read access to an object only if the clearance of the subject dominates the classification of the object.

- "Tranquillity property": The classification of an object does not change while the object is being processed by the system.

$ BER
See: Basic Encoding Rules.

$ beyond A1
(O) (1.) Formally, a level of security assurance that is beyond the highest level of criteria specified by the TCSEC. (2.) Informally, a level of trust so high that it cannot be provided or verified by currently available assurance methods, and particularly not by currently available formal methods.

$ BIN
See: bank identification number.

$ bind
(I) To inseparably associate by applying some mechanism, such as when a CA uses a digital signature to bind together a subject and a public key in a public-key certificate.

$ biometric authentication
(I) A method of generating authentication information for a person by digitizing measurements of a physical characteristic, such as a fingerprint, a hand shape, a retina pattern, a speech pattern (voiceprint), or handwriting.

$ bit
(I) The smallest unit of information storage; a contraction of the term "binary digit"; one of two symbols--"0" (zero) and "1" (one) --that are used to represent binary numbers.

$ BLACK
(I) Designation for information system equipment or facilities that handle (and for data that contains) only ciphertext (or, depending on the context, only unclassified information), and for such data itself. This term derives from U.S. Government COMSEC terminology. (See: RED, RED/BLACK separation.)

$ block cipher
(I) An encryption algorithm that breaks plaintext into fixed-size segments and uses the same key to transform each plaintext segment into a fixed-size segment of ciphertext. (See: mode, stream cipher.)

(C) For example, Blowfish, DEA, IDEA, RC2, and SKIPJACK. However, a block cipher can be adapted to have a different external interface, such as that of a stream cipher, by using a mode of operation to "package" the basic algorithm.

$ Blowfish
(N) 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. [Schn]

$ brand
(I) A distinctive mark or name that identifies a product or business entity.

(O) SET usage: The name of a payment card. 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. [SET1]

$ brand certification authority (BCA)
(O) SET usage: A CA owned by a payment card brand, such as MasterCard, Visa, or American Express. [SET2] (See: certification hierarchy, SET.)

$ brand CRL identifier (BCI)
(O) SET usage: 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. [SET2]

$ break
(I) Cryptographic usage: 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. (This term applies to encrypted data or, more generally, to a cryptographic algorithm or cryptographic system.)

$ bridge
(I) A computer that is a gateway between two networks (usually two LANs) at OSI layer 2. (See: router.)

$ British Standard 7799
(N) Part 1 is a standard code of practice and provides guidance on how to secure an information system. Part 2 specifies the management framework, objectives, and control requirements for information security management systems [B7799]. The certification scheme works like ISO 9000. It is in use in the UK, the Netherlands, Australia, and New Zealand and might be proposed as an ISO standard or adapted to be part of the Common Criteria.

$ browser
(I) An client computer program that can retrieve and display information from servers on the World Wide Web.

(C) For example, Netscape's Navigator and Communicator, and Microsoft's Explorer.

$ brute force
(I) A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

(C) For example, for ciphertext where the analyst already knows the decryption algorithm, a brute force technique to finding the original plaintext is to decrypt the message with every possible key.

$ BS7799
See: British Standard 7799.

$ byte
(I) 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. (See: octet.)

(C) Larger than a "bit", but smaller than a "word". Although "byte" almost always means "octet" today, bytes had other sizes (e.g., six bits, nine bits) in earlier computer architectures.

$ CA
See: certification authority.

$ CA certificate
(I) "A [digital] certificate for one CA issued by another CA." [X509]

(C) That is, a digital certificate whose holder is able to issue digital certificates. A v3 X.509 public-key certificate may have a "basicConstraints" extension containing a "cA" value that specifically "indicates whether or not the public key may be used to verify certificate signatures."

$ call back
(I) An authentication technique for terminals that remotely access a computer via telephone lines. The host system disconnects the caller and then calls back on a telephone number that was previously authorized for that terminal.

$ capability
(I) A token, usually an unforgeable data value (sometimes called a "ticket") 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 named or indicated by the token. (See: access control list, credential, digital certificate.)

(C) This concept can be implemented as a digital certificate. (See: attribute certificate.)

$ CAPI
See: cryptographic application programming interface.

$ CAPSTONE chip
(N) An integrated circuit (the Mykotronx, Inc. MYK-82) with a Type II cryptographic processor that implements SKIPJACK, KEA, DSA, SHA, and basic mathematical functions to support asymmetric cryptography, and includes the key escrow feature of the CLIPPER chip. (See: FORTEZZA card.)

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

$ card backup
See: token backup.

$ card copy
See: token copy.

$ card restore
See: token restore.

$ cardholder
(I) An entity that has been issued a card.

(O) SET usage: "The holder of a valid payment card account and user of software supporting electronic commerce." [SET2] 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. [SET1]

$ cardholder certificate
(O) SET usage: 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. [SET1]

$ cardholder certification authority (CCA)
(O) SET usage: 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. [SET2]

$ CAST
(N) A design procedure for symmetric encryption algorithms, and a resulting family of algorithms, invented by C.A. (Carlisle Adams) and S.T. (Stafford Tavares). [R2144, R2612]

$ category
(I) A grouping of sensitive information items to which a non-hierarchical restrictive security label is applied to increase protection of the data. (See: compartment.)

$ CAW
See: certification authority workstation.

$ CBC
See: cipher block chaining.

$ CCA
See: cardholder certification authority.

$ CCITT
(N) Acronym for French translation of International Telephone and Telegraph Consultative Committee. Now renamed ITU-T.

$ CERT
See: computer emergency response team.

$ certificate
(I) General English usage: A document that attests to the truth of something or the ownership of something.

(C) Security usage: See: capability, digital certificate.

(C) PKI usage: See: attribute certificate, public-key certificate.

$ certificate authority
(D) ISDs SHOULD NOT use this term because it looks like sloppy use of "certification authority", which is the term standardized by X.509.

$ certificate chain
(D) ISDs SHOULD NOT use this term because it duplicates the meaning of a standardized term. Instead, use "certification path".

$ certificate chain validation
(D) ISDs SHOULD NOT use this term because 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
(I) 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
(I) The event that occurs when a certificate ceases to be valid because its assigned lifetime has been exceeded. (See: certificate revocation, validity period.)

$ certificate extension
See: extension.

$ certificate holder
(D) ISDs SHOULD NOT use this term as a synonym for the subject of a digital certificate because the term is potentially ambiguous. For example, the term could also refer to a system entity, such as a repository, that simply has possession of a copy of the certificate. (See: certificate owner.)

$ certificate management
(I) The functions that a CA may perform during the life cycle 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 owner
(D) ISDs SHOULD NOT use this term as a synonym for the subject of a digital certificate because the term is potentially ambiguous. For example, the term could also refer to a system entity, such as a corporation, that has acquired a certificate to operate some other entity, such as a Web server. (See: certificate holder.)

$ certificate policy
(I) "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." [X509] (See: certification practice statement.)

(C) A certificate policy can help a certificate user 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 goods within a given price range." [R2527]

(C) 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.

(C) SET usage: Every 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
(I) Information that pertains to a certificate policy and is included in a "certificatePolicies" extension in a v3 X.509 public-key certificate.

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

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

(C) 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".

(O) MISSI usage: To rekey a MISSI X.509 public-key certificate means that the issuing authority creates a new certificate that is identical to the old one, except the new one has a new, different KEA key; or a new, different DSS key; or 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
(I) The act or process by which the validity of the data binding asserted by an existing public-key certificate is extended in time by issuing a new certificate. (See: certificate rekey, certificate update.)

(C) 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
(D) ISDs SHOULD NOT use this term because it looks like imprecise use of a term standardized by PKCS #10 and used in PKIX. Instead, use the standard term, "certification request".

$ certificate revocation
(I) The event that occurs when a CA declares that a previously valid digital certificate issued by that CA has become invalid; usually stated with a revocation date.

(C) 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 before certificate expiration.

$ certificate revocation list (CRL)
(I) 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, X.509 certificate revocation list.)

(O) "A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. After a certificate appears on a CRL, it is deleted from a subsequent CRL after the certificate's expiry. CRLs may be used to identify revoked public-key certificates or attribute certificates and may represent revocation of certificates issued to authorities or to users. The term CRL is also commonly used as a generic term applying to all the different types of revocation lists, including CRLs, ARLs, ACRLs, etc." [FPDAM]

$ certificate revocation tree
(I) A mechanism for distributing notice 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
(I) 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.

(O) "An integer value, unique within the issuing CA, which is unambiguously associated with a certificate issued by that CA." [X509]

$ certificate status responder
(N) FPKI usage: A trusted on-line server that acts for a CA to provide authenticated certificate status information to certificate users. [FPKI] Offers an alternative to issuing a CRL, but is not supported in X.509. (See: certificate revocation tree.)

$ certificate update
(I) 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.)

(C) 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
(I) A system entity that depends on the validity of information (such as another entity’s public key value) provided by a digital certificate. (See: relying party.)

(O) "An entity that needs to know, with certainty, the public key of another entity." [X509]

(C) The system entity may be a human being or an organization, or a device or process under the control of a human or an organization.

(D) ISDs SHOULD NOT use this term as a synonym for the "subject" of a certificate.

$ certificate validation
(I) 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.)

(O) "The process of ensuring that a certificate is valid including possibly the construction and processing of a certification path, and ensuring that all certificates in that path have not expired or been revoked." [FPDAM]

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

- Checks the signature: Employs 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 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 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. (CRLs themselves require a similar validation process.)

$ certification

(I) Information system usage: Technical evaluation (usually made in support of an accreditation action) of an information system's security features and other safeguards to establish the extent to which the system's design and implementation meet specified security requirements. [FP102] (See: accreditation.)

(I) Digital certificate usage: The act or process of vouching for the truth and accuracy of the binding between data items in a certificate. (See: certify.)

(I) Public key usage: 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. In addition to binding a key to a name, a public-key certificate may bind those items to other restrictive or explanatory data items. (See: X.509 public-key certificate.)

(O) SET usage: "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." [SET2]

$ certification authority (CA)
(I) An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

(O) "An authority trusted by one or more users to create and assign certificates. Optionally, the certification authority may create the user's keys." [X509]

(C) Certificate users depend on the validity of information provided by a certificate. Thus, a CA should be someone that certificate users trust, and 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 life cycle of key pairs associated with the certificates (see: key management).

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

$ certification hierarchy
(I) A tree-structured (loop-free) topology of relationships among CAs and the entities to whom the CAs issue public-key certificates. (See: hierarchical PKI.)

(C) 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 of the hierarchy issue certificates only to non-CA entities, called "end 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.

(O) MISSI usage: A MISSI certification hierarchy 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".

(O) PEM usage: A PEM certification hierarchy has three levels of CAs [R1422]:

- 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".

(O) SET usage: A SET certification hierarchy 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

(I) An ordered sequence of public-key certificates (or a sequence of public-key certificates followed by 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 a certified public key (or certified attributes) of the entity that is the subject of that last certificate. (See: certificate validation, valid certificate.)

(O) "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." [X509, R2527]

(C) The path is the "list of certificates needed to allow a particular user to obtain the public key of another." [X509] The list is "linked" in the sense that the digital signature of each certificate (except 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 owned by the entity that signed.

(C) In the X.509 quotation in the previous "C" paragraph, 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 should be a trusted certificate (it might be a root certificate) or the signature on the first certificate should be verified by a trusted key (it might be a root key), but such trust is defined relative to each user, not absolutely for all users.

$ certification policy
(D) ISDs SHOULD NOT use this term. Instead, use either "certificate policy" or "certification practice statement", depending on what is meant.

$ certification practice statement (CPS)
(I) "A statement of the practices which a certification authority employs in issuing certificates." [ABA96, R2527] (See: certificate policy.)

(C) 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 employs 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. [ABA]

(C) 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 a single CPS may support multiple certificate policies, which may be used for different application purposes or by different user communities. Multiple CAs, each with a different CPS, may support the same certificate policy. [R2527]

$ certification request
(I) A algorithm-independent transaction format, defined by PCKS #10 and used in PKIX, that contains a DN, a public key, and 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. (I) Issue a digital certificate and thus vouch for the truth, accuracy, and binding between data items in the certificate (e.g., see: X.509 public key certificate), such as the identity of the certificate's subject and the ownership of a public key. (See: certification.)

(C) 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. (I) The act by which a CA employs measures to verify the truth, accuracy, and binding between data items in a digital certificate.

(C) A description of the measures used for verification should be included in the CA's CPS.

$ CFB
See: cipher feedback.

$ Challenge Handshake Authentication Protocol (CHAP)
(I) A peer entity authentication method for PPP, using a randomly-generated challenge and requiring a matching response that depends on a cryptographic hash of the challenge and a secret key. [R1994] (See: challenge-response, PAP.)

$ challenge-response
(I) 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.

$ Challenge-Response Authentication Mechanism (CRAM)
(I) IMAP4 usage: 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.)

(C) The server includes a unique timestamp 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 timestamp with a shared secret that is known only to the client and the server.

$ channel
(I) An information transfer path within a system. (See: covert channel.)

$ CHAP
See: Challenge Handshake Authentication Protocol.

$ checksum
(I) 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 the purpose of detecting changes in the data. (See: cyclic redundancy check, data integrity service, error detection code, hash, keyed hash, protected checksum.)

(C) To gain confidence that a data object has not been changed, an entity that later uses the data can compute a checksum and compare it with the checksum that was stored or transmitted with the object.

(C) Computer systems and networks employ 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).

$ chosen-ciphertext attack
(I) A cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected (i.e., dictated) by the analyst.

$ chosen-plaintext attack
(I) A cryptanalysis technique in which the analyst tries to determine the key from knowledge of ciphertext that corresponds to plaintext selected (i.e., dictated) by the analyst.

$ CIAC
See: Computer Incident Advisory Capability.

$ CIK
See: cryptographic ignition key.

$ cipher
(I) A cryptographic algorithm for encryption and decryption.

$ cipher block chaining (CBC)
(I) An block cipher mode that enhances electronic codebook mode by chaining together blocks of ciphertext it produces. [FP081] (See: [R1829], [R2451].)

(C) 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)
(I) An block cipher mode that enhances electronic code book mode by chaining together the blocks of ciphertext it produces and operating on plaintext segments of variable length less than or equal to the block length. [FP081]

(C) This mode operates by using the previously generated ciphertext segment as the algorithm's input (i.e., by "feeding back" the ciphertext) 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 ciphertext segment.

$ ciphertext
(I) 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: cleartext, plaintext.)

(O) "Data produced through the use of encipherment. The semantic content of the resulting data is not available." [I7498 Part 2]

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

$ CIPSO
See: Common IP Security Option.

$ CKL
See: compromised key list.

$ class 2, 3, 4, or 5
(O) U.S. Department of Defense usage: Levels of PKI assurance based on risk and value of information to be protected [DOD3]:

- Class 2: For handling low-value information (unclassified, not mission-critical, or low monetary value) or protection of system-high information in low- to medium-risk environment.

- Class 3: For handling medium-value information in low- to medium-risk environment. Typically requires identification of a system entity as a legal person, rather than merely a member of an organization.

- Class 4: For handling medium- to high-value information in any environment. Typically requires identification of an entity as a legal person, rather than merely a member of an organization, and a cryptographic hardware token for protection of keying material.

- Class 5: For handling high-value information in a high-risk environment.

$ classification
$ classification level
(I) (1.) A grouping of classified information to which a hierarchical, restrictive security label is applied to increase protection of the data. (2.) The level of protection that is required to be applied to that information. (See: security level.)

$ classified
(I) Refers to information (stored or conveyed, in any form) that is formally required by a security policy to be given data confidentiality service and to be marked with a security label (which in some cases might be implicit) to indicate its protected status. (See: unclassified.)

(C) The term is mainly used in government, especially in the military, although the concept underlying the term also applies outside government. In the U.S. Department of Defense, for example, it means information that has been determined pursuant to Executive Order 12958 ("Classified National Security Information", 20 April 1995) or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

$ clean system
(I) A computer system in which the operating system and application system software and files have just been freshly installed from trusted software distribution media.

(C) A clean system is not necessarily in a secure state.

$ clearance
See: security clearance.

$ clearance level
(I) The security level of information to which a security clearance authorizes a person to have access.

$ cleartext
(I) Data in which the semantic information content (i.e., the meaning) is intelligible or is directly available. (See: plaintext.)

(O) "Intelligible data, the semantic content of which is available." [I7498 Part 2]

(D) ISDs SHOULD NOT use this term as a synonym for "plaintext", the input to an encryption operation, because the plaintext input to encryption may itself be ciphertext that was output from another operation. (See: superencryption.)

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

(C) Usually, the requesting entity is a computer process, and it makes the request on behalf of a human user. In some cases, the server may itself be a client of some other server.

$ CLIPPER chip
(N) The Mykotronx, Inc. MYK-82, an integrated microcircuit with a cryptographic processor that implements the SKIPJACK encryption algorithm and supports key escrow. (See: CAPSTONE, Escrowed Encryption Standard.)

(C) The key escrow scheme for a chip involves a SKIPJACK key common to all chips 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
(O) U.S. Department of Defense usage: 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: open security environment.)

$ code
(I) noun: A system of symbols used to represent information, which might originally have some other representation. (See: encode.)

(D) ISDs SHOULD NOT use this term as synonym for the following: (a) "cipher", "hash", or other words that mean "a cryptographic algorithm"; (b) "ciphertext"; or (c) "encrypt", "hash", or other words that refer to applying a cryptographic algorithm.

(D) ISDs SHOULD NOT this word as an abbreviation for the following terms: country code, cyclic redundancy code, Data Authentication Code, error detection code, Message Authentication Code, object code, or source code. To avoid misunderstanding, use the fully qualified term, at least at the point of first usage.

$ color change
(I) In a system that is 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.

$ Common Criteria
$ Common Criteria for Information Technology Security
(N) "The Common Criteria" is a standard for evaluating information technology products and systems, such as operating systems, computer networks, distributed systems, and applications. It states requirements for security functions and for assurance measures. [CCIB]

(C) 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" (FC) 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 2.1 of the Criteria is equivalent to ISO's International Standard 15408 [I15408]. The U.S. Government intends that this standard eventually will supersede both the TCSEC and FIPS PUB 140-1. (See: NIAP.)

(C) 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.

$ Common IP Security Option (CIPSO)
See: (secondary definition under) Internet Protocol Security Option.

$ common name
(I) 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. [X520] (See: ("subject" and "issuer" under) X.509 public-key certificate.)

(C) For example, "Dr. E. F. Moore", "The United Nations", or "12-th Floor Laser Printer".

$ communication security (COMSEC)
(I) 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.

(C) Usually understood to include cryptographic algorithms and key management methods and processes, devices that implement them, and the life cycle management of keying material and devices.

$ community string
(I) A community name in the form of an octet string that serves as a cleartext password in SNMP version 1. [R1157]

$ compartment
(I) A grouping of sensitive information items that require special access controls beyond those normally provided for the basic classification level of the information. (See: category.)

(C) The term is usually understood to include the special handling procedures to be used for the information.

$ compromise
See: data compromise, security compromise.

$ compromised key list (CKL)
(O) MISSI usage: A list that identifies keys for which unauthorized disclosure or alteration may have occurred. (See: compromise.)

(C) A CKL is issued by an 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)
(I) 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.)

(C) For example, the CERT Coordination Center at Carnegie-Mellon University (sometimes called "the" CERT) and the Computer Incident Advisory Capability.

$ Computer Incident Advisory Capability (CIAC)
(N) A computer emergency response team in the U.S. Department of Energy.

$ computer network
(I) A collection of host computers together with the subnetwork or internetwork through which they can exchange data.

(C) 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 security (COMPUSEC)
(I) Measures that implement and assure security services in a computer system, particularly those that assure access control service.

(C) Usually understood to include functions, features, and technical characteristics of computer hardware and software, especially operating systems.

$ computer security incident response team (CSIRT)
(I) An organization "that coordinates and supports the response to security incidents that involve sites within a defined constituency." [R2350] (See: CERT, FIRST, security incident.)

(C) To be considered a CSIRT, an organization must do as follows:

- Provide a (secure) channel for receiving reports about suspected security incidents.
- Provide assistance to members of its constituency in handling the incidents.
- Disseminate incident-related information to its constituency and other involved parties.

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

$ Computer Security Objects Register (CSOR)
(N) 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.

(C) 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) gov(101) csor(3)}.

$ COMSEC
See: communication security.

$ confidentiality
See: data confidentiality.

$ configuration control
(I) The process of regulating changes to hardware, firmware, software, and documentation throughout the development and operational life of a system. (See: administrative security.)

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

$ confinement property
See: (secondary definition under) Bell-LaPadula Model.

$ connectionless data integrity service
(I) A security service that provides data integrity service for an individual IP datagram, by detecting modification of the datagram, without regard to the ordering of the datagram in a stream of datagrams.

(C) A connection-oriented data integrity service would be able to detect lost or reordered datagrams within a stream of datagrams.

$ contingency plan
(I) 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. [NCS04] (See: availability.)

$ controlled security mode
(D) ISDs SHOULD NOT use this term. It was defined in an earlier version of the U.S. Department of Defense policy that regulates system accreditation, but was subsumed by "partitioned security mode" in the current version. [DOD2]

(C) The term refers to a mode of operation of an information system, wherein at least some users with access to the system have neither a security clearance nor a need-to-know for all classified material contained in the system. However, separation and control of users and classified material on the basis, respectively, of clearance and classification level are not essentially under operating system control like they are in "multilevel security mode".

(C) Controlled mode was intended to encourage ingenuity in meeting the security requirements of Defense policy 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 the true "multilevel security mode". This was 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 permitted concurrent access to the system.

$ cookie
(I) access control usage: A synonym for "capability" or "ticket" in an access control system.

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

(I) HTTP usage: 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.

(C) 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.

$ Coordinated Universal Time (UTC)
(N) 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: GeneralizedTime, UTCTime.)

$ copy
See: card copy.

$ correctness integrity
(I) Accuracy and consistency of the information that data values represent, rather than of the data itself. Closely related to issues of accountability and error handling. (See: data integrity, source integrity.)

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

$ countermeasure
(I) An action, device, procedure, or technique that reduces 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.

(C) In an Internet protocol, a countermeasure may take the form of a protocol feature, an element function, or a usage constraint.

$ country code
(I) An identifier that is defined for a nation by ISO. [I3166]

(C) 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.

$ covert channel
(I) A intra-system channel that permits two cooperating entities, without exceeding their access authorizations, to transfer information in a way that violates the system's security policy. (See: channel, out of band.)

(O) "A communications channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy." [NCS04]

(C) 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:

- "Timing channel": A system feature that enable 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.

- "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.

$ CPS
See: certification practice statement.

$ cracker
(I) Someone who tries to break the security of, and gain access to, someone else's system without being invited to do so. (See: hacker and intruder.)

$ CRAM
See: Challenge-Response Authentication Mechanism.

$ CRC
See: cyclic redundancy check.

$ credential(s)
(I) Data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity. (See: authentication information, capability, ticket.)

(O) "Data that is transferred to establish the claimed identity of an entity." [I7498 Part 2]

$ critical
1. (I) "Critical" system resource: A condition of a service or other system resource such that denial of access to (i.e., 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. (See: availability, sensitive.)

2. (N) "Critical" extension: Each extension of an X.509 certificate (or CRL) is marked as being either critical or non-critical. If an extension is critical and a certificate user (or CRL user) does not recognize the extension type or does not implement its semantics, then the user is required to treat the certificate (or CRL) as invalid. If an extension is non-critical, a user that does not recognize or implement that extension type is permitted to ignore the extension and process the rest of the certificate (or CRL).

$ CRL
See: certificate revocation list.

$ CRL distribution point
See: distribution point.

$ CRL extension
See: extension.

$ cross-certificate
See: cross-certification.

$ cross-certification
(I) The act or process by which two CAs each certify a public key of the other, issuing a public-key certificate to that other CA.

(C) Cross-certification enables users to validate each other's certificate when the users are certified under different certification hierarchies.

$ cryptanalysis
(I) The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. (See: cryptology.)

(O) "The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext." [I7498 Part 2]

(C) The "O" definition states the traditional goal of cryptanalysis--convert the ciphertext to plaintext (which usually is cleartext) 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 the "I" definition reflects that. In all cases, however, a cryptanalyst tries to uncover or reproduce someone else's sensitive data, such as cleartext, a key, or an algorithm. The basic cryptanalytic attacks on encryption systems are ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext; and these generalize to the other kinds of cryptography.

$ crypto
(D) Except as part of certain long-established terms listed in this Glossary, ISDs SHOULD NOT use this abbreviated term because it may be misunderstood. Instead, use "cryptography" or "cryptographic".

$ cryptographic algorithm
(I) An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

$ cryptographic application programming interface (CAPI)
(I) The source code formats and procedures through which an application program accesses cryptographic services, which are defined abstractly compared to their actual implementation. For example, see: PKCS #11, [R2628].

$ cryptographic card
(I) A cryptographic token in the form of a smart card or a PC card.

$ cryptographic component
(I) 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)
(I) A physical (usually electronic) token used to store, transport, and protect cryptographic keys. (Sometimes abbreviated as "crypto ignition key".)

(C) A typical use is to divide a split key between a CIK and a cryptographic module, so that it is necessary to combine the two to regenerate a key-encrypting key and thus activate the module and other keys it contains.

$ cryptographic key
(I) Usually shortened to just "key". An input parameter that varies the transformation performed by a cryptographic algorithm.

(O) "A sequence of symbols that controls the operations of encipherment and decipherment." [I7498 Part 2]

(C) If a key value needs to be kept secret, the sequence of symbols (usually bits) that comprise it should be random, or at least pseudo-random, because that makes the key hard for an adversary to guess. (See: cryptanalysis, brute force attack.)

$ Cryptographic Message Syntax (CMS)
(I) A encapsulation syntax for digital signatures, hashes, and encryption of arbitrary messages. [R2630]

(C) CMS was derived 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
(I) 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. [FP140]

$ cryptographic system
(I) A set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context.

(C) This "I" definition covers a wider range of algorithms than the following "O" definition:

(O) "A collection of transformations from plaintext into ciphertext 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." [X509]

$ cryptographic token
(I) A portable, user-controlled, physical device used to store cryptographic information and possibly perform cryptographic functions. (See: cryptographic card, token.)

(C) A smart token may implement some set of cryptographic algorithms and may implement related algorithms and 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
(I) 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.)

(O) "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." [I7498 Part 2]

$ Cryptoki
See: (secondary definition under) PKCS #11.

$ cryptology
(I) The science that includes both cryptography and cryptanalysis, and sometimes is said to include steganography.

$ cryptonet
(I) A group of system entities that share a secret cryptographic key for a symmetric algorithm.

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

(C) A cryptoperiod 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 cryptoperiod involves a tradeoff between the cost of rekeying and the risk of successful cryptanalysis.

(C) Although we deprecate its prefix, this term is long-established in COMPUSEC usage. (See: crypto) In the context of certificates and public keys, "key lifetime" and "validity period" are often used instead.

$ cryptosystem
(D) ISDs SHOULD NOT use this term as an abbreviation for cryptographic system. (For rationale, see: crypto.)

$ CSIRT
See: computer security incident response team.

$ CSOR
See: Computer Security Objects Register.

$ cut-and-paste attack
(I) An active attack on the data integrity of ciphertext, effected by replacing sections of ciphertext with other ciphertext, such that the result appears to decrypt correctly but actually decrypts to plaintext that is forged to the satisfaction of the attacker.

$ cyclic redundancy check (CRC)
(I) Sometimes called "cyclic redundancy code". 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.

$ DAC
See: Data Authentication Code, discretionary access control.

$ DASS
See: Distributed Authentication Security Service.

$ data
(I) Information in a specific physical representation, usually a sequence of symbols that have meaning; especially a representation of information that can be processed or produced by a computer.

$ Data Authentication Algorithm
(N) A keyed hash function equivalent to DES cipher block chaining with IV = 0. [A9009]

(D) ISDs SHOULD NOT use the uncapitalized form of this term as a synonym for other kinds of checksums.

$ data authentication code vs. Data Authentication Code (DAC)
1. (N) Capitalized: "The Data Authentication Code" refers to a U.S. Government standard [FP113] for a checksum that is computed by the Data Authentication Algorithm. (Also known as the ANSI standard Message Authentication Code [A9009].)

2. (D) Not capitalized: ISDs SHOULD NOT use "data authentication code" as a synonym for another kind of checksum, because this term mixes concepts in a potentially misleading way. (See: authentication code.) Instead, use "checksum", "error detection code", "hash", "keyed hash", "Message Authentication Code", or "protected checksum", depending on what is meant.

$ data compromise
(I) A security incident in which information is exposed to potential unauthorized access, such that unauthorized disclosure, alteration, or use of the information may have occurred. (See: compromise.)

$ data confidentiality
(I) "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [I7498 Part 2]. (See: data confidentiality service.)

(D) ISDs SHOULD NOT use this term as a synonym for "privacy", which is a different concept.

$ data confidentiality service
(I) A security service that protects data against unauthorized disclosure. (See: data confidentiality.)

(D) ISDs SHOULD NOT use this term as a synonym for "privacy", which is a different concept.

$ Data Encryption Algorithm (DEA)
(N) A symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard. 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. [FP046] (See: DES, symmetric cryptography.)

(C) This algorithm is usually referred to as "DES". The algorithm has also been adopted in standards outside the Government (e.g., [A3092]).

$ data encryption key (DEK)
(I) A cryptographic key that is used to encipher application data. (See: key-encrypting key.)

$ Data Encryption Standard (DES)
(N) A U.S. Government standard [FP046] that specifies the Data Encryption Algorithm and states policy for using the algorithm to protect unclassified, sensitive data. (See: AES, DEA.)

$ data integrity
(I) The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (See: data integrity service.)

(O) "The property that information has not been modified or destroyed in an unauthorized manner." [I7498 Part 2]

(C) Deals with constancy of and confidence in data values, not with the information that the values represent (see: correctness integrity) or the trustworthiness of the source of the values (see: source integrity).

$ data integrity service
(I) 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.)

(C) 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.

(C) 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 a 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
(I) "The corroboration that the source of data received is as claimed." [I7498 Part 2] (See: authentication.)

$ data origin authentication service
(I) 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.)

(C) 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.

(C) 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.

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

$ data privacy
(D) ISDs SHOULD NOT use this term because it mix concepts in a potentially misleading way. Instead, use either "data confidentiality" or "privacy", depending on what is meant.

$ data security
(I) The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorized.

(C) Both data confidentiality service and data integrity service are needed to achieve data security.

$ datagram
(I) "A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination." [R1983]

$ DEA
See: Data Encryption Algorithm.

$ deception
See: (secondary definition under) threat consequence.

$ decipher
(D) ISDs SHOULD NOT use this term as a synonym for "decrypt", except in special circumstances. (See: (usage discussion under) encryption.)

$ decipherment
(D) ISDs SHOULD NOT use this term as a synonym for "decryption", except in special circumstances. (See: (usage discussion under) encryption.)

$ decode
(I) Convert encoded data back to its original form of representation. (See: decrypt.)

(D) ISDs SHOULD NOT use this term as a synonym for "decrypt", because that would mix concepts in a potentially misleading way.

$ decrypt
(I) Cryptographically restore ciphertext to the plaintext form it had before encryption.

$ decryption
See: (secondary definition under) encryption.

$ dedicated security mode
(I) A mode of operation of an information system, wherein all users have the clearance or authorization, and the need-to-know, for all data handled by the system. In this mode, the system may handle either a single classification level or category of information or a range of levels and categories. [DOD2]

(C) This mode is defined formally in U.S. Department of Defense policy regarding system accreditation, but the term is also used outside the Defense Department and outside the Government.

$ default account
(I) A system login account (usually accessed with a user name and password) that has been predefined in a manufactured system to permit initial access when the system is first put into service.

(C) Sometimes, the default user name and password are the same in each copy of the system. In any case, when the system is put into service, the default password should immediately be changed or the default account should be disabled.

$ degauss
(N) Apply a magnetic field to permanently remove, erase, or clear data from a magnetic storage medium, such as a tape or disk [NCS25]. Reduce magnetic flux density to zero by applying a reversing magnetic field.

$ degausser
(N) An electrical device that can degauss magnetic storage media.

$ DEK
See: data encryption key.

$ delta CRL
(I) A partial CRL that only contains entries for X.509 certificates that have been revoked since the issuance of a prior, base CRL. This method can be used to partition CRLs that become too large and unwieldy.

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

$ DES
See: Data Encryption Standard.

$ dictionary attack
(I) An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.

(C) For example, an attack on an authentication service by trying all possible passwords; or an attack on encryption by encrypting some known plaintext phrase with all possible keys so that the key for any given encrypted message containing that phrase may be obtained by lookup.

$ Diffie-Hellman
(N) A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman [DH76, R2631].

(C) Diffie-Hellman 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.

(C) The difficulty of breaking Diffie-Hellman is considered to be equal to the difficulty of computing discrete logarithms modulo a large prime. The algorithm is described in [R2631] and [Schn]. 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, k, 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. 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
(I) 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. (See: attribute certificate, capability, public-key certificate.)

(D) ISDs SHOULD NOT use this term to refer to a signed CRL or CKL. Although the recommended definition can be interpreted to include those items, the security community does not use the term with those meanings.

$ digital certification
(D) ISDs SHOULD NOT use this term as a synonym for "certification", 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
(I) 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
(I) A digital envelope for a recipient is a combination of (a) encrypted content data (of any kind) and (b) the content encryption key in an encrypted form that has been prepared for the use of the recipient.

(C) In ISDs, this 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 yet widely established.

(C) 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 PCKS #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 and the public key of the intended recipient. In S/MIME, additional methods are defined for conveying the content encryption key.

$ Digital ID(service mark)
(D) ISDs SHOULD NOT use this term as a synonym for "digital certificate" because (a) it is the service mark of a commercial firm, (b) it unnecessarily duplicates the meaning of other, well-established terms, and (c) a certificate is not always used as authentication information. In some contexts, however, it may be useful to explain that the key conveyed in a public-key certificate can be used to verify an identity and, therefore, that the certificate can be thought of as digital identification information. (See: identification information.)

$ digital key
(C) 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
(I) Analogous to a notary public. Provides a trusted date-and-time stamp for a document, so that someone can later prove that the document existed at a point in time. May also verify the signature(s) on a signed document before applying the stamp. (See: notarization.)

$ digital signature
(I) A value computed with a cryptographic algorithm and appended to 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, digitized signature, electronic signature, signer.)

(I) "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." [I7498 Part 2]

(C) Typically, 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.

(C) Some digital signature schemes use a asymmetric encryption algorithm (e.g., see: 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.

(C) Other digital signature schemes (e.g., see: DSS) transform the hash result with an algorithm (e.g., see: 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.

$ Digital Signature Algorithm (DSA)
(N) An asymmetric cryptographic algorithm that produces 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: Digital Signature Standard.)

$ Digital Signature Standard (DSS)
(N) The U.S. Government standard [FP186] that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

$ digital watermarking
(I) 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.

(C) The set of embedded bits (the digital watermark) 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. [ACM]

$ digitized signature
(D) ISDs SHOULD NOT use this term because there is no current consensus on its definition. Although it appears to be used mainly to refer to various forms of digitized images of handwritten signatures, the term should be avoided because it might be confused with "digital signature".

$ directory
$ Directory
See: directory vs. Directory.

$ Directory Access Protocol (DAP)
(N) An OSI protocol [X519] for communication between a Directory User Agent (a client) and a Directory System Agent (a server). (See: Lightweight Directory Access Protocol.)

$ directory vs. Directory
1. (I) Not capitalized: The term "directory" refers generically to a database server or other system that provides information--such as a digital certificate or CRL--about an entity whose name is known.

2. (I) Capitalized: "Directory" refers specifically to the X.500 Directory. (See: repository.)

$ disaster plan
(D) A synonym for "contingency plan". In the interest of consistency, ISDs SHOULD use "contingency plan" instead of "disaster plan".

$ disclosure (i.e., unauthorized disclosure)
See: (secondary definition under) threat consequence.

$ discretionary access control (DAC)
(I) An access control service that enforces a security policy based on the identity of system entities and their authorizations to access system resources. (See: access control list, identity-based security policy, mandatory access control.)

(C) This service is termed "discretionary" because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.

(O) "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." [DOD1]

$ disruption
See: (secondary definition under) threat consequence.

$ Distinguished Encoding Rules (DER)
(N) A subset of the Basic Encoding Rules, which gives exactly one way to represent any ASN.1 value as an octet string [X690].

(C) Since there is more than one way to encode ASN.1 in BER, DER is used in applications in which a unique encoding is needed, such as when a digital signature is computed on an ASN.1 value.

$ distinguished name (DN)
(I) An identifier that uniquely represents an object in the X.500 Directory Information Tree (DIT) [X501]. (See: domain name.)

(C) 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 Authentication Security Service (DASS)
(I) An experimental Internet protocol [R1507] that uses cryptographic mechanisms to provide strong, mutual authentication services in a distributed environment.

$ distribution point
(I) 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 might list the certificate.

(C) A v3 X.509 public-key certificate may have a "cRLDistributionPoints" extension that names places to get CRLs on which the certificate might be listed. 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 (c') contain revocation entries for multiple CAs.

$ DN
See: distinguished name.

$ DNS
See: Domain Name System.

$ DOI
See: Domain of Interpretation.

$ domain
(I) Security usage: An environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources. (See: domain of interpretation, security perimeter.)

(I) Internet usage: That part of the Internet domain name space tree [R1034] that is at or below the name the 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. (See: Domain Name System.)

(O) MISSI usage: The domain of a MISSI CA is the set of MISSI users whose certificates are signed by the CA.

(O) OSI usage: An administrative partition of a complex distributed OSI system.

$ domain name
(I) The style of identifier--a sequence of case-insensitive ASCII labels separated by dots ("bbn.com.")--defined for subtrees in the Internet Domain Name System [R1034] and used in other 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: distinguished name, domain.)

(C) The domain 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). The root's label is the null

string, so a complete domain name properly ends in a dot. The top-level domains, those immediately below the root, include COM, EDU, GOV, INT, MIL, NET, ORG, and two-letter country codes (such as US) from ISO-3166. [R1591] (See: country code.)

$ Domain Name System (DNS)
(I) The main Internet operations database, which is distributed over a collection of servers and used by client software for purposes such as translating a domain name-style host name into an IP address (e.g., "rosslyn.bbn.com" is "192.1.7.10") and locating a host that accepts mail for some mailbox address. [R1034]

(C) 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.

(C) Extensions to the DNS [R2065, R2137, R2536] 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)
(I) IPsec usage: An ISAKMP/IKE DOI defines payload formats, exchange types, and conventions for naming security-relevant information such as security policies or cryptographic algorithms and modes.

(C) For example, see [R2407]. The DOI concept is based on work by the TSIG's CIPSO Working Group.

$ dominate
(I) 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 the nonhierarchical categories of A include all of those of B.

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

(C) A dongle is essentially a physical key used for copy protection of software, because 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
(I) Reduce the classification level of information in an authorized manner.

$ draft RFC
(D) ISDs SHOULD NOT use this term, because the Request for Comment series is archival in nature and does not have a "draft" category. (Instead, see: Internet Draft, Draft Standard (in Internet Standard).)

$ DSA
See: Digital Signature Algorithm.

$ DSS
See: Digital Signature Standard.

$ dual control
(I) 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
(D) ISDs SHOULD NOT use this term except when stated as "SET(trademark) dual signature" with the following meaning:

(O) SET usage: A single digital signature that protects two separate messages by including the hash results for both sets in a single encrypted value. [SET2]

(C) 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.

$ EAP
See: Extensible Authentication Protocol

$ eavesdropping
(I) 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 mechanism
(I) The principle that each security mechanism should be designed to be as simple as possible, so that the mechanism can be correctly implemented and so that it can be verified that the operation of the mechanism enforces the containing system's security policy. (See: least privilege.)

$ EDI
See: electronic data interchange.

$ EDIFACT
See: (secondary definition under) electronic data interchange.

$ EE
(D) ISDs SHOULD NOT use this abbreviation because of possible confusion among "end entity", "end-to-end encryption", "escrowed encryption standard", and other terms.

$ EES
See: Escrowed Encryption Standard.

$ El Gamal algorithm
(N) 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. [ElGa, Schn]

$ electronic codebook (ECB)
(I) An 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 ciphertext [FP081].

$ electronic commerce
(I) General usage: 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.

(O) SET usage: "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." [SET2]

$ electronic data interchange (EDI)
(I) Computer-to-computer exchange, between trading partners, of business data in standardized document formats.

(C) 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 signature
(D) ISDs SHOULD NOT use this term because there is no current consensus on its definition. (Instead, see: digital signature.)

$ elliptic curve cryptography (ECC)
(I) A type of asymmetric cryptography based on mathematics of groups that are defined by the points on a curve.

(C) The most efficient implementation of ECC is claimed to be stronger per bit of key (against cryptanalysis that uses a brute force attack) than any other known form of asymmetric cryptography. ECC is based on mathematics different than the kinds originally used to define the Diffie-Hellman algorithm and the Digital Signature Algorithm. ECC is based on the mathematics of groups defined by the points on a curve, where the curve is defined by a quadratic equation in a finite field. ECC can be used to define both an algorithm for key agreement that is an analog of Diffie-Hellman and an algorithm for digital signature that is an analog of DSA. (See: ECDSA.)

$ Elliptic Curve Digital Signature Algorithm (ECDSA)
(N) A standard [A9062] that is the elliptic curve cryptography analog of the Digital Signature Algorithm.

$ emanation
(I) An signal (electromagnetic, acoustic, or other medium) that is emitted by a system (through radiation or conductance) as a consequence (i.e., byproduct) of its operation, and that may contain information. (See: TEMPEST.)

$ emanations security (EMSEC)
(I) Physical constraints to prevent information compromise through signals emanated by a system, particular the application of TEMPEST technology to block electromagnetic radiation.

$ emergency plan
(D) A synonym for "contingency plan". In the interest of consistency, ISDs SHOULD use "contingency plan" instead of "emergency plan".

$ EMSEC
See: emanations security.

$ EMV
(I) An abbreviation of "Europay, MasterCard, Visa". Refers to a specification for smart cards that are used as payment cards, and for related terminals and applications. [EMV1, EMV2, EMV3]

$ Encapsulating Security Payload (ESP)
(I) An Internet IPsec protocol [R2406] designed to provide a mix of security services--especially data confidentiality service--in the Internet Protocol. (See: Authentication Header.)

(C) ESP may be used alone, or in combination with the IPsec AH protocol, 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
(D) ISDs SHOULD NOT use this term as a synonym for "encrypt". However, see the usage note under "encryption".

$ encipherment
(D) ISDs SHOULD NOT use this term as a synonym for "encryption", except in special circumstances that are explained in the usage discussion under "encryption".

$ encode
(I) Use a system of symbols to represent information, which might originally have some other representation. (See: decode.)

(C) Examples include Morse code, ASCII, and BER.

(D) ISDs SHOULD NOT use this term as a synonym for "encrypt", because encoding is not usually intended to conceal meaning.

$ encrypt
(I) Cryptographically transform data to produce ciphertext. (See: encryption.)

$ encryption
(I) Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state. (See: cryptography.)

(C) Usage note: For this concept, ISDs should use the verb "to encrypt" (and related variations: encryption, decrypt, and decryption). However, because of cultural biases, some international usage, particularly ISO and CCITT standards, avoids "to encrypt" and instead uses the verb "to encipher" (and related variations: encipherment, decipher, decipherment).

(O) "The cryptographic transformation of data (see: cryptography) to produce ciphertext." [I7498 Part 2]

(C) Usually, the plaintext input to an encryption operation is cleartext. But in some cases, the plaintext may be ciphertext that was output from another encryption operation. (See: superencryption.)

(C) Encryption and decryption involve a mathematical algorithm for transforming data. In addition to the data to be transformed, the algorithm has one or more inputs that are control parameters: (a) a key value that varies the transformation and, in some cases, (b) an initialization value that establishes the starting state of the algorithm.

$ encryption certificate
(I) 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.

C) A v3 X.509 public-key certificate may have a "keyUsage" extension that indicates the purpose for which the certified public key is intended.

$ end entity
(I) 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 a purpose or purposes other than signing a digital certificate; i.e., an entity that is not a CA.

(D) "A certificate subject which uses its public [sic] key for purposes other than signing certificates." [X509]

(C) ISDs SHOULD NOT use the X.509 definition, because it is misleading and incomplete. First, the X.509 definition should say "private key" rather than "public key" because certificates are not usefully signed with a public key. Second, the X.509 definition is weak 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. Thus, it would have been better for the X.509 definition to have said "only for purposes other than signing certificates".

(C) 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.

(C) Whether a subject can play both CA and non-CA roles, with either the same or different certificates, is a matter of policy. (See: certification practice statement.) A v3 X.509 public-key certificate may have a "basicConstraints" extension containing a "cA" value that specifically "indicates whether or not the public key may be used to verify certificate signatures".

$ end system
(I) An OSI term for a computer that implements all seven layers of the OSIRM and may attach to a subnetwork. (In the context of the Internet Protocol Suite, usually called a "host".)

$ end-to-end encryption
(I) Continuous protection of data that flows between two points in a network, provided by encrypting data when it leaves its source, leaving it encrypted while it passes through any intermediate computers (such as routers), and decrypting only when the data arrives at the intended destination. (See: link encryption, wiretapping.)

(C) 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
(I) General usage: A system entity, usually a human individual, that makes use of system resources, primarily for application purposes as opposed to system management purposes.

(I) PKI usage: A synonym for "end entity"; but the term "end entity" is preferred.

$ entity
See: system entity.

$ entrapment
(I) "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." [FP039] (See: honey pot.)

$ ephemeral key
(I) A public key or a private key that is relatively short-lived. (See: session key.)

$ error detection code
(I) A checksum designed to detect, but not correct, accidental (i.e., unintentional) changes in data.

$ Escrowed Encryption Standard (EES)
(N) A U.S. Government standard [FP185] that specifies use of a symmetric encryption algorithm (SKIPJACK) and a Law Enforcement

Access Field (LEAF) creation method to implement part of a key escrow system that provides for decryption of encrypted telecommunications when interception is lawfully authorized.

(C) Both SKIPJACK and the LEAF are to be implemented in equipment used to encrypt and decrypt unclassified, sensitive telecommunications data.

$ ESP
See: Encapsulating Security Payload.

$ Estelle
(N) A language (ISO 9074-1989) for formal specification of computer network protocols.

$ evaluated products list
(O) General usage: A list of information system equipment items that have been evaluated against, and found to be compliant with, a particular set of criteria.

(O) U.S. Department of Defense usage: The Evaluated Products List (http://www.radium.ncsc.mil/tpep/epl/) contains items that have been evaluated against the TCSEC by the NCSC, or against the Common Criteria by the NCSC or one of its partner agencies in another county. The List forms Chapter 4 of NSA's "Information Systems Security Products and Services Catalogue".

$ evaluated system
(I) Refers to a system that has been evaluated against security criteria such as the TCSEC or the Common Criteria.

$ expire
See: certificate expiration.

$ exposure
See: (secondary definition under) threat consequence.

$ Extensible Authentication Protocol
(I) A framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. [R2284]

(C) This protocol is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines.

$ extension
(I) A data item defined for optional inclusion in a v3 X.509 public-key certificate or a v2 X.509 CRL.

(C) The formats defined in X.509 can be extended to provide methods for associating additional attributes with subjects and public keys and for managing a certification hierarchy:

- "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.

- "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.

- "Private extension": Additional extensions, each named by an OID, can be locally defined as needed by applications or communities. (See: PKIX private extension, SET private extensions.)

$ extranet
(I) A computer network that an organization uses to carry application data traffic between the organization and its business partners. (See: intranet.)

(C) An extranet can be implemented securely, either on the Internet or using Internet technology, by constructing the extranet as a VPN.

$ fail safe
(I) A mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.

$ fail soft
(I) Selective termination of affected non-essential system functions and processes when a failure occurs or is detected in the system.

$ failure control
(I) A methodology used to provide fail-safe or fail-soft termination and recovery of functions and processes when failures are detected or occur in a system. [FP039]

$ Federal Information Processing Standards (FIPS)
(N) The Federal Information Processing Standards Publication (FIPS PUB) series issued by the U.S. National Institute of Standards and Technology as technical guidelines for U.S. Government procurements of information processing system equipment and services. [FP031, FP039, FP046, FP081, FP102, FP113, FP140, FP151, FP180, FP185, FP186, FP188]

(C) Issued 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.

$ Federal Public-key Infrastructure (FPKI)
(N) A PKI being planned to establish facilities, specifications, and policies needed by the U.S. Federal Government to use public-key certificates for INFOSEC, COMSEC, and electronic commerce involving unclassified but sensitive applications and interactions between Federal agencies as well as with entities of other branches of the Federal Government, state, and local governments, business, and the public. [FPKI]

$ Federal Standard 1027
(N) An U.S. Government document defining emanation, anti-tamper, security fault analysis, and manual key management criteria for DES encryption devices, primary for OSI layer 2. Was renamed "FIPS PUB 140" when responsibility for protecting unclassified, sensitive information was transferred from NSA to NIST, and then was superseded by FIPS PUB 140-1.

$ File Transfer Protocol (FTP)
(I) A TCP-based, application-layer, Internet Standard protocol [R0959] for moving data files from one computer to another.

$ filtering router
(I) An internetwork router that selectively prevents the passage of data packets according to a security policy.

(C) A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. 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). [R2179]

$ financial institution
(N) "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." [SET2]

$ fingerprint
(I) A pattern of curves formed by the ridges on a fingertip. (See: biometric authentication, thumbprint.)

(D) ISDs SHOULD NOT use this term as a synonym for "hash result" because it mixes concepts in a potentially misleading way.

(D) ISDs SHOULD NOT use this term with the following PGP definition, because the term and definition mix concepts in a potentially misleading way and duplicate the meaning of "hash result":

(O) PGP usage: A hash result used to authenticate a public key (key fingerprint) or other data. [PGP]

$ FIPS
See: Federal Information Processing Standards.

$ FIPS PUB 140-1
(N) The U.S. Government standard [FP140] for security requirements to be met by a cryptographic module used to protect unclassified information in computer and communication systems. (See: Common Criteria, FIPS, Federal Standard 1027.)

(C) 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.

$ firewall
(I) 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.)

(C) 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 security policy rules to control traffic that flows in and out of the protected network.

(C) 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 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 intruders out, but usually also needs to let authorized users in and out.

$ firmware
(I) 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 hypothesis methodology
(I) 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. [NCS04]

$ flooding
(I) An attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly. (See: denial of service.)

$ flow analysis
(I) 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
(I) 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, simple security property, confinement property.)

$ formal specification
(I) A specification of hardware or software functionality in a computer-readable language; usually a precise mathematical description of the behavior of the system with the aim of providing a correctness proof.

$ formulary
(I) 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)
(N) 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 that contains a CAPSTONE chip, serial port modems, server boards, smart cards, and software implementations.

$ Forum of Incident Response and Security Teams (FIRST)
(N) An international consortium of CSIRTs that work together to handle computer security incidents and promote preventive activities. (See: CSIRT, security incident.)

(C) FIRST was founded in 1990 and, as of September 1999, had nearly 70 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 government, private industry, academia, and the individual.
- Enhance the image and status of the CSIRT community.

$ forward secrecy
See: public-key forward secrecy.

$ FPKI
See: Federal Public-Key Infrastructure.

$ FTP
See: File Transfer Protocol.

$ gateway
(I) A relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other; an intermediate system that is the interface between two computer networks. (See: bridge, firewall, guard, internetwork, proxy server, router, and subnetwork.)

(C) In theory, gateways are conceivable at any OSI layer. In practice, they operate at OSI layer 3 (see: bridge, router) or layer 7 (see: proxy server). When the two networks differ in the protocol by which they offer service to hosts, the gateway may translate one protocol into another or otherwise facilitate interoperation of hosts (see: Internet Protocol).

$ GCA
See: geopolitical certificate authority.

$ GeneralizedTime
(N) The ASN.1 data type "GeneralizedTime" (specified in 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 allowing Coordinated Universal Time to be calculated. (See: Coordinated Universal Time, UTCTime.)

$ Generic Security Service Application Program Interface (GSS-API)
(I) An Internet Standard protocol [R2078] 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 allowing the application source code to be ported to different environments.

(C) "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]." [R2078]

$ geopolitical certificate authority (GCA)
(O) SET usage: 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.

$ Green Book
(D) Except as an explanatory appositive, ISDs SHOULD NOT use this term as a synonym for "Defense Password Management Guideline" [CSC2]. Instead, use the full proper name of the document or, in subsequent references, a conventional abbreviation. (See: Rainbow Series.)

(D) Usage note: To improve international comprehensibility of Internet Standards and the Internet Standards Process, ISDs SHOULD NOT use "cute" synonyms for document titles. No matter how popular and clearly understood a nickname may be in one community, it is likely to cause confusion in others. For example, several other information system standards also are called "the Green Book". The following are some examples:

- Each volume of 1992 ITU-T (at that time, CCITT) standards.
- "PostScript Language Program Design", Adobe Systems, Addison-Wesley, 1988.
- IEEE 1003.1 POSIX Operating Systems Interface.
- "Smalltalk-80: Bits of History, Words of Advice", Glenn Krasner, Addison-Wesley, 1983.
- "X/Open Compatibility Guide".
- A particular CD-ROM format developed by Phillips.

$ GRIP
(I) A contraction of "Guidelines and Recommendations for Security Incident Processing", the name of the IETF working group that seeks to facilitate consistent handling of security incidents in the Internet community. (See: security incident.)

(C) Guidelines to be produced by the WG will address technology vendors, network service providers, and response teams in their roles assisting organizations in resolving security incidents. These relationships are functional and can exist within and across organizational boundaries.

$ GSS-API
See: Generic Security Service Application Program Interface.

$ guard
(I) A gateway that is interposed between two networks (or computers, or other information systems) operating at different security levels (one level is usually higher than the other) and is trusted to mediate all information transfers between the two levels, either to ensure that no sensitive information from the first (higher) level is disclosed to the second (lower) level, or to protect the integrity of data on the first (higher) level. (See: firewall.)

$ guest login
See: anonymous login.

$ GULS
(I) 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.

$ hacker
(I) Someone with a strong interest in computers, who enjoys learning about them and experimenting with them. (See: cracker.)

(C) The recommended definition is the original meaning of the term (circa 1960), which then had a neutral or positive connotation of "someone who figures things out and makes something cool happen". Today, the term is frequently misused, especially by journalists, to have the pejorative meaning of cracker.

$ handle
(I) (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. (2.) Noun: An on-line pseudonym, particularly one used by a cracker; derived from citizens band radio culture.

$ hardware
(I) The material physical components of a computer system. (See: firmware, software.)

$ hardware token
See: token.

$ hash code
(D) ISDs SHOULD NOT use this term (especially not as a synonym for "hash result") because it mixes concepts in a potentially misleading way. A hash result is not a "code" in any sense defined by this glossary. (See: code, hash result, hash value, message digest.)

$ hash function
(I) An algorithm that computes a value based on a data object (such as a message or file; usually variable-length; possibly very large), thereby mapping the data object to a smaller data object (the "hash result") which is usually a fixed-size value. (See: checksum, keyed hash.)

(O) "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." [X509]

(C) The kind of hash function needed for security applications is called a "cryptographic hash function", an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the "one-way" property) or (b) two data objects that map to the same hash result (the "collision-free" property). (See: MD2, MD4, MD5, SHA-1.)

(C) A cryptographic hash is "good" in the sense stated in the "O" definition for hash function. Any change to an input data object will, with high probability, result in a different hash result, so that the result of a cryptographic hash makes a good checksum for a data object.

$ hash result
(I) The output of a hash function. (See: hash code, hash value.)

(O) "The output produced by a hash function upon processing a message" (where "message" is broadly defined as "a digital representation of data"). [ABA] (The recommended definition is compatible with this ABA definition, but we avoid the unusual definition of "message".)

$ hash value
(D) ISDs SHOULD NOT use this term (especially not as a synonym for "hash result", the output of a hash function) because it might be confused with "hashed value" (the input to a hash function). (See: hash code, hash result, message digest.)

$ hierarchical PKI
(I) A PKI architecture based on a certification hierarchy. (See: mesh PKI, trust-file PKI.)

$ hierarchy management
(I) The process of generating configuration data and issuing public-key certificates to build and operate a certification hierarchy.

$ hierarchy of trust
(D) ISDs SHOULD NOT use this term with regard to PKI, especially not as a synonym for "certification hierarchy", because this term mixes concepts in a potentially misleading way. (See: certification hierarchy, trust, web of trust.)

$ hijack attack
(I) 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.)

$ HMAC
(I) A keyed hash [R2104] 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. (See: [R2202, R2403, R2404].)

(C) 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 the 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, OPAD = the byte 0x5C repeated B times. HMAC is computed by H(K XOR OPAD, H(K XOR IPAD, inputdata)).

(C) The goals of HMAC are as follows:

- 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
(I) A system (e.g., a web server) or a 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.)

(D) It is likely that other cultures have different metaphors for this concept. To ensure international understanding, ISDs should not use this term unless they also provide an explanation like this one. (See: (usage note under) Green Book.)

$ host
(I) General computer network usage: 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.)

(I) Specific Internet Protocol Suite usage: A networked computer that does not forward Internet Protocol packets that are not addressed to the computer itself. (See: router.)

(C) Derivation: As viewed by its users, a host "entertains" guests, 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
(I) 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. (See: S-HTTP.)

$ hybrid encryption
(I) An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption. (E.g., see: digital envelope.)

(C) Asymmetric algorithms require more computation than equivalently strong symmetric ones. Thus, asymmetric encryption is not normally used for data confidentiality except in distributing

symmetric keys in applications where the key data is usually short (in terms of bits) compared to the data it protects. (E.g., see: MSP, PEM, PGP.)

$ hyperlink
(I) In hypertext or hypermedia, an information object (such as a word, a phrase, or an image; usually highlighted by color or underscoring) that points (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
(I) A generalization of hypertext; any media that contain hyperlinks that point to material in the same or another data object.

$ hypertext
(I) 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 Hypertext Markup Language and accessed using a web browser. (See: hypermedia.)

$ Hypertext Markup Language (HTML)
(I) A platform-independent system of syntax and semantics 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. [R1866]

$ Hypertext Transfer Protocol (HTTP)
(I) A TCP-based, application-layer, client-server, Internet protocol [R2616] 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.

$ ICANN
See: Internet Corporation for Assigned Names and Numbers.

$ ICMP
See: Internet Control Message Protocol.

$ ICMP flood
(I) 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
(I) 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 Protocol
(I) An client-server Internet protocol [R1413] for learning the identity of a user of a particular TCP connection.

(C) 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 is not intended for authorization or access control. At best, it provides additional auditing information with respect to TCP.

$ identity-based security policy
(I) "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." [I7498 Part 2] (See: rule-based security policy.)

$ IEEE
See: Institute of Electrical and Electronics Engineers, Inc.

$ IEEE 802.10
(N) An IEEE committee developing security standards for local area networks. (See: SILS.)

$ IEEE P1363
(N) An IEEE working group, Standard for Public-Key Cryptography, 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
(I) A IMAP4 "command" (better described as a transaction type, or a protocol-within-a-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.)

(C) 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, GSSAPI, and S/Key--are described in [R1731].

$ in the clear
(I) Not encrypted. (See: cleartext.)

$ indirect certificate revocation list (ICRL)
(I) In X.509, a CRL that may contain certificate revocation notifications for certificates issued by CAs other than the issuer of the ICRL.

$ indistinguishability
(I) 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.

(C) Under certain conditions, this notion is equivalent to "semantic security".

$ information
(I) Facts and ideas, which can be represented (encoded) as various forms of data.

$ Information Technology Security Evaluation Criteria (ITSEC)
(N) Standard developed for use in the European Union; accommodates a wider range of security assurance and functionality combinations than the TCSEC. Superseded by the Common Criteria. [ITSEC]

$ INFOSEC
(I) Abbreviation for "information security", referring to security measures that implement and assure security services in computer systems (i.e., COMPUSEC) and communication systems (i.e., COMSEC).

$ initialization value (IV)
(I) An input parameter that sets the starting state of a cryptographic algorithm or mode. (Sometimes called "initialization vector" or "message indicator".)

(C) An IV can be used to introduce cryptographic variance in addition to that provided by a key (see: salt), and to synchronize one cryptographic process with another. For an example of the latter, cipher block chaining mode requires an IV. [R2405]

$ initialization vector
(D) For consistency, ISDs SHOULD NOT use this term as a synonym for "initialization value".

$ insider attack
See: (secondary definition under) attack.

$ Institute of Electrical and Electronics Engineers, Inc. (IEEE)
(N) The IEEE is a not-for-profit association of more than 330,000 individual members in 150 countries. The IEEE produces 30 percent of the world’s published literature in electrical engineering, computers, and control technology; holds annually more than 300 major conferences; and has more than 800 active standards with 700 under development. (See: Standards for Interoperable LAN/MAN Security.)

$ integrity
See: data integrity, correctness integrity, source integrity, system integrity.

$ integrity check
(D) ISDs SHOULD NOT use this term as a synonym for "cryptographic hash" or "protected checksum", because this term unnecessarily duplicates the meaning of other, well-established terms.

$ intelligent threat
(I) A circumstance in which an adversary has the technical and operational capability to detect and exploit a vulnerability and also has the demonstrated, presumed, or inferred intent to do so. (See: threat.)

$ International Data Encryption Algorithm (IDEA)
(N) A patented, symmetric block cipher that uses a 128-bit key and operates on 64-bit blocks. [Schn] (See: symmetric cryptography.)

$ International Standard
See: (secondary definition under) ISO.

$ International Traffic in Arms Regulations (ITAR)
(N) 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: Wassenaar Arrangement.)

$ internet
$ Internet
See: internet vs. Internet.

$ Internet Architecture Board (IAB)
(I) 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. [R2026]

$ Internet Assigned Numbers Authority (IANA)
(I) 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)
(I) An Internet Standard protocol [R0792] 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)
(I) The non-profit, private corporation that has assumed responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions formerly performed under U.S. Government contract by IANA and other entities.

(C) The Internet Protocol Suite, 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 object identifiers, 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.

(C) 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: the allocation of IP address space, the assignment of protocol parameters, the management of the DNS, and the management of the DNS root server system.

$ Internet Draft
(I) A working document of the IETF, its areas, and its working groups. (Other groups may also distribute working documents as Internet Drafts.) 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 "work in progress."

$ Internet Engineering Steering Group (IESG)
(I) 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. [R2026]

$ Internet Engineering Task Force (IETF)
(I) 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. [R2026, R2323]

$ Internet Message Access Protocol, version 4 (IMAP4)
(I) An Internet protocol [R2060] 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.)

(C) IMAP4 has mechanisms for optionally authenticating a client to a server and providing other security services. (See: IMAP4 AUTHENTICATE.)

$ Internet Policy Registration Authority (IPRA)
(I) An X.509-compliant CA that is the top CA of the Internet certification hierarchy operated under the auspices of the ISOC [R1422]. (See: (PEM usage under) certification hierarchy.)

$ Internet Protocol (IP)
(I) A Internet Standard protocol (version 4 [R0791] and version 6 [R2460]) 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. (See: IP address, TCP/IP.)

(C) In the OSIRM, IP would be located at the top of layer 3.

$ Internet Protocol security (IPsec)
(I) (1.) The name of the IETF working group that is specifying a security architecture [R2401] and protocols to provide security services for Internet Protocol traffic. (2.) A collective name for that architecture and set of protocols. (Implementation of IPsec protocols is optional for IP version 4, but mandatory for IP version 6.) (See: Internet Protocol Security Option.)

(C) Note that the letters "sec" are lower-case.

(C) The IPsec architecture 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. The set of security services 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.

$ Internet Protocol Security Option (IPSO)
(I) Refers to one of three types of IP security options, which are fields that may be added to an IP datagram for the purpose of carrying security information about the datagram. (See: IPsec.)

(D) ISDs SHOULD NOT use this term without a modifier to indicate which of the three types is meant.

1. "DoD Basic Security Option" (IP option type 130): Defined for use on U.S. Department of Defense common user data networks. Identifies the Defense classification level at which the datagram is to be protected and the protection authorities whose rules apply to the datagram. [R1108]

A "protection authority" is a National Access Program (e.g., GENSER, SIOP-ESI, SCI, NSA, Department of Energy) or Special Access Program that specifies protection rules for transmission and processing of the information contained in the datagram. [R1108]

2. "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]

3. "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".) Was published as Internet-Draft [CIPSO]; not advanced to RFC.

$ Internet Protocol Suite
See: (secondary definition under) Internet.

$ Internet Security Association and Key Management Protocol (ISAKMP)
(I) An Internet IPsec protocol [R2408] 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.

(C) ISAKMP supports negotiation of security associations for protocols at all TCP/IP 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.

$ Internet Society (ISOC)
(I) 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. [R2026]

$ Internet Standard
(I) 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. [R2026] (See: RFC.)

(C) 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 Internet Protocol Suite. The "Internet Standards Track" has three levels of increasing maturity: Proposed Standard, Draft Standard, and Standard. (See: (standards levels under) ISO.)

$ Internet Standards document (ISD)
(C) In this Glossary, this term refers to an RFC, Internet-Draft, or other item that is produced as part of the Internet Standards Process [R2026]. However, neither the term nor the abbreviation is widely accepted and, therefore, SHOULD NOT be used in an ISD unless it is accompanied by an explanation like this. (See: Internet Standard.)

$ internet vs. Internet
1. (I) Not capitalized: A popular abbreviation for "internetwork".

2. (I) Capitalized: "The Internet" is the single, interconnected, worldwide system of commercial, government, educational, and other computer networks that share the set of protocols specified by the IAB [R2026] and the name and address spaces managed by the ICANN.

(C) The protocol set is named the "Internet Protocol Suite". It also is popularly known as "TCP/IP", because TCP and IP are two of its fundamental components. These protocols enable a user of any one of the networks in the Internet to communicate with, or use services located on, any of the other networks.

(C) Although the Internet does have architectural principles [R1958], no Internet Standard formally defines a layered reference model for the IPS that is similar to the OSIRM. However, Internet community documents do refer (inconsistently) to layers: application, socket, transport, internetwork, network, data link,

and physical. In this Glossary, Internet layers are referred to by name to avoid confusing them with OSIRM layers, which are referred to by number.

$ internetwork
(I) A system of interconnected networks; a network of networks. Usually shortened to "internet". (See: internet vs. Internet.)

(C) An internet is usually built using OSI layer 3 gateways to connect a set of subnetworks. When the subnetworks differ in the OSI layer 3 protocol service they provide, the gateways sometimes implement a uniform internetwork protocol (e.g., IP) that operates at the top of layer 3 and hides the underlying heterogeneity from hosts that use communication services provided by the internet. (See: router.)

$ intranet
(I) 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, virtual private network.)

$ intruder
(I) An entity that gains or attempts to gain access to a system or system resource without having authorization to do so. (See: cracker.)

$ intrusion
See: security intrusion.

$ intrusion detection
(I) A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

$ invalidity date
(N) 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" [X509].

(C) 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.

$ IP
See: Internet Protocol.

$ IP address
(I) A computer's internetwork address that is assigned for use by the Internet Protocol and other protocols.

(C) An IP version 4 [R0791] address is written as a series of four 8-bit numbers separated by periods. For example, the address of the host named "rosslyn.bbn.com" is 192.1.7.10.

(C) An IP version 6 [R2373] address is written as x:x:x:x:x:x:x:x, where each "x" is the hexadecimal value of one of the eight 16-bit parts of the address. For example, 1080:0:0:0:8:800:200C:417A and FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

$ IP Security Option
See: Internet Protocol Security Option.

$ IPRA
See: Internet Policy Registration Authority.

$ IPsec
See: Internet Protocol security.

$ IPsec Key Exchange (IKE)
(I) An Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

$ IPSO
See: Internet Protocol Security Option.

$ ISAKMP
See: Internet Security Association and Key Management Protocol.

$ ISD
See: Internet Standards document.

$ ISO
(I) International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of

participating nations and non-voting observer organizations. (See: ANSI, ITU-T.)

(C) Legally, ISO is a Swiss, non-profit, private organization. ISO and the IEC (the International Electrotechnical 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 ITU-T.)

(C) 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). (See: (standards track levels 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.

$ ISOC
See: Internet Society.

$ issue (a digital certificate or CRL)
(I) Generate and sign a digital certificate (or CRL) and, usually, distribute it and make it available to potential certificate users (or CRL users). (See: certificate creation.)

(C) The ABA Guidelines [ABA] explicitly limit this term to certificate creation, and exclude the act of publishing. In general usage, however, "issuing" a digital certificate (or CRL) includes not only certificate creation but also making it available to potential users, such as by storing it in a repository or other directory or otherwise publishing it.

$ issuer
1. (I) "Issuer" of a certificate or CRL: The CA that signs the digital certificate or CRL.

(C) An X.509 certificate always includes the issuer’s name. The name may include a common name value.

2. (N) "Issuer" of a payment card: SET usage: "The financial institution or its agent that issues the unique primary account number to the cardholder for the payment card brand." [SET2]

(C) 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. [SET1]

$ ITAR
See: International Traffic in Arms Regulations.

$ ITSEC
See: Information Technology System Evaluation Criteria.

$ ITU-T
(N) 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.)

(C) 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.

$ KDC
See: Key Distribution Center.

$ KEA
See: Key Exchange Algorithm.

$ KEK
See: key-encrypting key.

$ Kerberos
(N) 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. [R1510, Stei]

(C) Kerberos was developed by Project Athena and is named for the three-headed dog guarding Hades.

$ key
See: cryptographic key.

$ key agreement (algorithm or protocol)
(I) 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 computes the same key value. I.e., each can independently generate the same key value, but that key cannot be computed by other entities. (See: Diffie-Hellman, key establishment, Key Exchange Algorithm, key transport.)

(O) "A method for negotiating a key value on line without transferring the key, even in an encrypted form, e.g., the Diffie-Hellman technique." [X509]

(O) "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." [A9042]

(C) For 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 algorithm to first compute a shared secret value and, from that value, derive a session key to encrypt the message.

$ key authentication
(N) "The assurance of the legitimate participants in a key agreement that no non-legitimate party possesses the shared symmetric key." [A9042]

$ key center
(I) A centralized key distribution process (used in symmetric cryptography), usually a separate computer system, that uses key-encrypting keys (master keys) to encrypt and distribute session keys needed in a community of users.

(C) An ANSI standard [A9017] defines two types of key center: key distribution center and key translation center.

$ key confirmation
(N) "The assurance of the legitimate participants in a key establishment protocol that the intended parties sharing the symmetric key actually possess the shared symmetric key." [A9042]

$ key distribution
(I) 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 management.)

$ key distribution center (KDC)
(I) 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. (See: key translation center.)

(C) 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 sends that encrypted set to Alice for her to forward to Bob, or sends it directly to Bob (although the latter option is not supported in the ANSI standard [A9017]).

$ key encapsulation
See: (secondary definition under) key recovery.

$ key-encrypting key (KEK)
(I) A cryptographic key that is used to encrypt other keys, either DEKs or other KEKs, but usually is not used to encrypt application data.

$ key escrow
See: (secondary definition under) key recovery.

$ key establishment (algorithm or protocol)
(I) A process that combines the key generation and key distribution steps needed to set up or install a secure communication association. (See: key agreement, key transport.)

(O) "The procedure to share a symmetric key among different parties by either key agreement or key transport." [A9042]

(C) Key establishment involves either key agreement or key transport:

- Key transport: One entity generates a secret key and securely sends it to the other entity. (Or 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.)

- Key agreement: No secret is sent from one entity to another. Instead, both entities, without prior arrangement except a public exchange of data, compute the same secret value. I.e.,

each can independently generate the same value, but that value cannot be computed by other entities.

$ Key Exchange Algorithm (KEA)
(N) A key agreement algorithm [NIST] that is similar to the Diffie-Hellman algorithm, uses 1024-bit asymmetric keys, and was developed and formerly classified at the "Secret" level by NSA. (See: CAPSTONE, CLIPPER, FORTEZZA, SKIPJACK.)

(C) On 23 June 1998, the NSA announced that KEA had been declassified.

$ key generation
(I) A process that creates the sequence of symbols that comprise a cryptographic key. (See: key management.)

$ key generator
1. (I) An algorithm that uses mathematical rules to deterministically produce a pseudo-random sequence of cryptographic key values.

2. (I) An encryption device that incorporates a key generation mechanism and applies the key to plaintext (e.g., by exclusive OR-ing the key bit string with the plaintext bit string) to produce ciphertext.

$ key length
(I) The number of symbols (usually bits) needed to be able to represent any of the possible values of a cryptographic key. (See: key space.)

$ key lifetime
(N) MISSI usage: 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: cryptoperiod.)

$ key management
(I) The process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material. (See: key distribution, key escrow, keying material, public-key infrastructure.)

(O) "The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy." [I7498 Part 2]

(O) "The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, counters) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving." [FP140]

$ Key Management Protocol (KMP)
(N) 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.)

$ key material identifier (KMID)
(N) MISSI usage: 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.

$ key pair
(I) 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 (e.g., see: Diffie-Hellman, Rivest-Shamir-Adleman).

(C) A key pair’s owner discloses the public key to other system entities so they can use the key to encrypt data, verify a digital signature, compute a protected checksum, or generate a key in a key agreement algorithm. The matching private key is kept secret by the owner, who uses it to decrypt data, generate a digital signature, verify a protected checksum, or generate a key in a key agreement algorithm.

$ key recovery
1. (I) A process for learning the value of a cryptographic key that was previously used to perform some cryptographic operation. (See: cryptanalysis.)

2. (I) Techniques that provide an intentional, alternate (i.e., secondary) means to access the key used for data confidentiality service in an encrypted association. [DOD4]

(C) We assume that the encryption mechanism has 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 escrow and key encapsulation:

- "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.

  Key escrow is typically implemented with split knowledge techniques. For example, the Escrowed Encryption Standard [FP185] 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 encapsulation": A key recovery technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that that only certain third parties called "recovery agents" can perform the decryption operation to retrieve the stored key.

  Key encapsulation typically allows direct retrieval of the secret key used to provide data confidentiality.

$ key space
(I) 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
(I) A type of key center (used in a symmetric cryptography) that implements a key distribution protocol to convey keys between two (or more) parties who wish to communicate securely. (See: key distribution center.)

(C) A key translation center translates 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, reencrypts the set in the KEK it shares with Bob, and either sends that encrypted set to Alice for her to forward to Bob, or sends it directly to Bob (although direct distribution is not supported in the ANSI standard [A9017]).

$ key transport (algorithm or protocol)
(I) A key establishment method by which a secret key is generated by one entity in a communication association and securely sent to another entity in the association. (See: key agreement.)

(O) "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." [A9042]

(C) For example, a message originator can generate a random session key and then use the Rivest-Shamir-Adleman algorithm to encrypt that key with the public key of the intended recipient.

$ key update
(I) Derive a new key from an existing key. (See: certificate rekey.)

$ key validation
(N) "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." [A9042]

$ keyed hash
(I) A cryptographic hash (e.g., [R1828]) in which the mapping to a hash result is varied by a second input parameter that is a cryptographic key. (See: checksum.)

(C) If the input data object is changed, a new 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 least two forms of keyed hash:

- A function based on a keyed encryption algorithm. (E.g., see: 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. (E.g., see: HMAC.)

$ keying material
(I) Data (such as keys, key pairs, and initialization values) needed to establish and maintain a cryptographic security association.

$ KMID
See: key material identifier.

$ known-plaintext attack
(I) 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 the knowing the cryptographic algorithm).

$ L2F
See: Layer 2 Forwarding Protocol.

$ L2TP
See: Layer 2 Tunneling Protocol.

$ label
See: security label.

$ Language of Temporal Ordering Specification (LOTOS)
(N) A language (ISO 8807-1990) for formal specification of computer network protocols; describes the order in which events occur.

$ lattice model
(I) A security 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] (See: flow control, security level, security model.)

(C) The model describes the semantic structure formed by a finite set of security levels, such as those used in military organizations.

(C) A lattice is 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. For 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 (X1, ..., Xm), and c is a (possibly empty) subset of a finite set C of non-hierarchical categories (C1, ..., Cn) -- together with the "dominate" relation. (See: dominate.)

$ Law Enforcement Access Field (LEAF)
(N) A data item that is automatically embedded in data encrypted by devices (e.g., see: CLIPPER chip) that implement the Escrowed Encryption Standard.

$ Layer 2 Forwarding Protocol (L2F)
(N) 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)
(N) 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: virtual private network.)

(C) PPP can in turn encapsulate any OSI 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 privilege
(I) 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. (See: economy of mechanism.)

(C) This principle tends to limit damage that can be caused by an accident, error, or unauthorized act.

$ Lightweight Directory Access Protocol (LDAP)
(N) A 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). [R1777]

(C) 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
(I) World Wide Web usage: See: hyperlink.

(I) Subnetwork usage: A point-to-point communication channel connecting two subnetwork relays (especially one between two packet switches) that is implemented at OSI layer 2. (See: link encryption.)

(C) 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.

$ link-by-link encryption
$ link encryption
(I) Stepwise 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. [R1455] (See: end-to-end encryption.)

$ logic bomb
(I) 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
(I) The act of a system entity gaining access to a session in which the entity can use system resources; usually accomplished by providing a user name and password to an access control system that authenticates the user.

(C) Derives from "log" file", a security audit trail that records security events, such as the beginning of sessions, and who initiates them.

$ LOTOS
See: Language of Temporal Ordering Specification.

$ MAC
See: mandatory access control, Message Authentication Code.

$ malicious logic
(I) Hardware, software, or firmware that is intentionally included or inserted in a system for a harmful purpose. (See: logic bomb, Trojan horse, virus, worm.)

$ malware
(I) A contraction of "malicious software". (See: malicious logic.)

(D) ISDs SHOULD NOT use this term because it is not listed in most dictionaries and could confuse international readers.

$ man-in-the-middle
(I) A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association. (See: hijack attack, piggyback attack.)

(C) For example, suppose Alice and Bob try to establish a session key by using the Diffie-Hellman 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 in order to capture or modify sensitive information that Alice and Bob think they are sending only to each other.

$ mandatory access control (MAC)
(I) 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 system entities are eligible to access certain resources). (See: discretionary access control, rule-based security policy.)

(C) This kind of access control is called "mandatory" because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.

(O) "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." [DOD1]

$ manipulation detection code
(D) ISDs SHOULD NOT use this term as a synonym for "checksum" because 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.

$ masquerade attack
(I) A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity. (See: spoofing attack.)

$ MCA
See: merchant certificate authority.

$ MD2
(N) A cryptographic hash [R1319] that produces a 128-bit hash result, was designed by Ron Rivest, and is similar to MD4 and MD5 but slower. (See: message digest.)

$ MD4
(N) A cryptographic hash [R1320] that produces a 128-bit hash result and was designed by Ron Rivest. (See: message digest and SHA-1.)

$ MD5
(N) A cryptographic hash [R1321] that produces a 128-bit hash result and was designed by Ron Rivest to be an improved version of MD4.

$ merchant
(O) SET usage: "A seller of goods, services, and/or other information who accepts payment for these items electronically." [SET2] 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. [SET1, SET2]

$ merchant certificate
(O) SET usage: 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)
(O) SET usage: 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. [SET2]

$ mesh PKI
(I) 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. (See: hierarchical PKI, trust-file PKI.)

$ message authentication code vs. Message Authentication Code (MAC)
1. (N) Capitalized: "(The) Message Authentication Code" refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES. [A9009] (Also known as the U.S. Government standard Data Authentication Code. [FP113])

(C) The ANSI standard MAC algorithm is equivalent to cipher block chaining with IV = 0.

2. (D) Not capitalized: ISDs SHOULD NOT use the uncapitalized form "message authentication code", because this term mixes concepts in a potentially misleading way. Instead, use "checksum", "error detection code", "hash", "keyed hash", "Message Authentication Code", or "protected checksum", depending on what is meant. (See: authentication code.)

(C) In the uncapitalized form, 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, and 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
(D) ISDs SHOULD NOT use this term as a synonym for "hash result" because it unnecessarily duplicates the meaning of the other, more general term and mixes concepts in a potentially misleading way. (See: cryptographic hash, Message Handling System.)

$ Message Handling Systems
(I) A ITU-T/ISO system concept, which 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".) (See: X.400.)

$ message indicator
(D) ISDs SHOULD NOT use this term as a synonym for "initialization value" because it mixes concepts in a potentially misleading way.

$ message integrity check
$ message integrity code
(D) ISDs SHOULD NOT use these terms because they mix concepts in a potentially misleading way. (The word "message" is misleading because it suggests that the mechanism is particularly suitable for or limited to electronic mail. The word "code" is misleading because it suggests that either encoding or encryption is involved, or that the term refers to computer software.) Instead, use "checksum", "error detection code", "hash", "keyed hash", "Message Authentication Code", or "protected checksum", depending on what is meant.

$ Message Security Protocol (MSP)
(N) A secure message handling protocol [SDNS7] for use with X.400 and Internet mail protocols. Developed by NSA's SDNS program and used in the U.S. Defense Message System.

$ MHS
See: message handling system.

$ MIME
See: Multipurpose Internet Mail Extensions.

$ MIME Object Security Services (MOSS)
(I) An Internet protocol [R1848] 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. [MISPC]

$ MISPC
See: Minimum Interoperability Specification for PKI Components.

$ MISSI
(N) 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 Government missions. (See: MSP.)

$ MISSI user
(O) MISSI usage: 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.)

(C) 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. Some machines are required to operate non-stop. To avoid downtime needed to exchange the FORTEZZA cards of machine operators at shift changes, the machines may be issued their own cards, as if they were persons.

$ mode
$ mode of operation
(I) Encryption usage: 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: electronic codebook, cipher block chaining, cipher feedback, output feedback.)

(I) System operation usage: 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: dedicated security mode, multilevel security mode, partitioned security mode, system high security mode.)

$ modulus
(I) 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, Rivest-Shamir-Adleman.)

$ Morris Worm
(I) A worm program written by Robert T. Morris, Jr. that flooded the ARPANET in November, 1988, causing problems for thousands of hosts. (See: worm.)

$ MOSS
See: MIME Object Security Services.

$ MSP
See: Message Security Protocol.

$ multilevel secure (MLS)
(I) A class of system that has system resources (particularly stored information) at more than one security level (i.e., has different types of sensitive resources) and that permits

concurrent access by users who differ in security clearance and need-to-know, but is able to prevent each user from accessing resources for which the user lacks authorization.

$ multilevel security mode
(I) A mode of operation of an information system, that allows two or more classification levels of information to be processed concurrently within the same system when not all users have a clearance or formal access authorization for all data handled by the system.

(C) This mode is defined formally in U.S. Department of Defense policy regarding system accreditation [DOD2], but the term is also used outside the Defense Department and outside the Government.

$ Multipurpose Internet Mail Extensions (MIME)
(I) An Internet protocol [R2045] that enhances the basic format of Internet electronic mail messages [R0822] to be able to use character sets other than US-ASCII for textual headers and text content, and to carry non-textual and multi-part content. (See: S/MIME.)

$ mutual suspicion
(I) 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.

$ National Computer Security Center (NCSC)
(N) A U.S. Department of Defense organization, housed in NSA, that has responsibility for encouraging widespread availability of trusted computer systems throughout the Federal Government. It has established criteria for, and performs evaluations of, computer and network systems that have a trusted computing base. (See: Evaluated Products List, Rainbow Series, TCSEC.)

$ National Information Assurance Partnership (NIAP)
(N) An organization created by 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.

(C) NIAP is registered, through the U.S. Department of Defense, 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.
- Working to establish a formal, international mutual recognition scheme for a Common Criteria-based evaluation.

$ National Institute of Standards and Technology (NIST)
(N) A U.S. Department of Commerce agency that promotes U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. Has primary Government responsibility for INFOSEC standards for unclassified but sensitive information. (See: ANSI, DES, DSA, DSS, FIPS, NIAP, NSA.)

$ National Security Agency (NSA)
(N) A U.S. Department of Defense intelligence agency that has primary Government responsibility for INFOSEC for classified information and for unclassified but sensitive information handled by national security systems. (See: FORTEZZA, KEA, MISSI, NIAP, NIST, SKIPJACK.)

$ need-to-know
(I) The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

(C) This 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
See: computer network.

$ NIAP
See: National Information Assurance Partnership.

$ NIST
See: National Institute of Standards and Technology.

$ NLSP
Network Layer Security Protocol. An OSI protocol (IS0 11577) for end-to-end encryption services at the top of OSI layer 3. NLSP is derived from an SDNS protocol, SP3, but is much more complex.

$ no-lone zone
(I) A room or other space 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.)

$ nonce
(I) 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.

$ non-critical
See: critical (extension of certificate).

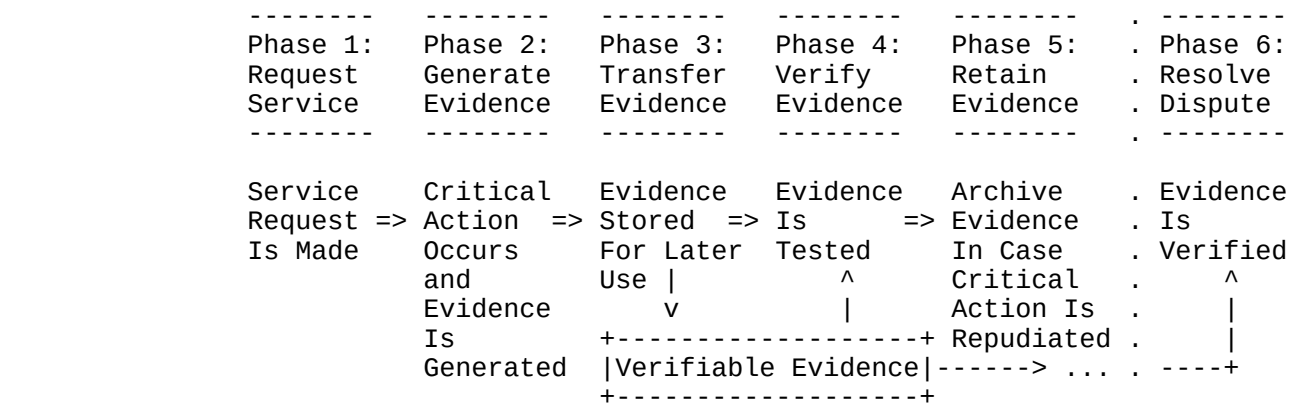
$ non-repudiation service
(I) A security service that provide protection against false denial of involvement in a communication. (See: repudiation.)

(C) Non-repudiation service does not and cannot 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. There are two basic kinds of non-repudiation service:

- "Non-repudiation with proof of origin" 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. This service can be viewed as a stronger version of an data origin authentication service, in that it proves authenticity to a third party.

- "Non-repudiation with proof of receipt" 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.

(C) Phases of a Non-Repudiation Service: Ford [For94, For97] uses the term "critical action" to refer to the act of communication that is the subject of the service:



Phase / Explanation

1. Before the critical action, the service requester asks, either implicitly or explicitly, to have evidence of the action be generated.
2. When the critical action occurs, evidence is generated by a process involving the potential repudiator and possibly also a trusted third party.
3. The evidence is transferred to the requester, or stored by a third party, for later use if needed.
4. The entity that holds the evidence tests to be sure that it will suffice if a dispute arises.
5. The evidence is retained for possible future retrieval and use.
6. 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.

$ no-PIN ORA (NORA)
(O) MISSI usage: 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.

$ NORA
See: no-PIN ORA.

$ notarization
(I) 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, and delivery. [I7498 Part 2] (See: digital notary.)

$ NULL encryption algorithm
(I) An algorithm [R2410] that does nothing to transform plaintext data; i.e., a no-op. It originated because of IPsec ESP, which always specifies the use of an encryption algorithm to provide 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 this is needed).

$ OAKLEY
(I) A key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP. [R2412]

(C) 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 exchange is threatened by active wiretapping. Also, provides public-key forward secrecy for the shared key and supports key updates, incorporation of keys distributed by out-of-band mechanisms, and user-defined abstract group structures for use with Diffie-Hellman.

$ object
(I) Trusted computer system modeling usage: A system element that contains or receives information. (See: Bell-LaPadula Model, trusted computer system.)

$ object identifier (OID)
(I) 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.

(O) "A value (distinguishable from all other such values) which is associated with an object." [X680]

(C) 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.

(C) 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}.

(C) The following are additional examples: ANSI registers organization names below the branch {joint-iso-ccitt(2) country(16) US(840) organization(1)}. The NIST CSOR records PKI objects below the branch {joint-iso-ccitt(2) country(16) us(840) gov(101) csor(3) pki(4)}. The U.S. Department of Defense registers INFOSEC objects below the branch {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1)}. The OID for the PKIX private extension is defined in an arc below the arc for the PKIX name space, as {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 1 1}.

$ object reuse
(N) "The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more [information] objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media." [NCS04]

$ OCSP
See: On-line Certificate Status Protocol.

$ octet
(I) A data unit of eight bits. (See: byte.)

(c) 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.

$ OFB
See: output feedback.

$ ohnosecond
(C) That minuscule fraction of time in which you realize that your private key has been compromised.

$ OID
See: object identifier.

$ On-line Certificate Status Protocol (OCSP)
(I) An Internet protocol used by a client to obtain from a server the validity status and other information concerning a digital certificate.

(C) In some applications, such as those involving high-value commercial transactions, it may be necessary to obtain certificate revocation status that is more timely than is possible with CRLs or 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
(I) An encryption algorithm in which the key is a random sequence of symbols and each symbol is used for encryption only one time--to encrypt only one plaintext symbol to produce only one ciphertext symbol--and a copy of the key is used similarly for decryption.

(C) 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 [Schn], 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 [R1938] 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
(I) Irreversible transformation of plaintext to ciphertext, such that the plaintext cannot be recovered from the ciphertext by other than exhaustive procedures even if the cryptographic key is known. (See: encryption.)

$ one-way function
(I) "A (mathematical) function, f, which 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." [X509]

(D) ISDs SHOULD NOT use this term as a synonym for "cryptographic hash".

$ open security environment
(O) U.S. Department of Defense usage: A system environment that meets at least one of the following 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. [NCS04] (See: closed security environment.)

$ Open Systems Interconnection (OSI) Reference Model (OSIRM)
(N) A joint ISO/ITU-T standard [I7498 Part 1] for a seven-layer, architectural communication framework for interconnection of computers in networks.

(C) OSI-based standards include communication protocols that are mostly incompatible with the Internet Protocol Suite, but also include security models, such as X.509, that are used in the Internet.

(C) The OSIRM layers, from highest to lowest, are (7) Application, (6) Presentation, (5) Session, (4) Transport, (3) Network, (2) Data Link, and (1) Physical. In this Glossary, these layers are referred to by number to avoid confusing them with Internet Protocol Suite layers, which are referred to by name.

(C) Some unknown person described how the OSI layers correspond to the seven deadly sins:

7. Wrath: Application is always angry at the mess it sees below itself. (Hey! Who is it to be pointing fingers?)
6. Sloth: Presentation is too lazy to do anything productive by itself.
5. Lust: Session is always craving and demanding what truly belongs to Application’s functionality.
4. Avarice: Transport wants all of the end-to-end functionality. (Of course, it deserves it, but life isn’t fair.)

3. Gluttony: (Connection-Oriented) Network is overweight and overbearing after trying too often to eat Transport's lunch.
2. Envy: Poor Data Link is always starved for attention. (With Asynchronous Transfer Mode, maybe now it is feeling less neglected.)
1. Pride: Physical has managed to avoid much of the controversy, and nearly all of the embarrassment, suffered by the others.

(C) John G. Fletcher described how the OSI layers also correspond to Snow White's dwarf friends:

7. Doc: Application acts as if it is in charge, but sometimes muddles its syntax.
6. Sleepy: Presentation is indolent, being guilty of the sin of Sloth.
5. Dopey: Session is confused because its charter is not very clear.
4. Grumpy: Transport is irritated because Network has encroached on Transport's turf.
3. Happy: Network smiles for the same reason that Transport is irritated.
2. Sneezy: Data Link makes loud noises in the hope of attracting attention.
1. Bashful: Physical quietly does its work, unnoticed by the others.

$ operational integrity
(I) A synonym for "system integrity"; emphasizes the actual performance of system functions rather than just the ability to perform them.

$ operations security (OPSEC)
(I) 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.

$ OPSEC
See: operations security.

$ ORA
See: organizational registration authority.

$ Orange Book
(D) ISDs SHOULD NOT use this term as a synonym for "Trusted Computer System Evaluation Criteria" [CSC001, DOD1]. Instead, use

the full, proper name of the document or, in subsequent references, the abbreviation "TCSEC". (See: (usage note under) Green Book.)

$ organizational certificate
(O) MISSI usage: A type of MISSI X.509 public-key certificate that is issued to support organizational message handling for the U.S. Government's Defense Message System.

$ organizational registration authority (ORA)
(I) General usage: An RA for an organization.

(O) MISSI usage: The MISSI implementation of RA. A MISSI 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 office or role, and to the person who fills that office. An ORA does not sign certificates, CRLs, or CKLs. (See: no-PIN ORA, SSO-PIN ORA, user-PIN ORA.)

$ origin authentication
$ origin authenticity
(D) ISDs SHOULD NOT use these terms because they look like careless use of an internationally standardized term. Instead, use "data origin authentication" or "peer entity authentication", depending which is meant.

$ OSI
$ OSIRM
See: Open Systems Interconnection Reference Model.

$ OTP
See: One-Time Password.

$ out of band
(I) Transfer of information using a channel that is outside (i.e., separate from) the channel that is normally used. (See: covert channel.)

(C) 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. (See: key distribution.)

$ output feedback (OFB)
(N) A block cipher mode [FP081] that modifies electronic codebook mode to operate on plaintext segments of variable length less than or equal to the block length.

(C) 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
$ outsider attack
See: (secondary definition under) attack.

$ P1363
See: IEEE P1363.

$ PAA
See: policy approving authority.

$ packet filter
See: (secondary definition under) filtering router.

$ pagejacking
(I) 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, rehosts the page on a server the attacker controls, and causes the rehosted page to be indexed by the major Web search services, thereby diverting browsers from the target server to the attacker's server.

(D) ISDs SHOULD NOT use this term without including a definition, because the term is not listed in most dictionaries and could confuse international readers. (See: (usage note under) Green Book.)

$ PAN
See: primary account number.

$ PAP
See: Password Authentication Protocol.

$ partitioned security mode
(N) A mode of operation of an information system, wherein all users have the clearance, but not necessarily formal access authorization and need-to-know, for all information handled by the system. This mode is defined in U.S. Department of Defense policy regarding system accreditation. [DoD2]

$ passive attack
See: (secondary definition under) attack.

$ passive wiretapping
See: (secondary definition under) wiretapping.

$ password
(I) A secret data value, usually a character string, that is used as authentication information. (See: challenge-response.)

(C) A password is usually matched with a user identifier that is explicitly presented in the authentication process, but in some cases the identity may be implicit.

(C) Using a password as authentication information assumes that the password is known only by the system entity whose 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 as cleartext is inadequate. (See: one-time password, strong authentication.)

$ Password Authentication Protocol (PAP)
(I) A simple authentication mechanism in PPP. In PAP, a user identifier and password are transmitted in cleartext. [R1334] (See: CHAP.)

$ password sniffing
(I) Passive wiretapping, usually on a local area network, to gain knowledge of passwords. (See: (usage note under) sniffing.)

$ path discovery
(I) 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
(I) 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.)

$ payment card
(N) SET usage: 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." [SET2]

$ payment gateway
(O) SET usage: A system operated by an acquirer, or a third party designated by an acquirer, for the purpose of providing 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. [SET1, SET2]

$ payment gateway certification authority (SET PCA)
(O) SET usage: 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. [SET2] (See: PCA.)

$ PC card
(N) 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.)

(C) The international PC Card Standard defines a non-proprietary form factor in three standard 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
(D) ISDs SHOULD NOT use this acronym without a qualifying adjective because that would be ambiguous. (See: Internet policy certification authority, (MISSI) policy creation authority, (SET) payment gateway certification authority.)

$ PCMCIA
(N) 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.)

$ peer entity authentication
(I) "The corroboration that a peer entity in an association is the one claimed." [I7498 Part 2] (See: authentication.)

$ peer entity authentication service
(I) A security service that verifies an identity claimed by or for a system entity in an association. (See: authentication, authentication service.)

(C) 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.

(C) See: "relationship between data integrity service and authentication services" under data integrity service.

$ PEM
See: Privacy Enhanced Mail.

$ penetration
(I) Successful, repeatable, unauthorized access to a protected system resource. (See: attack, violation.)

$ penetration test
(I) A system test, often part of system certification, in which evaluators attempt to circumvent the security features of the system. [NCS04]

(C) Penetration testing may be performed under various constraints and conditions. However, 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
See: (discussion under) public-key forward secrecy.

$ perimeter
See: security perimeter.

$ periods processing
(I) 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.)

$ permission
(I) A synonym for "authorization", but "authorization" is preferred in the PKI context. (See: privilege.)

$ personal identification number (PIN)
(I) A character string used as a password to gain access to a system resource. (See: authentication information.)

(C) Despite the words "identification" and "number", a PIN seldom serves as a user identifier, and a PIN's characters are not necessarily all numeric. A better name for this concept would have been "personal authentication system string (PASS)".

(C) Retail banking applications commonly use 4-digit PINs. FORTEZZA PC card's use up to 12 characters for user or SSO PINs.

$ personality
$ personality label
(O) MISSI usage: 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.

(C) 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 security
(I) 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.

$ PGP(trademark)
See: Pretty Good Privacy.

$ Photuris
(I) A UDP-based, key establishment protocol for session keys, designed for use with the IPsec protocols AH and ESP. Superseded by IKE.

$ phreaking
(I) A contraction of "telephone breaking". An attack on or penetration of a telephone system or, by extension, any other communication or information system. [Raym]

(D) ISDs SHOULD NOT use this term because it is not listed in most dictionaries and could confuse international readers.

$ physical security
(I) Tangible means of preventing unauthorized physical access to a system. E.g., fences, walls, and other barriers; locks, safes, and vaults; dogs and armed guards; sensors and alarm bells. [FP031, R1455]

$ piggyback attack
(I) 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.)

$ PIN
See: personal identification number.

$ ping of death
(I) An attack that sends an improperly large ICMP [R0792] echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

$ ping sweep
(I) An attack that sends ICMP [R0792] echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

$ PKCS
See: Public-Key Cryptography Standards.

$ PKCS #7
(N) A standard [PKC07, R2315] from the PKCS series; defines a syntax for data that may have cryptography applied to it, such as for digital signatures and digital envelopes.

$ PKCS #10
(N) A standard [PKC10] from the PKCS series; defines a syntax for requests for public-key certificates. (See: certification request.)

(C) 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
(N) A standard [PKC11] from the PKCS series; defines a software CAPI called Cryptoki (pronounced "crypto-key"; short for "cryptographic token interface") for devices that hold cryptographic information and perform cryptographic functions.

$ PKI
See: public-key infrastructure.

$ PKIX
(I) (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 needed to support an X.509-based PKI for the Internet. (2.) A collective name for that architecture and set of protocols.

(C) 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.

$ PKIX private extension
(I) PKIX defines a private extension to identify an on-line verification service supporting the issuing CA.

$ plaintext
(I) Data that is input to and transformed by an encryption process, or that is output by a decryption process.

(C) Usually, the plaintext input to an encryption operation is cleartext. But in some cases, the input is ciphertext that was output from another encryption operation. (See: superencryption.)

$ Point-to-Point Protocol (PPP)
(I) An Internet Standard protocol [R1661] for encapsulation and full-duplex transportation of network layer (mainly OSI layer 3) protocol data packets over a link between two peers, and for multiplexing different network layer 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 network layer data. (See: CHAP, EAP, PAP.)

$ Point-to-Point Tunneling Protocol (PPTP)
(I) 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.)

(C) PPP can encapsulate any Internet Protocol Suite network layer protocol (or OSI 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., the PPTP Network Server, which runs on a general-purpose host).

$ policy
(D) ISDs SHOULD NOT use this word as an abbreviation for either "security policy" or "certificate policy". Instead, to avoid misunderstanding, use the fully qualified term, at least at the point of first usage.

$ policy approving authority (PAA)
(O) MISSI usage: 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: root registry.)

(C) A PAA registers MISSI PCAs and signs their X.509 public-key certificates. A PAA issues CRLs but does not issue a CKL. A PAA may issue cross-certificates to other PAAs.

$ policy certification authority (Internet PCA)
(I) An X.509-compliant CA at the second level of the Internet certification hierarchy, under the Internet Policy Registration Authority (IPRA). Each PCA operates in accordance with its published security policy (see: certification practice statement) and within constraints established by the IPRA for all PCAs. [R1422]. (See: policy creation authority.)

$ policy creation authority (MISSI PCA)
(O) MISSI usage: 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.)

(C) A MISSI PCA’s certificate is issued by a policy approving authority. 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
(N) Canadian usage: An organization responsible for PKI oversight and policy management in the Government of Canada.

$ policy mapping
(I) "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." [X509]

$ POP3
See: Post Office Protocol, version 3.

$ POP3 APOP
(I) A POP3 "command" (better described as a transaction type, or a protocol-within-a-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.)

(C) The server includes a unique timestamp 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 timestamp and a shared secret that is known only to the client and the server. APOP was designed to provide as an alternative to using POP3's USER and PASS (i.e., password) command pair, in which the client sends a cleartext password to the server.

$ POP3 AUTH
(I) A "command" [R1734] (better described as a transaction type, or a protocol-within-a-protocol) in POP3, 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.)

(C) 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
(I) An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.

$ POSIX
(N) Portable Operating System Interface for Computer Environments, a standard [FP151, IS9945-1] (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.

(C) P1003.1 supports security functionality like those on most UNIX systems, including discretionary access control and privilege. IEEE Draft Standard P1003.6.1 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)
(I) An Internet Standard protocol [R1939] 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.)

(C) 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.

$ pre-authorization
(I) A capability of a CAW that enables certification requests to be automatically validated against data provided in advance to the CA by an authorizing entity.

$ Pretty Good Privacy(trademark) (PGP(trademark))
(O) 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. (See: MOSS, PEM, S/MIME.)

(C) PGP encrypts messages with IDEA in CFB mode, distributes the IDEA keys by encrypting them with RSA, and creates digital signatures on messages with MD5 and RSA. To establish ownership of public keys, PGP depends on the web of trust. (See: Privacy Enhanced Mail.)

$ primary account number (PAN)
(O) SET usage: "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." [SET2, IS7812] (See: bank identification number.)

(C) 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 bank identification number part of the PAN is the American Bankers Association.

$ privacy
(I) 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 information about itself with others. (See: anonymity.)

(O) "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." [I7498 Part 2]

(D) ISDs 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.

$ Privacy Enhanced Mail (PEM)
(I) An Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail. [R1421, R1422]. (See: MOSS, MSP, PGP, S/MIME.)

(C) PEM encrypts messages with DES in CBC mode, provides key distribution of DES keys by encrypting them with RSA, and signs messages with 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 RSA and MD2. (See: Pretty Good Privacy.)

(C) 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
(I) A synonym for "private key".

(D) In most cases, ISDs SHOULD NOT use this term; to avoid confusing readers, use "private key" instead. However, the term MAY be used when specifically 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
(I) The secret component of a pair of cryptographic keys used for asymmetric cryptography. (See: key pair, public key.)

(O) "(In a public key cryptosystem) that key of a user's key pair which is known only by that user." [X509]

$ privilege
(I) An authorization or set of authorizations to perform security-relevant functions, especially in the context of a computer operating system.

$ privilege management infrastructure
(N) "The complete set of processes required to provide an authorization service", i.e., processes concerned with attribute certificates. [FPDAM] (See: PKI.)

(D) ISDs SHOULD NOT use this term and its definition because the definition is vague, and there is no consensus on an alternate definition.

$ privileged process
(I) An computer process that is authorized (and, therefore, trusted) to perform some security-relevant functions that ordinary processes are not. (See: privilege, trusted process.)

$ procedural security
(D) ISDs SHOULD NOT use this term as a synonym for "administrative security". Any type of security may involve procedures; therefore, the term may be misleading. Instead, use "administrative security", "communication security", "computer security", "emanations security", "personnel security", "physical security", or whatever specific type is meant. (See: security architecture.)

$ proprietary
(I) 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
(I) 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, (discussion under) checksum.

$ protected distribution system
(I) A wireline or fiber-optic system that includes sufficient safeguards (acoustic, electric, electromagnetic, and physical) to permit its use for unencrypted transmission of (cleartext) data.

$ protection authority
See: (secondary definition under) Internet Protocol Security Option.

$ protection ring
(I) One of a hierarchy of privileged operation modes of a system that gives certain access rights to processes authorized to operate in that mode.

$ protocol
(I) A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. (E.g., see: Internet Protocol.)

(C) In particular, a series of ordered steps involving computing and communication that are performed by two or more system entities to achieve a joint objective. [A9042]

$ protocol suite
(I) A complementary collection of communication protocols used in a computer network. (See: Internet, OSI.)

$ proxy server
(I) A computer process--often used as, or as part of, a firewall--that relays 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.)

(C) In a firewall, a proxy server usually runs on a bastion host, which may support proxies for several 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 remote 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.

(C) 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 capability. A proxy at OSI layer 7 can also provide finer-grained security service than can a filtering router at OSI layer 3. For example, an FTP proxy could permit transfers out of, but not into, a protected network.

$ pseudo-random
(I) A sequence of values that appears to be random (i.e., unpredictable) but is actually generated by a deterministic algorithm. (See: random.)

$ pseudo-random number generator
(I) A process used to deterministically generate a series of numbers (usually integers) that appear to be random according to certain statistical tests, but actually are pseudo-random.

(C) Pseudo-random number generators are usually implemented in software.

$ public component
(I) A synonym for "public key".

(D) In most cases, ISDs SHOULD NOT use this term; to avoid confusing readers, use "private key" instead. However, the term MAY be used when specifically discussing a key pair; e.g., "A key pair has a public component and a private component."

$ public key
(I) The publicly-disclosable component of a pair of cryptographic keys used for asymmetric cryptography. (See: key pair, private key.)

(O) "(In a public key cryptosystem) that key of a user's key pair which is publicly known." [X509]

$ public-key certificate
(I) A digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items; a digitally-signed data structure that attests to the ownership of a public key. (See: X.509 public-key certificate.)

(C) 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.

(O) "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." [X509]

$ public-key cryptography
(I) The popular synonym for "asymmetric cryptography".

$ Public-Key Cryptography Standards (PKCS)
(I) A series of specifications published by RSA Laboratories for data structures and algorithm usage for basic applications of asymmetric cryptography. (See: PKCS #7, PKCS #10, PKCS #11.)

(C) 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)
(I) 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.

(C) Some existing RFCs use the term "perfect forward secrecy" but either do not define it or do not define it precisely. While preparing this Glossary, we tried to find a good definition for that term, but 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 algorithm. The term "public-key forward secrecy" (suggested by Hilarie Orman) and the "I" definition stated for it here were crafted to be compatible with current Internet documents, yet be narrow and leave room for improved terminology.

(C) Challenge to the Internet security community: We need a taxonomy--a family of mutually exclusive and collectively exhaustive terms and definitions to cover the basic properties discussed here--for the full range of cryptographic algorithms and protocols used in Internet Standards:

(C) 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.

(C) 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.

(C) 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 long-term 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.

(C) 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.

(C) Acknowledgements: Bill Burr, Burt Kaliski, Steve Kent, Paul Van Oorschot, Michael Wiener, and, especially, Hilarie Orman contributed ideas to this discussion.

$ public-key infrastructure (PKI)
(I) 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.)

(O) PKIX usage: The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

(C) 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.

(C) A number of other servers and agents may support the core PKI, and PKI clients may obtain services from them. 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, and time stamp agent.

$ RA
See: registration authority.

$ RA domains
(I) A capability of a CAW that allows a CA to divide the responsibility for certification requests among multiple RAs.

(C) This capability might be used to restrict access to private authorization data that is provided with a certification request, and to distribute the responsibility to review and approve certification requests in high volume environments. RA domains might segregate certification requests according to an attribute of the certificate subject, such as an organizational unit.

$ RADIUS
See: Remote Authentication Dial-In User Service.

$ Rainbow Series
(O) 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
(I) General usage: In mathematics, random means "unpredictable". A sequence of values is called random if each successive value is obtained merely by chance and does not depend on the preceding values of the sequence, and a selected individual value is called random if each of the values in the total population of possibilities has equal probability of being selected. [Knuth] (See: cryptographic key, pseudo-random, random number generator.)

(I) Security usage: In cryptography and other security applications, random means not only unpredictable, but also "unguessable". When selecting data values to use for cryptographic keys, "the requirement is for data that an adversary has a very low probability of guessing or determining." It is not sufficient to use data that "only meets traditional statistical tests for randomness or which is based on limited range sources, such as clocks. Frequently such random quantities are determinable [i.e., guessable] by an adversary searching through an embarrassingly small space of possibilities." [R1750]

$ random number generator
(I) A process used to generate an unpredictable, uniformly distributed series of numbers (usually integers). (See: pseudo-random, random.)

(C) True random number generators are hardware-based devices that depend on the output of a "noisy diode" or other physical phenomena. [R1750]

$ RBAC
See: Role-Based Access Control.

$ RC2
$ RC4
See: Rivest Cipher #2, Rivest Cipher #4.

$ realm
(O) Kerberos usage: The domain of authority of a Kerberos server (consisting of an authentication server and a ticket-granting server), including the Kerberized clients and the Kerberized application servers

$ RED
(I) Designation for information system equipment or facilities that handle (and for data that contains) only plaintext (or, depending on the context, classified information), and for such data itself. This term derives from U.S. Government COMSEC terminology. (See: BLACK, RED/BLACK separation.)

$ Red Book
(D) ISDs SHOULD NOT use this term as a synonym for "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria" [NCS05]. Instead, use the full proper name of the document or, in subsequent references, a more conventional abbreviation. (See: TCSEC, Rainbow Series, (usage note under) Green Book.)

$ RED/BLACK separation
(I) An architectural concept for cryptographic systems that strictly separates the parts of a system that handle plaintext (i.e., RED information) from the parts that handle ciphertext (i.e., BLACK information). This term derives from U.S. Government COMSEC terminology. (See: BLACK, RED.)

$ reference monitor
(I) "An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects." [NCS04] (See: security kernel.)

(C) 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
(I) A type of replay attack in which transmitted data is sent back to its originator.

$ register
$ registration
(I) 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.)

(C) 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 authenticating the entity's identity and verifying the correctness of the other attributes, in accordance with the CA's CPS.

(C) Among the registration issues that a CPS may address are the following [R2527]:

- 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)

(I) 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: organizational registration authority, registration.)

(C) 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 component, 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, and handling revocation reports. (Such functions may be assigned to a PKI element that is separate from both the CA and the RA.)

(I) PKIX usage: 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. [R2510]

(O) SET usage: "An independent third-party organization that processes payment card applications for multiple payment card brands and forwards applications to the appropriate financial institutions." [SET2]

$ regrade
(I) Deliberately change the classification level of information in an authorized manner.

$ rekey
(I) Change the value of a cryptographic key that is being used in an application of a cryptographic system. (See: certificate rekey.)

(C) For example, rekey is required at the end of a cryptoperiod or key lifetime.

$ reliability
(I) The ability of a system to perform a required function under stated conditions for a specified period of time. (See: availability, survivability.)

$ relying party
(N) A synonym for "certificate user". Used in a legal context to mean a recipient of a certificate who acts in reliance on that certificate. (See: ABA Guidelines.)

$ Remote Authentication Dial-In User Service (RADIUS)
(I) An Internet protocol [R2138] 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.)

(C) A user of the RADIUS client presents authentication information to the client, and the client passes that information to the RADIUS server. The server authenticates the client using a shared secret value, then checks the user's authentication information, and finally returns to the client all authorization and configuration information needed by the client to deliver service to the user.

$ renew
See: certificate renewal.

$ replay attack
(I) An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack. (See: active wiretapping.)

$ repository
(I) A system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users. (See: directory.)

(O) "A trustworthy system for storing and retrieving certificates or other information relevant to certificates." [ABA]

(C) 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 Federal Public-key Infrastructure, for example, the expected repository is a directory that uses LDAP, but also may be the X.500 Directory that uses DAP, or an HTTP server, or an FTP server that permits anonymous login.

$ repudiation
(I) Denial by a system entity that was involved in an association (especially an association that transfers information) of having participated in the relationship. (See: accountability, non-repudiation service.)

(O) "Denial by one of the entities involved in a communication of having participated in all or part of the communication." [I7498 Part 2]

$ Request for Comment (RFC)
(I) One of the documents in the archival series that is the official channel for ISDs and other publications of the Internet Engineering Steering Group, the Internet Architecture Board, and the Internet community in general. [R2026, R2223] (See: Internet Standard.)

(C) This term is *not* a synonym for "Internet Standard".

$ residual risk
(I) The risk that remains after countermeasures have been applied.

$ restore
See: card restore.

$ revocation
See: certificate revocation.

$ revocation date
(N) In an X.509 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.)

(C) 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.

$ risk
(I) An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

(O) SET usage: "The possibility of loss because of one or more threats to information (not to be confused with financial or business risk)." [SET2]

$ risk analysis
$ risk assessment
(I) A process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

(C) The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first. It is usually financially and technically infeasible to counteract all aspects of risk, and so some residual risk will remain, even after all available countermeasures have been deployed. [FP031, R2196]

$ risk management
(I) The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. (See: risk analysis.)

$ Rivest Cipher #2 (RC2)
(N) A proprietary, variable-key-length block cipher invented by Ron Rivest for RSA Data Security, Inc. (now a wholly-owned subsidiary of Security Dynamics, Inc.).

$ Rivest Cipher #4 (RC4)
(N) A proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc. (now a wholly-owned subsidiary of Security Dynamics, Inc.).

$ Rivest-Shamir-Adleman (RSA)
(N) An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman [RSA78, Schn].

(C) 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.

(C) 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).

(C) 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 destroyed after computing n.)

(C) 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) = m to recover m.

(C) 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.

(C) 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 (as explained for 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.

$ role-based access control (RBAC)
(I) A form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process.

$ root
(I) A CA that is directly trusted by an end entity. Acquiring the value of a root CA's public key involves an out-of-band procedure.

(I) Hierarchical PKI usage: 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 trust. (See: top CA.)

(C) In a hierarchical PKI, a root 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. 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.

(O) MISSI usage: 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.

(O) UNIX usage: A user account (also called "superuser") that has all privileges (including all security-related privileges) and thus can manage the system and its other user accounts.

$ root certificate
(I) A certificate for which the subject is a root.

(I) Hierarchical PKI usage: The self-signed public-key certificate at the top of a certification hierarchy.

$ root key
(I) A public key for which the matching private key is held by a root.

$ root registry
(O) MISSI usage: A name previously used for a MISSI policy approving authority.

$ router
(I) A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that internetwork. The most common form of router operates on IP packets. (See: bridge.)

(I) Internet usage: In the context of the Internet protocol suite, a networked computer that forwards Internet Protocol packets that are not addressed to the computer itself. (See: host.)

$ RSA
See: Rivest-Shamir-Adleman.

$ rule-based security policy
(I) "A security policy based on global 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." [I7498 Part 2] (See: identity-based security policy.)

$ safety
(I) The property of a system being free from risk of causing harm to system entities and outside entities.

$ SAID
See: security association identifier.

$ salt
(I) A random value that is concatenated with a password before applying the one-way encryption function used to protect passwords that are stored in the database of an access control system. (See: initialization value.)

(C) Salt protects a password-based access control system against a dictionary attack.

$ sanitize
(I) Delete sensitive data from a file, a device, or a system; or modify data so as to be able to downgrade its classification level.

$ SASL
See: Simple Authentication and Security Layer.

$ SCA
See: subordinate certification authority.

$ scavenging
See: (secondary definition under) threat consequence.

$ screening router
(I) A synonym for "filtering router".

$ SDE
See: Secure Data Exchange.

$ SDNS
See: Secure Data Network System.

$ seal
(O) To use cryptography to provide data integrity service for a data object. (See: sign, wrap.)

(D) ISDs SHOULD NOT use this definition; instead, use language that is more specific with regard to the mechanism(s) used, such as "sign" when the mechanism is digital signature.

$ secret
(I) (1.) Adjective: The condition of information being protected from being known by any system entities except those who are intended to know it. (2.) Noun: An item of information that is protected thusly.

(C) This term applies to symmetric keys, private keys, and passwords.

$ secret-key cryptography
(I) A synonym for "symmetric cryptography".

$ Secure Data Exchange (SDE)
(N) A local area network security protocol defined by the IEEE 802.10 standard.

$ Secure Data Network System (SDNS)
(N) An NSA program that developed security protocols for electronic mail (Message Security Protocol), OSI layer 3 (SP3), OSI layer 4 (SP4), and key management (KMP).

$ Secure Hash Standard (SHS)
(N) The U.S. Government standard [FP180] that specifies the Secure Hash Algorithm (SHA-1), a cryptographic hash function that produces a 160-bit output (hash result) for input data of any length < 2**64 bits.

$ Secure Hypertext Transfer Protocol (Secure-HTTP, S-HTTP)
(I) A Internet protocol for providing client-server security services for HTTP communications. (See: https.)

(C) 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 both asymmetric and symmetric key operation modes. 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 (S/MIME)
(I) Secure/Multipurpose Internet Mail Extensions, an Internet protocol [R2633] to provide encryption and digital signatures for Internet mail messages.

$ Secure Sockets Layer (SSL)
(N) 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.)

(C) SSL is layered below HTTP and above a reliable transport protocol (TCP). SSL is independent of the application it encapsulates, and any higher level protocol can layer on top of SSL transparently. However, many Internet applications might be better served by IPsec.

(C) SSL has two layers: (a) SSL's lower layer, the SSL Record Protocol, is layered on top of the transport protocol and encapsulates higher level protocols. One such encapsulated protocol is SSL Handshake Protocol. (b) SSL's upper layer provides 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 enables them to negotiate a symmetric encryption algorithm and secret session key (to use for data confidentiality) before the application protocol transmits or receives data. A keyed hash provides data integrity service for encapsulated data.

$ secure state
(I) A system condition in which no subject can access any object in an unauthorized manner. (See: (secondary definition under) Bell-LaPadula Model, clean system.)

$ security
(I) (1.) Measures taken to protect a system. (2.) The condition of a system that results from the establishment and maintenance of

measures to protect the system. (3.) The condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

$ security architecture
(I) 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 elements required to implement the services, and (c) the performance levels required in the elements to deal with the threat environment. (See: (discussion under) security policy.)

(C) 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 (e.g., see: [R2179]). A complete security architecture needs to deal with both intentional, intelligent threats and accidental kinds of threats.

$ security association
(I) A relationship established between two or more entities to enable them to protect data they exchange. The relationship is used to negotiate characteristics of protection mechanisms, but does not include the mechanisms themselves. (See: association.)

(C) A security association describes how entities will use security services. The relationship is represented by a set of information that is shared between the entities and is agreed upon and considered a contract between them.

(O) IPsec usage: 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 selected, 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.

$ security association identifier (SAID)
(I) A data field in a security protocol (such as NLSP or SDE), used to identify the security association to which a protocol data unit is bound. The SAID value is usually used to select a key for decryption or authentication at the destination. (See: Security Parameter Index.)

$ security audit
(I) 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. [I7498 Part 2, NCS01]

(C) 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 attacks and security compromises.

$ security audit trail
(I) 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. [NCS04] (See: security audit.)

$ security class
(D) A synonym for "security level". For consistency, ISDs SHOULD use "security level" instead of "security class".

$ security clearance
(I) 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
(I) A security violation in which a system resource is exposed, or is potentially exposed, to unauthorized access. (See: data compromise, violation.)

$ security domain
See: domain.

$ security environment
(I) The set of external entities, procedures, and conditions that affect secure development, operation, and maintenance of a system.

$ security event
(I) A occurrence in a system that is relevant to the security of the system. (See: security incident.)

(C) The term includes 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:

- 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 information to an X.500 Directory.
- Receiving a key compromise notification.
- Receiving an improper certification request.
- Detecting an alarm condition reported by a cryptographic module.
- Logging the operator in or out.
- Failing a built-in hardware self-test or a software system integrity check.

$ security fault analysis
(I) A security analysis, usually performed on hardware at a logic gate level, gate-by-gate, to determine the security properties of a device when a hardware fault is encountered.

$ security gateway
(I) A gateway that separates trusted (or relatively more trusted) hosts on the internal network side from untrusted (or less trusted) hosts on the external network side. (See: firewall and guard.)

(O) IPsec usage: "An intermediate system that implements IPsec protocols." [R2401] Normally, AH or ESP is implemented to serve a set of internal hosts, providing security services for the hosts when they communicate with other, external hosts or gateways that also implement IPsec.

$ security incident
(I) A security event that involves a security violation. (See: CERT, GRIP, security event, security intrusion, security violation.)

(C) In other words, a security-relevant system event in which the system’s security policy is disobeyed or otherwise breached.

(O) "Any adverse event which compromises some aspect of computer or network security." [R2350]

(D) ISDs SHOULD NOT use this "O" definition because (a) a security incident may occur without actually being harmful (i.e., adverse) and (b) this Glossary defines "compromise" more narrowly in relation to unauthorized access.

$ security intrusion
(I) 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
(I) "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." [NCS04] (See: reference monitor.)

(C) That is, a security kernel is an implementation of a reference monitor for a given hardware base.

$ security label
(I) A marking that is bound to a system resource and that names or designates the security-relevant attributes of that resource. [I7498 Part 2, R1457]

(C) The recommended definition is usefully broad, but usually the term is understood more narrowly as a marking that represents the security level of an information object, i.e., a marking that indicates how sensitive an information object is. [NCS04]

(C) System security mechanisms interpret security labels according to applicable security policy to determine how to control access to the associated information, otherwise constrain its handling, and affix appropriate security markings to visible (printed and displayed) images thereof. [FP188]

$ security level
(I) The combination of a hierarchical classification level and a set of non-hierarchical category designations that represents how sensitive information is. (See: (usage note under) classification level, dominate, lattice model.)

$ security management infrastructure (SMI)
(I) System elements and activities that support security policy by monitoring and controlling security services and mechanisms, distributing security information, and reporting security events. The associated functions are as follows [I7498-4]:

- 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: public-key infrastructure.)

$ security mechanism
(I) A process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system. (See: (discussion under) security policy.)

(C) Some examples of security mechanisms are authentication exchange, checksum, digital signature, encryption, and traffic padding.

$ security model
(I) 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. (See: (discussion under) security policy.)

(C) An example is the Bell-LaPadula Model.

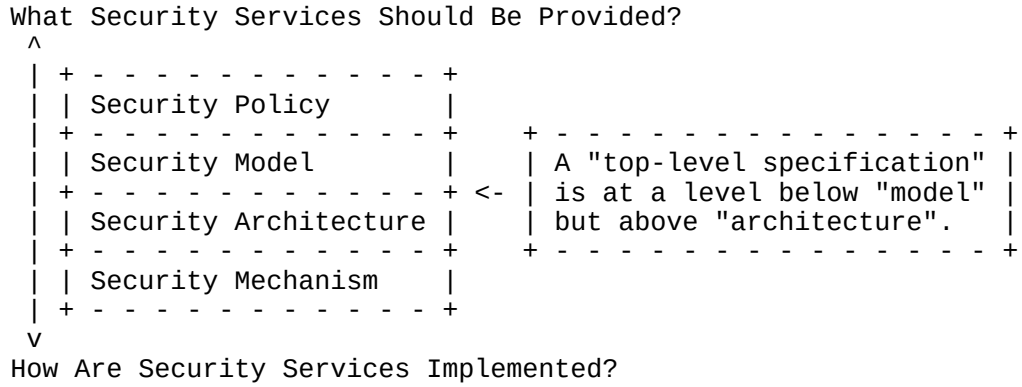
$ security parameters index (SPI)
(I) IPsec usage: The type of security association identifier used in IPsec protocols. A 32-bit value used to distinguish among different security associations terminating at the same destination (IP address) and using the same IPsec security protocol (AH or ESP). Carried in AH and ESP to enable the receiving system to determine under which security association to process a received packet.

$ security perimeter
(I) The boundary of the domain in which a security policy or security architecture applies; i.e., the boundary of the space in which security services protect system resources.

$ security policy
(I) A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources. (See: identity-based security policy, rule-based security policy, security architecture, security mechanism, security model.)

(O) "The set of rules laid down by the security authority governing the use and provision of security services and facilities." [X509]

(C) Ravi Sandhu notes that security policy is one of four layers of the security engineering process (as shown in the following diagram). Each layer provides a different view of security, ranging from what services are needed to how services are implemented.



$ Security Protocol 3 (SP3)
(O) A protocol [SDNS3] developed by SDNS to provide connectionless data security at the top of OSI layer 3. (See: NLSP.)

$ Security Protocol 4 (SP4)
(O) A protocol [SDNS4] developed by SDNS to provide either connectionless or end-to-end connection-oriented data security at the bottom of OSI layer 4. (See: TLSP.)

$ security-relevant event
See: security event.

$ security service
(I) 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.)

(O) "A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or the data transfers." [I7498 Part 2]

(C) Security services implement security policies, and are implemented by security mechanisms.

$ security situation
(I) ISAKMP usage: The set of all security-relevant information--e.g., network addresses, security classifications, manner of operation (normal or emergency)--that is needed to decide the security services that are required to protect the association that is being negotiated.

$ security token
See: token.

$ security violation
(I) An act or event that disobeys or otherwise breaches security policy. (See: compromise, penetration, security incident.)

$ self-signed certificate
(I) 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. (See: root certificate.)

(C) In a self-signed X.509 public-key certificate, the issuer’s DN is the same as the subject’s DN.

$ semantic security
(I) An attribute of a encryption algorithm that is a formalization of the notion that the algorithm not only hides the plaintext but also reveals no partial information about the plaintext. Whatever is efficiently computable about the plaintext when given the ciphertext, is also efficiently computable without the ciphertext. (See: indistinguishability.)

$ sensitive (information)
(I) Information is sensitive if disclosure, alteration, destruction, or loss of the information would adversely affect the interests or business of its owner or user. (See: critical.)

$ separation of duties
(I) The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process. (See: dual control, administrative security.)

$ serial number
See: certificate serial number.

$ server
(I) A system entity that provides a service in response to requests from other system entities called clients.

$ session key
(I) In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. (See: ephemeral key, key distribution center, master key.)

(C) Usually, a session key is used for a defined period of communication between two computers, 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
See: SET Secure Electronic Transaction(trademark).

$ SET private extension
(O) 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
(O) A certificate policy qualifier that provides information about the location and content of a SET certificate policy.

(C) In addition to 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 URL where a copy of the policy statement may be found.
- An electronic mail address where a copy of the policy statement may be found.

- A hash result of the policy statement, computed using the indicated algorithm.
- A statement declaring any disclaimers associated with the issuing of the certificate.

$ SET Secure Electronic Transaction(trademark) or SET(trademark)
(N) 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. [SET1] (See: acquirer, brand, cardholder, dual signature, electronic commerce, issuer, merchant, payment gateway, third party.)

(C) This term and acronym are trademarks of SETCo. MasterCard and Visa announced the SET standard on 1 February 1996. On 19 December 1997, MasterCard and Visa formed SET Secure Electronic Transaction LLC (commonly referred to as "SETCo") to implement the SET 1.0 specification. A memorandum of understanding adds American Express and JCB Credit Card Company as co-owners of SETCo.

$ SETCo
See: (secondary definition under) SET Secure Electronic Transaction.

$ SHA-1
See: Secure Hash Standard.

$ shared secret
(I) A synonym for "keying material" or "cryptographic key".

$ S-HTTP
See: Secure HTTP.

$ sign
(I) Create a digital signature for a data object.

$ signature
See: digital signature, electronic signature.

$ signature certificate
(I) 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.

(C) A v3 X.509 public-key certificate may have a "keyUsage" extension which indicates the purpose for which the certified public key is intended.

$ signer
(N) A human being or an organization entity that uses its private key to create a digital signature for a data object. [ABA]

$ SILS
See: Standards for Interoperable LAN/MAN Security.

$ simple authentication
(I) An authentication process that uses a password as the information needed to verify an identity claimed for an entity. (See: strong authentication.)

(O) "Authentication by means of simple password arrangements." [X509]

$ Simple Authentication and Security Layer (SASL)
(I) An Internet specification [R2222] for adding authentication service to connection-based protocols. 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, GSSAPI, 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. [R2356] (See: IKE, IPsec.)

(C) SKIP uses the Diffie-Hellman 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 of the entities to the other. The KEK is used with a symmetric algorithm 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)
(I) A TCP-based, application-layer, Internet Standard protocol [R0821] for moving electronic mail messages from one computer to another.

$ Simple Network Management Protocol (SNMP)
(I) A UDP-based, application-layer, Internet Standard protocol [R2570, R2574] for conveying management information between managers and agents.

(C) SNMP version 1 uses cleartext passwords for authentication and access control. (See: community string.) Version 2 adds cryptographic mechanisms based on DES and MD5. Version 3 provides enhanced, integrated support for security services, including data confidentiality, data integrity, data origin authentication, and message timeliness and limited replay protection.

$ simple security property
See: (secondary definition under) Bell-LaPadula Model.

$ single sign-on
(I) A system that enables a user to access multiple computer platforms (usually a set of hosts on the same network) or application systems after being authenticated just one time. (See: Kerberos.)

(C) Typically, a user logs in just once, and then is transparently granted access to a variety of permitted resources with no further login being required until after the user logs out. Such a system has the advantages of being user friendly and enabling authentication to be managed consistently across an entire enterprise, and has the disadvantage of requiring all hosts and applications to trust the same authentication mechanism.

$ situation
See: security situation.

$ S/Key
(I) A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. [R1760]

(C) 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.

$ SKIP
See: Simple Key-management for IP.

$ SKIPJACK
(N) A Type II block cipher [NIST] with a block size of 64 bits and a key size of 80 bits, that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level. (See: CAPSTONE, CLIPPER, FORTEZZA, Key Exchange Algorithm.)

(C) On 23 June 1998, NSA announced that SKIPJACK had been declassified.

$ slot
(O) MISSI usage: One of the FORTEZZA PC card storage areas that are each able to hold an X.509 certificate and additional data that is associated with the certificate, such as the matching private key.

$ smart card
(I) A credit-card sized device containing one or more integrated circuit chips, which perform the functions of a computer’s central processor, memory, and input/output interface. (See: PC card.)

(C) 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. At other times, the term is used loosely to include cards that are larger than credit cards, especially cards that are thicker, such as PC cards.

(C) A "smart token" is a device that conforms to the definition of smart card except that rather than having standard credit card dimensions, the token is packaged in some other form, such as a dog tag or door key shape.

$ smart token
See: (secondary definition under) smart card.

$ SMI
See: security management infrastructure.

$ S/MIME
See: Secure/MIME.

$ SMTP
See: Simple Mail Transfer Protocol.

$ smurf
(I) Software that mounts a denial-of-service attack ("smurfing") by exploiting IP broadcast addressing and ICMP ping packets to cause flooding. (See: flood, ICMP flood.)

(D) ISDs SHOULD NOT use this term because it is not listed in most dictionaries and could confuse international readers.

(C) A smurf program builds a network packet that appears to originate from another address, that of the "victim", either a host or an IP router. The packet contains an ICMP ping message that is addressed to an IP broadcast address, i.e., to all IP addresses in a given network. The echo responses to the ping message return to the victim's address. The goal of smurfing may be either to deny service at a particular host or to flood all or part of an IP network.

$ sniffing
(C) A synonym for "passive wiretapping". (See: password sniffing.)

(D) ISDs SHOULD NOT use this term because it unnecessarily duplicates the meaning of a term that is better established. (See: (usage note under) Green Book.

$ SNMP
See: Simple Network Management Protocol.

$ social engineering
(I) A euphemism for non-technical or low-technology means--such as lies, impersonation, tricks, bribes, blackmail, and threats--used to attack information systems. (See: masquerade attack.)

(D) ISDs SHOULD NOT use this term because it is vague; instead, use a term that is specific with regard to the means of attack.

$ SOCKS
(I) An Internet protocol [R1928] that provides a generalized proxy server that enables client-server applications--such as TELNET, FTP, and HTTP; running over either TCP or UDP--to use the services of a firewall.

(C) SOCKS is layered under the 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
(O) The use of software techniques to reduce the radio frequency information leakage from computer displays and keyboards. [Kuhn] (See: TEMPEST.)

$ software
(I) 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. (See: firmware, hardware.)

$ SORA
See: SSO-PIN ORA.

$ source authentication
(D) ISDs SHOULD NOT use this term because it is ambiguous. If the intent is to authenticate the original creator or packager of data received, then say "data origin authentication". If the intent is to authenticate the identity of the sender of data, then say "peer entity authentication". (See: data origin authentication, peer entity authentication).

$ source integrity
(I) The degree of confidence that can be placed in information based on the trustworthiness of its sources. (See: integrity.)

$ SP3
See: Security Protocol 3.

$ SP4
See: Security Protocol 4.

$ spam
(I) (1.) Verb: To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. (2.) Noun: electronic "junk mail". [R2635]

(D) This term SHOULD NOT be written in upper-case 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 commercial email (UCE)], 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."

(C) In sufficient volume, spam can cause denial of service. (See: flooding.) According to the SPAM Web site, the term was adopted as a result of the Monty Python skit in which a group of Vikings sang a chorus of 'SPAM, SPAM, SPAM . . .' in an increasing crescendo, drowning out other conversation. Hence, the analogy applied because UCE was drowning out normal discourse on the Internet.

$ SPC
See: software publisher certificate.

$ SPI
See: Security Parameters Index.

$ split key
(I) A cryptographic key that is divided into 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
(I) A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items. (See: dual control, split key.)

(O) "A condition under which two or more entities separately have key components which individually convey no knowledge of the plaintext key which will be produced when the key components are combined in the cryptographic module." [FP140]

$ spoofing attack
(I) A synonym for "masquerade attack".

$ SSH
(I) A protocol for secure remote login and other secure network services over an insecure network.

(C) Consists of three major components:

- Transport layer protocol: Provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used 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.

$ SSL
See: Secure Sockets Layer, Standard Security Label.

$ SSO
See: system security officer.

$ SSO PIN
(O) MISSI usage: One of two personal identification numbers that control access to the functions and stored data of a FORTEZZA PC card. Knowledge of the SSO PIN enables the card user to perform the FORTEZZA functions intended for use by an end user and also the functions intended for use by a MISSI certification authority. (See: user PIN.)

$ SSO-PIN ORA (SORA)
(O) MISSI usage: 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 an end user's FORTEZZA PC card.

$ Standards for Interoperable LAN/MAN Security (SILS)
(N) (1.) The IEEE 802.10 standards committee. (2.) A developing 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
(I) (Written "*-property".) See: "confinement property" under Bell-LaPadula Model.

$ Star Trek attack
(C) An attack that penetrates your system where no attack has ever gone before.

$ steganography
(I) 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. (See: cryptology.)

(C) An example of a steganographic method is "invisible" ink. (See: digital watermark.)

$ storage channel
See: (secondary definition under) covert channel.

$ stream cipher
(I) An encryption algorithm that breaks plaintext into a stream of successive bits (or characters) and encrypts the n-th plaintext bit with the n-th element of a parallel key stream, thus converting the plaintext bit stream into a ciphertext bit stream. [Schn] (See: block cipher.)

$ strong authentication
(I) An authentication process that uses cryptography--particularly public-key certificates--to verify the identity claimed for an entity. (See: X.509.)

(O) "Authentication by means of cryptographically derived credentials." [X509]

$ subject
1. (I) In a computer system: A system entity that causes information to flow among objects or changes the system state; technically, a process-domain pair. (See: Bell-LaPadula Model.)

2. (I) Of a certificate: The entity name that is bound to the data items in a digital certificate, and particularly a name that is bound to a key value in a public-key certificate.

$ subnetwork
(N) An OSI term for a system of packet relays and connecting links that implement the lower three protocol layers of the OSIRM to provide a communication service that interconnects attached end systems. Usually the relays operate at OSI layer 3 and are all of the same type (e.g., all X.25 packet switches, or all interface units in an IEEE 802.3 LAN). (See: gateway, internet, router.)

$ subordinate certification authority (SCA)
(I) A CA whose public-key certificate is issued by another (superior) CA. (See: certification hierarchy.)

(O) MISSI usage: The fourth-highest (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 distinguished name
(I) 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>.

$ superencryption
(I) An encryption operation for which the plaintext input to be transformed is the ciphertext output of a previous encryption operation.

$ survivability
(I) The ability of a system to remain in operation or existence despite adverse conditions, including both natural occurrences, accidental actions, and attacks on the system. (See: availability, reliability.)

$ symmetric cryptography
(I) A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). (See: asymmetric cryptography.)

(C) Symmetric cryptography has been used for thousands of years [Kahn]. A modern example of a symmetric encryption algorithm is the U.S. Government’s Data Encryption Algorithm. (See: DEA, DES.)

(C) Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key, such as the originator and the recipient of a message, need to keep the key secret. For example, when Alice wants to ensure confidentiality for data she sends to Bob, she encrypts the data with a secret key, and Bob uses the same key to decrypt. Keeping the shared key secret entails both cost and risk when the key is distributed to both Alice and Bob. Thus, symmetric cryptography has a key management disadvantage compared to asymmetric cryptography.

$ symmetric key
(I) A cryptographic key that is used in a symmetric cryptographic algorithm.

$ SYN flood
(I) A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle. (See: flooding.)

$ system
(C) In this Glossary, the term is mainly used as an abbreviation for "automated information system".

$ system entity
(I) An active element of a system--e.g., an automated process, a subsystem, a person or group of persons--that incorporates a specific set of capabilities.

$ system high
(I) The highest security level supported by a system at a particular time or in a particular environment. (See: system high security mode.)

$ system high security mode
(I) A mode of operation of an information system, wherein all users having access to the system possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the system. (See: mode of operation.)

(C) This mode is defined formally in U.S. Department of Defense policy regarding system accreditation [DOD2], but the term is widely used outside the Defense Department and outside the Government.

$ system integrity
(I) "The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation." [NCS04] (See: system integrity service.)

$ system integrity service
(I) A security service that protects system resources in a verifiable manner against unauthorized or accidental change, loss, or destruction. (See: system integrity.)

$ system low
(I) The lowest security level supported by a system at a particular time or in a particular environment. (See: system high.)

$ system resource
(I) Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

$ system security officer (SSO)
(I) A person responsible for enforcement or administration of the security policy that applies to the system.

$ system verification
See: (secondary definition under) verification.

$ TACACS
$ TACACS+
See: Terminal Access Controller (TAC) Access Control System.

$ tamper
(I) 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.

$ TCB
See: trusted computing base.

$ TCP
See: Transmission Control Protocol.

$ TCP/IP
(I) A synonym for "Internet Protocol Suite", in which the Transmission Control Protocol (TCP) and the Internet Protocol (IP) are important parts.

$ TCSEC
See: Trusted Computer System Evaluation Criteria.

$ TELNET
(I) A TCP-based, application-layer, Internet Standard protocol [R0854] for remote login from one host to another.

$ TEMPEST
(O) A nickname for specifications and standards for limiting the strength of electromagnetic emanations from electrical and electronic equipment and thus reducing vulnerability to eavesdropping. This term originated in the U.S. Department of Defense. [Army, Kuhn, Russ] (See: emanation security, soft tempest.)

(D) ISDs SHOULD NOT use this term as a synonym for "electromagnetic emanations security".

$ Terminal Access Controller (TAC) Access Control System (TACACS)
(I) A UDP-based authentication and access control protocol [R1492] 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.

(C) TACACS was developed for ARPANET and has evolved for use in commercial equipment. TACs were a type of network access server computer used to connect terminals to the early Internet, usually using dial-up modem connections. TACACS used centralized authentication servers and served not only network access servers like TACs but also routers and other networked computing devices. TACs are no longer in use, but TACACS+ is. [R1983]

- "XTACACS": The name of Cisco Corporation's implementation, which enhances and extends the original TACACS.

- "TACACS+": A TCP-based protocol that improves on TACACS and XTACACS by separating the functions of authentication, authorization, and accounting and by encrypting all traffic between the network access server and authentication server. It is extensible to allow any authentication mechanism to be used with TACACS+ clients.

$ TESS
See: The Exponential Encryption System.

$ The Exponential Encryption System (TESS)
(I) 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 employs asymmetric cryptography, based on discrete exponentiation, and a structure of self-certified public keys. [R1824]

$ threat
(I) A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. (See: attack, threat action, threat consequence.)

(C) That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal

organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).

(C) In some contexts, such as the following, the term is used narrowly to refer only to intelligent threats:

(N) U. S. Government usage: The technical and operational capability of a hostile entity to detect, exploit, or subvert friendly information systems and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

$ threat action
(I) An assault on system security. (See: attack, threat, threat consequence.)

(C) A complete security architecture deals with both intentional acts (i.e. attacks) and accidental events [FIPS31]. Various kinds of threat actions are defined as subentries under "threat consequence".

$ threat analysis
(I) An analysis of the probability of occurrences and consequences of damaging actions to a system.

$ threat consequence
(I) A security violation that results from a threat action. Includes disclosure, deception, disruption, and usurpation. (See: attack, threat, threat action.)

(C) The following subentries describe four kinds of threat consequences, and also list and describe the kinds of threat actions that cause each consequence. Threat actions that are accidental events are marked by "*".

1. "(Unauthorized) Disclosure" (a threat consequence): A circumstance or event whereby an entity gains access to data for which the entity is not authorized. (See: data confidentiality.) The following threat actions can cause unauthorized disclosure:

   A. "Exposure": A threat action whereby sensitive data is directly released to an unauthorized entity. This includes:

      a. "Deliberate Exposure": Intentional release of sensitive data to an unauthorized entity.

b. "Scavenging": Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

c* "Human error": Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data.

d* "Hardware/software error". System failure that results in an entity gaining unauthorized knowledge of sensitive data.

B. "Interception": A threat action whereby an unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. This includes:

a. "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.

b. "Wiretapping (passive)": Monitoring and recording data that is flowing between two points in a communication system. (See: wiretapping.)

c. "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 is not intended to communicate the data. (See: emanation.)

C. "Inference": A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. This includes:

a. Traffic analysis: Gaining knowledge of data by observing the characteristics of communications that carry the data. (See: (main Glossary entry for) traffic analysis.)

b. "Signals analysis": Gaining indirect knowledge 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.)

D. "Intrusion": A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system’s security protections. This includes:

a. "Trespass": Gaining unauthorized physical access to sensitive data by circumventing a system's protections.

b. "Penetration": Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

c. "Reverse engineering": Acquiring sensitive data by disassembling and analyzing the design of a system component.

d. Cryptanalysis: Transforming encrypted data into plaintext without having prior knowledge of encryption parameters or processes. (See: (main Glossary entry for) cryptanalysis.)

2. "Deception" (a threat consequence): A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. The following threat actions can cause deception:

A. "Masquerade": A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. (See: (main Glossary entry for) masquerade attack.)

a. "Spoof": Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

b. "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: (main Glossary entry for) malicious logic.)

B. "Falsification": A threat action whereby false data deceives an authorized entity. (See: active wiretapping.)

a. "Substitution": Altering or replacing valid data with false data that serves to deceive an authorized entity.

b. "Insertion": Introducing false data that serves to deceive an authorized entity.

C. "Repudiation": A threat action whereby an entity deceives another by falsely denying responsibility for an act. (See: non-repudiation service, (main Glossary entry for) repudiation.)

a. "False denial of origin": Action whereby the originator of data denies responsibility for its generation.

b. "False denial of receipt": Action whereby the recipient of data denies receiving and possessing the data.

3. "Disruption" (a threat consequence): A circumstance or event that interrupts or prevents the correct operation of system services and functions. (See: denial of service.) The following threat actions can cause disruption:

A. "Incapacitation": A threat action that prevents or interrupts system operation by disabling a system component.

a. "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: (main Glossary entry for) malicious logic.)

b. "Physical destruction": Deliberate destruction of a system component to interrupt or prevent system operation.

c* "Human error": Action or inaction that unintentionally disables a system component.

d* "Hardware or software error": Error that causes failure of a system component and leads to disruption of system operation.

e* "Natural disaster": Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component. [FP031 section 2]

B. "Corruption": A threat action that undesirably alters system operation by adversely modifying system functions or data.

a. "Tamper": In context of corruption, deliberate alteration of a system's logic, data, or control information to interrupt or prevent correct operation of system functions.

b. "Malicious logic": In context of corruption, any hardware, firmware, or software (e.g., a computer virus) intentionally introduced into a system to modify system functions or data. (See: (main Glossary entry for) malicious logic.)

c* "Human error": Human action or inaction that unintentionally results in the alteration of system functions or data.

d* "Hardware or software error": Error that results in the alteration of system functions or data.

e* "Natural disaster": Any "act of God" (e.g., power surge caused by lightning) that alters system functions or data. [FP031 section 2]

C. "Obstruction": A threat action that interrupts delivery of system services by hindering system operations.

a. "Interference": Disruption of system operations by blocking communications or user data or control information.

b. "Overload": Hindrance of system operation by placing excess burden on the performance capabilities of a system component. (See: flooding.)

4. "Usurpation" (a threat consequence): A circumstance or event that results in control of system services or functions by an unauthorized entity. The following threat actions can cause usurpation:

A. "Misappropriation": A threat action whereby an entity assumes unauthorized logical or physical control of a system resource.

a. "Theft of service": Unauthorized use of service by an entity.

b. "Theft of functionality": Unauthorized acquisition of actual hardware, software, or firmware of a system component.

c. "Theft of data": Unauthorized acquisition and use of data.

B. "Misuse": A threat action that causes a system component to perform a function or service that is detrimental to system security.

a. "Tamper": In context of misuse, deliberate alteration of a system’s logic, data, or control information to cause the system to perform unauthorized functions or services.

b. "Malicious logic": In context of misuse, any hardware, software, or firmware intentionally introduced into a system to perform or control execution of an unauthorized function or service.

c. "Violation of permissions": Action by an entity that exceeds the entity's system privileges by executing an unauthorized function.

$ thumbprint
(I) A pattern of curves formed by the ridges on the tip of a thumb. (See: biometric authentication, fingerprint.)

(D) ISDs SHOULD NOT use this term as a synonym for "hash result" because that meaning mixes concepts in a potentially misleading way.

$ ticket
(I) A synonym for "capability". (See: Kerberos.)

(C) 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 have been implemented with symmetric cryptography, but can also be implemented as attribute certificates using asymmetric cryptography.

$ timing channel
See: (secondary definition under) covert channel.

$ TLS
See: Transport Layer Security. (See: TLSP.)

$ TLSP
See: Transport Layer Security Protocol. (See: TLS.)

$ token
1. (I) General usage: 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.

2. (I) Authentication usage: A data object or a portable, user-controlled, physical device used to verify an identity in an authentication process. (See: authentication information, dongle.)

3. (I) Cryptographic usage: See: cryptographic token.

4. (O) SET usage: "A portable device [e.g., smart card or PCMCIA card] specifically designed to store cryptographic information and possibly perform cryptographic functions in a secure manner." [SET2]

$ token backup
(I) 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
(I) 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
(I) The process of initializing security tokens (e.g., see: smart card), loading data into the tokens, and controlling the tokens during their life cycle. 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
(I) 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.

$ token storage key
(I) A cryptography key used to protect data that is stored on a security token.

$ top CA
(I) A CA that is the highest level (i.e., is the most trusted CA) in a certification hierarchy. (See: root.)

$ top-level specification
(I) "A non-procedural description of system behavior at the most abstract level; typically a functional specification that omits all implementation details." [NCS04] (See: (discussion under) security policy.)

(C) 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.)

$ traffic analysis
(I) Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence. (See: wiretapping.)

(O) "The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency)." [I7498 Part 2]

$ traffic flow confidentiality
(I) A data confidentiality service to protect against traffic analysis.

(O) "A confidentiality service to protect against traffic analysis." [I7498 Part 2]

$ traffic padding
(I) "The generation of spurious instances of communication, spurious data units, and/or spurious data within data units." [I7498 Part 2]

$ tranquillity property
See: (secondary definition under) Bell-LaPadula Model.

$ Transmission Control Protocol (TCP)
(I) An Internet Standard protocol [R0793] that reliably delivers a sequence of datagrams (discrete sets of bits) from one computer to another in a computer network. (See: TCP/IP.)

(C) TCP is designed to fit into a layered hierarchy of protocols that support internetwork applications. TCP assumes it can obtain a simple, potentially unreliable datagram service (such as the Internet Protocol) from the lower-layer protocols.

$ Transport Layer Security (TLS)
(I) TLS Version 1.0 is an Internet protocol [R2246] based-on and very similar to SSL Version 3.0. (See: TLSP.)

(C) The TLS protocol is misnamed, because it operates well above the transport layer (OSI layer 4).

$ Transport Layer Security Protocol (TLSP)
(I) An end-to-end encryption protocol(ISO Standard 10736) that provides security services at the bottom of OSI layer 4, i.e., directly above layer 3. (See: TLS.)

(C) TLSP evolved directly from the SP4 protocol of SDNS.

$ transport mode vs. tunnel mode
(I) IPsec usage: Two ways to apply IPsec protocols (AH and ESP) to protect communications:

- "Transport mode": The protection applies to (i.e., the IPsec protocol encapsulates) the packets of upper-layer protocols, the ones that are carried above IP.

- "Tunnel mode": The protection applies to (i.e., the IPsec protocol encapsulates) IP packets.

(C) A transport mode security association is always between two hosts. In a tunnel mode security association, each end may be either a host or a gateway. Whenever either end of an IPsec security association is a security gateway, the association is required to be in tunnel mode.

$ trap door
(I) A hidden computer flaw known to an intruder, or a hidden computer mechanism (usually software) installed by an intruder, who can activate the trap door to gain access to the computer without being blocked by security services or mechanisms. (See: back door, Trojan horse.)

$ triple DES
(I) A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits. [A9052] (See: DES.)

(C) IPsec usage: The algorithm variation proposed for ESP uses a 168-bit key, consisting of three independent 56-bit quantities used by the Data Encryption Algorithm, and a 64-bit initialization value. 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. [R1851]

$ triple-wrapped
(I) S/MIME usage: Data that has been signed with a digital signature, and then encrypted, and then signed again. [R2634]

$ Trojan horse
(I) 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.

$ trust
1. (I) Information system usage: The extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions. (See: trust level.)

(C) "trusted vs. trustworthy": In discussing a system or system process or object, this Glossary (and industry usage) prefers the term "trusted" to describe a system that operates as expected, according to design and policy. When the trust can also be guaranteed in some convincing way, such as through formal analysis or code review, the system is termed "trustworthy"; this differs from the ABA Guidelines definition (see: trustworthy system).

2. (I) PKI usage: 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.

(O) "Generally, an entity can be said to 'trust' a second entity when it (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 and a [certification] authority; an entity shall be certain that it can trust the certification authority to create only valid and reliable certificates." [X509]

$ trust chain
(D) ISDs SHOULD NOT use this term as a synonym for "certification path" because it mixes concepts in a potentially misleading way. (See: trust.)

$ trust-file PKI
(I) A non-hierarchical PKI in which each certificate user has a local file (which is used by application software) of public-key certificates that the user trusts as starting points (i.e., roots) for certification paths. (See: hierarchical PKI, mesh PKI, root, web of trust.)

(C) For example, popular browsers are distributed with an initial file of trusted 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
(D) ISDs SHOULD NOT use this term as a synonym for "certification hierarchy" because this term mixes concepts (see: trust) in a potentially misleading way and duplicates the meaning of another, standardized term. (See: trust, web of trust.)

$ trust level
(I) A characterization of a standard of security protection to be met by a computer system.

(C) The TCSEC defines eight trust levels. From the lowest to the highest, they are D, C1, C2, B1, B2, B3, and A1. A trust level is based not only on the presence of security mechanisms but also on the use of systems engineering discipline to properly structure the system and implementation analysis to ensure that the system provides an appropriate degree of trust.

$ trusted
See: (discussion under) trust.

$ trusted certificate
(I) A certificate upon which a certificate user relies as being valid without the need for validation testing; especially a public-key certificate that is used to provide the first public key in a certification path. (See: certification path, root certificate, validation.)

(C) 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) any certificate accepted by the user in a trust-file PKI.

$ trusted computer system
(I) Multilevel security usage: "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." [NCS04] (See: (discussion under) trust.)

$ Trusted Computer System Evaluation Criteria (TCSEC)
(N) A standard for evaluating the security provided by operating systems [CSC001, DOD1]. Informally called the "Orange Book"

because of the color of its cover; first document in the Rainbow Series. (See: Common Criteria, (usage note under) Green Book, Orange Book, trust level.)

$ trusted computing base (TCB)
(I) "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." [NCS04] (See: (discussion of "trusted" under) trust.)

$ trusted distribution
(I) "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." [NCS04]

$ trusted key
(I) A public key upon which a user relies; especially a public key that can be used as the first public key in a certification path. (See: certification path, root key, validation.)

(C) A trusted public key might 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 path
(I) COMPUSEC usage: A mechanism by which a computer system user can communicate directly and reliably with the trusted computing base (TCB) and that can only be activated by the user or the TCB and cannot be imitated by untrusted software within the computer. [NCS04]

(I) COMSEC usage: 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. [FP140]

$ trusted process
(I) A system process 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, (discussion of "trusted" under) trust.)

$ trusted subnetwork
(I) 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--e.g., telephone lines, or a LAN--are protected from attack by some means.)

$ trusted system
See: (discussion under) trust, trusted computer system, trustworthy system.

$ Trusted Systems Interoperability Group (TSIG)
(N) A forum of computer vendors, system integrators, and users devoted to promoting interoperability of trusted computer systems. TSIG meetings are open to all persons who are working in the INFOSEC area.

$ trustworthy system
(O) ABA usage: "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." [ABA] This differs somewhat from other industry usage. (See: (discussion of "trusted vs. trustworthy" under) trust.)

$ TSIG
See: Trusted System Interoperability Group.

$ tunnel
(I) A communication channel created in a computer network by encapsulating (carrying, layering) a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. (See: L2TP, VPN.)

(C) Tunneling can involve almost any OSI or TCP/IP protocol layers; for example, a TCP connection between two hosts could conceivably be tunneled through email messages across the Internet. Most often, a tunnel is a logical point-to-point link--i.e., an OSI layer 2 connection--created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or internetwork layer protocol (such as IP), or in another link layer protocol. Often, encapsulation is accomplished with an extra, intermediate protocol, i.e., a tunneling protocol (such as L2TP) that is layered between the tunneled layer 2 protocol and the encapsulating protocol.

(C) Tunneling can 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: virtual private network.)

(O) SET usage: 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
(I) IPsec usage: See: transport mode vs. tunnel mode.

$ two-person control
(I) The close surveillance and control of a system, 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.)

$ Type I cryptography
(O) A cryptographic algorithm or device approved by NSA for protecting classified information.

$ Type II cryptography
(O) A cryptographic algorithm or device approved by NSA for protecting sensitive unclassified information (as specified in section 2315 of Title 10 United States Code, or section 3502(2) of Title 44, United States Code.)

$ Type III cryptography
(O) A cryptographic algorithm or device approved as a Federal Information Processing Standard.

$ UDP
See: User Datagram Protocol.

$ unclassified
(I) Not classified.

$ unencrypted
(I) Not encrypted.

$ unforgeable
(I) Cryptographic usage: The property of a cryptographic data structure (i.e., a data structure that is defined using one or more cryptographic functions) 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. (E.g., see: digital certificate.)

(C) 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)
(I) 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. [R1630]

(C) URIs are used in HTML to identify the target of hyperlinks. In common practice, URIs include uniform resource locators [R2368] and relative URLs, and may be URNs. [R1808]

$ uniform resource locator (URL)
(I) A type of formatted identifier that describes the access method and location of an information resource object on the Internet. [R1738]

(C) A URL is a URI that provides explicit instructions on how to access the named object. For example, "ftp://bbnarchive.bbn.com/foo/bar/picture/cambridge.zip" is a URL. 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)
(I) A URI that has an institutional commitment to persistence and availability.

$ untrusted process
(I) A system process that is not able to affect the state of system security through incorrect or malicious operation, usually because its operation is confined by a security kernel. (See: trusted process.)

$ UORA
See: user-PIN ORA.

$ update
See: certificate update and key update.

$ URI
See: uniform resource identifier.

$ URL
See: uniform resource locator.

$ URN
See: uniform resource name.

$ user
(I) A person, organization entity, or automated process that accesses a system, whether authorized to do so or not. (See: [R2504].)

(C) Any ISD that uses this term SHOULD provide an explicit definition, because this term is used in many ways and can easily be misunderstood.

$ User Datagram Protocol (UDP)
(I) An Internet Standard protocol [R0768] that provides a datagram mode of packet-switched computer communication in an internetwork.

(C) UDP is a transport layer protocol, and it 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 end-to-end services that TCP provides.

$ user identifier
(I) A character string or symbol that is used in a system to uniquely name a specific user or group of users.

(C) Often verified by a password in an authentication process.

$ user PIN
(O) MISSI usage: One of two personal identification numbers that control access to the functions and stored data of a FORTEZZA PC card. Knowledge of the user PIN enables the card user to perform the FORTEZZA functions that are intended for use by an end user. (See: SSO PIN.)

$ user-PIN ORA (UORA)
(O) 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
See: (secondary definition under) threat consequence.

$ UTCTime
(N) 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. Note: UTCTime has the Year 2000 problem. (See: Coordinated Universal Time, GeneralizedTime.)

$ v1 certificate
(C) Ambiguously refers to either an X.509 public-key certificate in its version 1 format, or an X.509 attribute certificate in its version 1 format. However, many people who use this term are not aware that X.509 specifies attribute certificates that do not contain a public key. Therefore, ISDs MAY use this term as an abbreviation for "version 1 X.509 public-key certificate", but only after using the full term at the first instance.

(D) ISDs SHOULD NOT use this term as an abbreviation for "version 1 X.509 attribute certificate".

$ v1 CRL
(I) An abbreviation for "X.509 CRL in version 1 format".

(C) ISDs should use this abbreviation only after using the full term at its first occurrence and defining the abbreviation.

$ v2 certificate
(I) An abbreviation for "X.509 public-key certificate in version 2 format".

(C) ISDs should use this abbreviation only after using the full term at its first occurrence and defining the abbreviation.

$ v2 CRL
(I) An abbreviation for "X.509 CRL in version 2 format".

(C) ISDs should use this abbreviation only after using the full term at its first occurrence and defining the abbreviation.

$ v3 certificate
(I) An abbreviation for "X.509 public-key certificate in version 3 format".

(C) ISDs should use this abbreviation only after using the full term at its first occurrence and defining the abbreviation.

$ valid certificate
(I) A digital certificate for which the binding of the data items can be trusted; one that can be validated successfully. (See: validate vs. verify.)

$ valid signature
(D) ISDs SHOULD NOT use this term; instead, use "authentic signature". 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 vs. verify.)

$ validate vs. verify
(C) The PKI community uses words inconsistently when describing what a certificate user does to make certain that a digital certificate can be trusted. Usually, we say "verify the signature" but say "validate the certificate"; i.e., we "verify" atomic truths but "validate" data structures, relationships, and systems that are composed of or depend on verified items. Too often, however, verify and validate are used interchangeably.

ISDs SHOULD comply with the following two rules to ensure consistency and to align Internet security terminology with ordinary English:

- Rule 1: Use "validate" when referring to a process intended to establish the soundness or correctness of a construct. (E.g., see: certificate validation.)

- 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., see: authenticate.)

The rationale for Rule 1 is that "valid" derives from a word that means "strong" in Latin. Thus, to validate means to make sure that a construction is sound. A certificate user validates a public-key certificate to establish trust in the binding that the certificate asserts between an identity and a key. (To validate can also mean to officially approve something; e.g., NIST validates cryptographic modules for conformance with FIPS PUB 140-1.)

The rationale for Rule 2 is that "verify" derives from a word that means "true" in Latin. Thus, to verify means to prove the truth of an assertion by examining evidence or performing tests. 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
(I) 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.

$ value-added network (VAN)
(I) A computer network or subnetwork (which is usually a commercial enterprise) that transmits, receives, and stores EDI transactions on behalf of its customers.

(C) 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. System verification: The process of comparing two levels of system specification for proper correspondence, such as comparing a security policy with a top-level specification, a top-level specification with source code, or source code with object code. [NCS04]

2. Identification verification: Presenting information to establish the truth of a claimed identity.

$ verify
See: validate vs. verify.

$ violation
See: security violation.

$ virtual private network (VPN)
(I) 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 (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

(C) 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 (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. 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 real network.

$ virus
(I) A hidden, self-replicating 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.

$ VPN
See: virtual private network.

$ vulnerability
(I) 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.

(C) Most systems have vulnerabilities of some sort, 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. However, if the attacks are well understood and easily made, and if the vulnerable system is employed by a wide range of users, then it is likely that there will be enough benefit for someone to make an attack.

$ W3
See: World Wide Web.

$ war dialer
(I) 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 into the systems.

$ Wassenaar Arrangement
(N) 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.)

(C) The Arrangement began operations in September 1996. The participating countries are 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. Participants meet on a regular basis in Vienna, where the Arrangement has its headquarters.

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.

$ web of trust
(O) PGP usage: A trust-file PKI technique used in PGP for building a file of validated public keys by making personal judgments about being able to trust certain people to be holding properly certified keys of other people. (See: certification hierarchy, mesh PKI.)

$ web server
(I) A software process that runs on a host computer connected to the Internet to respond to HTTP requests for documents from client web browsers.

$ web vs. Web
1. (I) Capitalized: ISDs 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 vs. Internet.)

2. (C) Not capitalized: ISDs 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.

(C) IETF documents SHOULD spell out "World Wide Web" fully at the first instance of usage and SHOULD Use "Web" and "web" especially carefully where confusion with the PGP "web of trust" is possible.

$ wiretapping
(I) An attack that intercepts and accesses data and other information contained in a flow in a communication system.

(C) 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 reading information from any sort of medium used for a link or even directly from a node, such as gateway or subnetwork switch.

(C) "Active wiretapping" attempts to alter the data or otherwise affect the flow; "passive wiretapping" only attempts to observe the flow and gain knowledge of information it contains. (See: active attack, end-to-end encryption, passive attack.)

$ work factor
(I) General security usage: 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.

(I) Cryptography usage: The estimated amount of computing time and power needed to break a cryptographic system.

$ World Wide Web ("the Web", WWW, W3)
(N) 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. (See: web vs. Web, [R2084].)

$ worm
(I) A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. (See: Morris Worm, virus.)

$ wrap
(O) To use cryptography to provide data confidentiality service for a data object. (See: encrypt, seal.)

(D) ISDs SHOULD NOT use this term with this definition because it duplicates the meaning of other, standard terms. Instead, use "encrypt" or use a term that is specific with regard to the mechanism used.

$ WWW
See: World Wide Web.

$ X.400
(N) An ITU-T Recommendation [X400] that is one part of a joint ITU-T/ISO multi-part standard (X.400-X.421) that defines the Message Handling Systems. (The ISO equivalent is IS 10021, parts 1-7.) (See: Message Handling Systems.)

$ X.500
$ X.500 Directory
(N) An ITU-T Recommendation [X500] 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. (The ISO equivalent is IS 9594-1 and related standards, IS 9594-x.) (See: directory vs. Directory, X.509.)

(C) 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 "userCertificate" in the Directory entry that has the DN that is the subject of the certificate.

$ X.509

(N) An ITU-T Recommendation [X509] that defines a framework to provide and support data origin authentication and peer entity authentication services, 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.)

(C) X.509 describes two levels of authentication: simple authentication based on a password, and strong authentication based on a public-key certificate.

$ X.509 attribute certificate

(N) 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.)

(C) 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.

(C) An X.509 attribute certificate contains a sequence of data items and has a digital signature that is computed from that sequence. In addition to the signature, an attribute certificate contains items 1 through 9 listed below:

1. version	Identifies v1.
2. subject	Is one of the following:
2a. baseCertificateID	- Issuer and serial number of an X.509 public-key certificate.
2b. subjectName	- DN of the subject.
3. issuer	DN of the issuer (the CA who signed).
4. signature	OID of algorithm that signed the cert.
5. serialNumber	Certificate serial number; an integer assigned by the issuer.
6. attCertValidityPeriod	Validity period; a pair of UTCTime values: "not before" and "not after".
7. attributes	Sequence of attributes describing the subject.
8. issuerUniqueId	Optional, when a DN is not sufficient.
9. extensions	Optional.

$ X.509 authority revocation list
(N) An ARL in one of the formats defined by X.509--version 1 (v1) or version 2 (v2). A specialized kind of certificate revocation list.

$ X.509 certificate
(N) Either an X.509 public-key certificate or an X.509 attribute certificate.

(C) This Glossary uses the term with the precise meaning recommended here. However, some who use the term may not be aware that X.509 specifies attribute certificates that do not contain a public key. Even among those who are aware, this term is commonly used as an abbreviation to mean "X.509 public-key certificate". ISDs MAY use the term as an abbreviation for "X.509 public-key certificate", but only after using the full term at the first instance.

(D) ISDs SHOULD NOT use this term as an abbreviation to mean "X.509 attribute certificate".

$ X.509 certificate revocation list (CRL)
(N) 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.)

(C) ISDs SHOULD NOT refer to an X.509 CRL as a digital certificate, but note that an X.509 CRL does meet this Glossary's definition of "digital certificate". 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.

(C) An X.509 CRL contains a sequence of data items and has a digital signature computed on that sequence. In addition to the signature, both v1 and v2 contain items 2 through 6b listed below. Version 2 contains item 1 and may optionally contain 6c and 7.

1. version	Optional. If present, identifies v2.
2. signature	OID of the algorithm that signed CRL.
3. issuer	DN of the issuer (the CA who signed).
4. thisUpdate	A UTCTime value.
5. nextUpdate	A UTCTime value.
6. revokedCertificates	3-tuples of 6a, 6b, and (optional) 6c:
6a. userCertificate	A certificate's serial number.
6b. revocationDate	UTCTime value for the revocation date.
6c. crlEntryExtensions	Optional.
7. crlExtensions	Optional.

$ X.509 public-key certificate

(N) 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.)

(C) An X.509 public-key certificate contains a sequence of data items and has a digital signature computed on that sequence. In addition to the signature, all three versions contain items 1 through 7 listed below. Only v2 and v3 certificates may also contain items 8 and 9, and only v3 may contain item 10.

1. version	Identifies v1, v2, or v3.
2. serialNumber	Certificate serial number; an integer assigned by the issuer.
3. signature	OID of algorithm that was used to sign the certificate.
4. issuer	DN of the issuer (the CA who signed).
5. validity	Validity period; a pair of UTCTime values: "not before" and "not after".
6. subject	DN of entity who owns the public key.
7. subjectPublicKeyInfo	Public key value and algorithm OID.
8. issuerUniqueIdentifier	Defined for v2, v3; optional.
9. subjectUniqueIdentifier	Defined for v2, v2; optional.
10. extensions	Defined only for v3; optional.

$ XTACACS
See: (secondary definition under) Terminal Access Controller (TAC) Access Control System.

$ Yellow Book
(D) ISDs SHOULD NOT use this term as a synonym for "Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments" [CSC3]. Instead, use the full proper name of the document or, in subsequent references, a conventional abbreviation. (See: (usage note under) Green Book, Rainbow Series.)

$ zeroize
(I) Use erasure or other means to render stored data unusable and unrecoverable, particularly a key stored in a cryptographic module or other device.

(O) Erase electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FP140]

4. References

This Glossary focuses on the Internet Standards Process. Therefore, this set of references emphasizes international, governmental, and industry standards documents; only a few other texts are listed. RFCs are listed, but not Internet-Drafts, because the latter are not an archival document series and should not be cited or quoted in an RFC.

[A3092] American National Standards Institute, "American National Standard Data Encryption Algorithm", ANSI X3.92-1981, 30 Dec 1980.

[A9009] ---, "Financial Institution Message Authentication (Wholesale)", ANSI X9.9-1986, 15 Aug 1986.

[A9017] ---, "Financial Institution Key Management (Wholesale)", X9.17, 4 Apr 1985. [Defines procedures for the manual and automated management of keying material and uses DES to provide key management for a variety of operational environments.]

[A9042] ---, "Public key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithms", X9.42, 29 Jan 1999.

[A9052] ---, "Triple Data Encryption Algorithm Modes of Operation", X9.52-1998, ANSI approval 9 Nov 1998.

[A9062] ---, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", X9.62-1998, ANSI approval 7 Jan 1999.

[ABA] American Bar Association, "Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce", Chicago, IL, 1 Aug 1996.

[ACM] Association for Computing Machinery, "Communications of the ACM", Jul 1998 issue with: Minerva M. Yeung, "Digital Watermarking"; Nasir Memom and Ping Wah Wong, "Protecting Digital Media Content"; and Scott Craver, Boon-Lock Yeo, and Minerva Yeung, "Technical Trials and Legal Tribulations".

[Army] U.S. Army Corps of Engineers, "Electromagnetic Pulse (EMP) and Tempest Protection for Facilities", EP 1110-3-2, 31 Dec 1990.

[B7799] British Standards Institution, "Information Security Management, Part 1: Code of Practice for Information Security Management", BS 7799-1:1999, effective 15 May 1999.

---, ---, "Part 2: Specification for Information Security Management Systems", BS 7799-2:1999, effective 15 May 1999.

[Bell] D. E. Bell and L. J. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model", M74-244, The MITRE Corporation, Bedford, MA, May 1973. (Available as AD-771543, National Technical Information Service, Springfield, VA.)

[CCIB] Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model", ver. 2.1, CCIB-99-01, Aug 1999.

[CIPSO] Trusted Systems Interoperability Working Group, "Common IP Security Option", ver. 2.3, 9 Mar 1993. [A "work in progress" that is probably defunct.]

[CSC1] U.S. Department of Defense Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", CSC-STD-001-83, 15 Aug 1983. (Superseded by [DOD1].)

[CSC2] ---, "Department of Defense Password Management Guideline", CSC-STD-002-85, 12 Apr 1985.

[CSC3] ---, "Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments", CSC-STD-003-85, 25 Jun 1985.

[CSOR] U.S. Department of Commerce, "General Procedures for Registering Computer Security Objects", National Institute of Standards Interagency Report 5308, Dec 1993.

[Denn] D. E. Denning, "A Lattice Model of Secure Information Flow", in "Communications of the ACM", vol. 19, no. 5, May 1976, pp. 236-243.

[DH76] W. Diffie and M. H. Hellman, "New Directions in Cryptography" in "IEEE Transactions on Information Theory", vol. IT-22, no. 6, Nov 1976, pp. 644-654.

[DOD1] U.S. Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, 26 Dec 1985. (Supersedes [CSC1].)

[DOD2] ---, Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)", 21 Mar 1988.

[DOD3] ---, "X.509 Certificate Policy", ver. 2, Mar 1999.

[DOD4] ---, "NSA Key Recovery Assessment Criteria", 8 Jun 1998.

[ElGa] T. El Gamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" in "IEEE Transactions on Information Theory", vol. IT-31, no. 4, 1985, pp. 469-472.

[EMV1] Europay International S.A., MasterCard International Incorporated, and Visa International Service Association, "EMV ’96 Integrated Circuit Card Specification for Payment Systems", ver. 3.1.1, 31 May 1998.

[EMV2] ---, "EMV ’96 Integrated Circuit Card Terminal Specification for Payment Systems", ver. 3.1.1, 31 May 1998.

[EMV3] ---, EMV ’96 Integrated Circuit Card Application Specification for Payment Systems", ver. 3.1.1, 31 May 1998.

[For94] W. Ford, "Computer Communications Security: Principles, Standard Protocols and Techniques", ISBN 0-13-799453-2, 1994.

[For97] W. Ford and M. Baum, "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption", ISBN 0-13-476342-4, 1994.

[FP031] U.S. Department of Commerce, "Guidelines for Automatic Data Processing Physical Security and Risk Management", Federal Information Processing Standards Publication (FIPS PUB) 31, Jun 1974.

[FP039] ---, "Glossary for Computer Systems Security", FIPS PUB 39, 15 Feb 1976.

[FP046] ---, "Data Encryption Standard (DES)", FIPS PUB 46-2, 30 Dec 1993.

[FP081] ---, "DES Modes of Operation", FIPS PUB 81, 2 Dec 1980.

[FP102] ---, "Guideline for Computer Security Certification and Accreditation", FIPS PUB 102, 27 Sep 1983.

[FP113] ---, "Computer Data Authentication", FIPS PUB 113, 30 May 1985.

[FP140] ---, "Security Requirements for Cryptographic Modules", FIPS PUB 140-1, 11 Jan 1994.

[FP151] ---, "Portable Operating System Interface (POSIX)--System Application Program Interface [C Language]", FIPS PUB 151-2, 12 May 1993

[FP180] ---, "Secure Hash Standard", FIPS PUB 180-1, 17 Apr 1995.

[FP185] ---, "Escrowed Encryption Standard", FIPS PUB 185, 9 Feb 1994.

[FP186] ---, "Digital Signature Standard (DSS)", FIPS PUB 186, 19 May 1994.

[FP188] ---, "Standard Security Label for Information Transfer", FIPS PUB 188, 6 Sep 1994.

[FPDAM] Collaborative ITU and ISO/IEC meeting on the Directory, "Final Proposed Draft Amendment on Certificate Extensions", April 1999. (This draft proposes changes to [X.509].)

[FPKI] U.S. Department of Commerce, "Public Key Infrastructure (PKI) Technical Specifications: Part A--Technical Concept of Operations", National Institute of Standards, 4 Sep 1998.

[I3166] International Standards Organization, "Codes for the Representation of Names of countries and Their Subdivisions --Part 1: Country Codes", ISO 3166-1:1997.

---, --- "Part 2: Country Subdivision Codes", ISO/DIS 3166-2.

---, --- "Part 3: Codes for Formerly Used Names of Countries", ISO/DIS 3166-3.

[I7498] ---, "Information Processing Systems--Open Systems Interconnection Reference Model--[Part 1:] Basic Reference Model", ISO/IEC 7498-1. (Equivalent to ITU-T Recommendation X.200.)

---, --- "Part 2: Security Architecture", ISO/IEC 7499-2.

---, --- "Part 4: Management Framework", ISO/IEC 7498-4.

[I7812] ---, "Identification cards--Identification of Issuers--Part 1: Numbering System", ISO/IEC 7812-1:1993

---, --- "Part 2: Application and Registration Procedures", ISO/IEC 7812-2:1993.

[I9945] ---, "Portable Operating System Interface for Computer Environments", ISO/IEC 9945-1:1990.

[I15408] ---, "Information Technology--Security Techniques--Evaluation criteria for IT Security--Part 1: Introduction and General Model", ISO/IEC 15408-1:1999.

[ITSEC] "Information Technology Security Evaluation Criteria (ITSEC): Harmonised Criteria of France, Germany, the Netherlands, and the United Kingdom", ver. 1.2, U.K. Department of Trade and Industry, Jun 1991.

[Kahn] David Kahn, "The Codebreakers: The Story of Secret Writing", The Macmillan Company, New York, 1967.

[Knuth] D. E. Knuth, Chapter 3 ("Random Numbers") in Volume 2 ("Seminumerical Algorithms") of "The Art of Computer Programming", Addison-Wesley, Reading, MA, 1969.

[Kuhn] Markus G. Kuhn and Ross J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", in David Aucsmith, ed., "Information Hiding, Second International Workshop, IH'98", Portland, Oregon, USA, 15-17 Apr 1998, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 124-142.

[MISPC] U.S. Department of Commerce, "Minimum Interoperability Specification for PKI Components (MISPC), Version 1", National Institute of Standards Special Publication 800-15, Sep 1997.

[NCS01] National Computer Security Center, "A Guide to Understanding Audit in Trusted Systems", NCSC-TG-001, 1 Jun 1988. (Part of the Rainbow Series.)

[NCS04] ---, "Glossary of Computer Security Terms", NCSC-TG-004, ver. 1, 21 Oct 1988. (Part of the Rainbow Series.)

[NCS05] ---, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, ver. 1, 31 Jul 1987. (Part of the Rainbow Series.)

[NCS25] ---, "A Guide to Understanding Data Remanence in Automated Information Systems", NCSC-TG-025, ver. 2, Sep 1991. (Part of the Rainbow Series.)

[NIST] National Institute of Standards and Technology, "SKIPJACK and KEA Algorithm Specifications", ver. 2, 29 May 1998. (http://csrc.nist.gov/encryption/skipjack-kea.htm)

[PGP] Simson Garfinkel, "PGP: Pretty Good Privacy", O'Reilly & Associates, Inc., Sebastopol, CA, 1995.

[PKCS] Burton S. Kaliski, Jr., "An Overview of the PKCS Standards", RSA Data Security, Inc., 3 Jun 1991.

[PKC07] RSA Laboratories, "PKCS #7: Cryptographic Message Syntax Standard", ver. 1.5, RSA Laboratories Technical Note, 1 Nov 1993.

[PKC10] ---, "PKCS #10: Certification Request Syntax Standard", ver. 1.0, RSA Laboratories Technical Note, 1 Nov 1993.

[PKC11] ---, "PKCS #11: Cryptographic Token Interface Standard", ver. 1.0, 28 Apr 1995.

[R0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[R0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[R0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981. [See: RFC 1885.]

[R0793] Postel, J., ed., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[R0821] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, August 1982.

[R0822] Crocker, D., "Standard for the Format of ARPA Internet Text Messages", STD 11, RFC 822, August 1982.

[R0854] Postel, J. and J. Reynolds, "TELNET Protocol Specification", STD 8, RFC 854, May 1983.

[R0959] Postel, J. and J. Reynolds, "File Transfer Protocol (FTP)", STD 9, RFC 959, October 1985.

[R1034] Mockapetris, P., "Domain Names--Concepts and Facilities", STD 13, RFC 1034, November 1987.

[R1157] Case, J., Fedor, M., Schoffstall, M. and J. Davin, "A Simple Network Management Protocol (SNMP)" [version 1], STD 15, RFC 1157, May 1990.

[R1208] Jacobsen O. and D. Lynch, "A Glossary of Networking Terms", RFC 1208, March 1991.

[R1319] Kaliski, B., "The MD2 Message-Digest Algorithm", RFC 1319, April 1992.

[R1320] Rivest, R., "The MD4 Message-Digest Algorithm", RFC 1320, April 1992.

[R1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[R1334] Lloyd, B. and W. Simpson, "PPP Authentication Protocols", RFC 1334, October 1992.

[R1413] St. Johns, M., "Identification Protocol", RFC 1413, February 1993.

[R1421] Linn, J., "Privacy Enhancement for Internet Electronic Mail, Part I: Message Encryption and Authentication Procedures", RFC 1421, February 1993.

[R1422] Kent, S., "Privacy Enhancement for Internet Electronic Mail, Part II: Certificate-Based Key Management", RFC 1422, February 1993.

[R1455] Eastlake, D., "Physical Link Security Type of Service", RFC 1455, May 1993.

[R1457] Housley, R., "Security Label Framework for the Internet", RFC 1457, May 1993.

[R1492] Finseth, C., "An Access Control Protocol, Sometimes Called TACACS", RFC 1492, July 1993.

[R1507] Kaufman, C., "DASS: Distributed Authentication Security Service", RFC 1507, September 1993.

[R1510] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

[R1591] Kohl, J. and C. Neuman, "Domain Name System Structure and Delegation", March 1994.

[R1630] Berners-Lee, T., "Universal Resource Identifiers in WWW", RFC 1630, June 1994.

[R1661] Simpson, W., ed., " The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[R1731] Myers, J., "IMAP4 Authentication Mechanisms", RFC 1731, December 1994.

[R1734] Myers, J., "POP3 AUTHentication Command", RFC 1734, December 1994.

[R1738] Myers, J., Masinter, L. and M. McCahill, ed’s., "Uniform Resource Locators (URL)", RFC 1738, December 1994.

[R1750] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[R1777] Yeong, W., Howes, T. and S. Kille, "Lightweight Directory Access Protocol", RFC 1777, March 1995.

[R1808] Fielding, R., "Relative Uniform Resource Locators", RFC 1808, June 1995.

[R1824] Danisch, H., "The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange (E.I.S.S.-Report 1995/4)", RFC 1824, August 1995.

[R1828] Metzger, P. and W. Simpson, "IP Authentication using Keyed MD5", RFC 1828, August 1995.

[R1829] Karn, P., Metzger, P. and W. Simpson, "The ESP DES-CBC Transform", RFC 1829, August 1995.

[R1848] Crocker, S., Freed, N., Galvin, J. and S. Murphy, "MIME Object Security Services", RFC 1848, October 1995.

[R1851] Karn, P., Metzger, P. and W. Simpson, "The ESP Triple DES Transform", RFC 1851, September 1995.

[R1866] Berners-Lee, T., "Hypertext Markup Language--2.0", RFC 1866, November 1995.

[R1885] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 1885, December 1995.

[R1928] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and L. Jones, "SOCKS Protocol Version 5", RFC 1928, March 1996.

[R1938] Haller, N. and C. Metzion, "A One-Time Password System", RFC 1938, May 1996.

[R1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

[R1958] Carpenter, B., ed., "Architectural Principles of the Internet", RFC 1958, June 1996.

[R1983] Malkin, G., ed., "Internet Users' Glossary", FYI 18, RFC 1983, August 1996.

[R1994] Simpson, W. "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[R2023] Postel, J. and J. Reynolds, "Instructions to RFC Authors", RFC 2023, October 1997.

[R2026] Bradner, S., "The Internet Standards Process--Revision 3", BCP 9, RFC 2026, March 1994.

[R2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[R2060] Crispin, M., "Internet Message Access Protocol--Version 4 Revision 1", RFC 2060, December 1996.

[R2065] Eastlake, D., 3rd, "Domain Name System Security Extensions", RFC 2065, January 1997.

[R2078] Linn, J., "Generic Security Service Application Program Interface, Version 2", RFC 2078, January 1997.

[R2084] Bossert, G., Cooper, S. and W. Drummond, "Considerations for Web Transaction Security", RFC 2084, January 1997.

[R2104] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[R2119] Bradner, S., "Key Words for Use in RFCs To Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[R2138] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[R2137] Eastlake, D., "Secure Domain Name System Dynamic Update", RFC 2137, April 1997.

[R2179] Gwinn, A., "Network Security For Trade Shows", RFC 2179, July 1997.

[R2195] Klensin, J., Catoe, R. and P. Krumviede, "IMAP/POP AUTHorize Extension for Simple Challenge/Response", RFC 2195, Sepember 1997.

[R2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, Sepember 1997.

[R2202] Cheng, P. and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1", RFC 2202, Sepember 1997.

[R2222] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[R2223] Postel, J., "Instructions to RFC Authors", RFC 2223, October 1997.

[R2246] Dierks, T. and C. Allen, "The TLS Protocol, Version 1.0", RFC 2246, January 1999.

[R2284] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[R2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax, Version 1.5", RFC 2315, March 1998.

[R2323] Ramos, A., "IETF Identification and Security Guidelines", RFC 2323, 1 April 1998. [Intended for humorous entertainment ("please laugh loud and hard"); does not contain serious security information.]

[R2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", RFC 2350, June 1998.

[R2356] Montenegro, C. and V. Gupta, "Sun’s SKIP Firewall Traversal for Mobile IP", RFC 2356, June 1998.

[R2373] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 2998.

[R2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[R2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[R2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[R2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[R2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[R2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[R2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[R2408] Maughan, D., Schertler, M., Schneider, M. and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[R2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[R2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[R2412] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[R2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[R2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[R2504] Guttman, E., Leong, L. and G. Malkin, "Users' Security Handbook", RFC 2504, February 1999.

[R2510] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[R2527] Chokhani, S. and W. Ford, "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework", RFC 2527, March 1999.

[R2536] EastLake, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, March 1999.

[R2570] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction to Version 3 of the Internet-Standard Network Management Framework", RFC 2570, April 1999.

[R2574] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2574, April 1999.

[R2612] Adams, C. and J. Gilchrist, "The CAST-256 Encryption Algorithm", RFC 2612, June 1999.

[R2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol-- HTTP/1.1", RFC 2616, June 1999.

[R2628] Smyslov, V., "Simple Cryptographic Program Interface", RFC 2628, June 1999.

[R2630] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[R2631] Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999.

[R2633] Ramsdell, B., ed., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

[R2634] Hoffman, P., ed., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[R2635] Hambridge, S. and A. Lunde, "Don't Spew: A Set of Guidelines for Mass Unsolicited Mailings and Postings", RFC 2635, June 1999.

[Raym] E. S. Raymond, ed., "The On-Line Hacker Jargon File", ver. 4.0.0, 24 Jul 1996. (Also available as "The New Hacker's Dictionary", 2nd edition, MIT Press, Sep 1993, ISBN 0-262-18154-1. See: http://www.tuxedo.org/jargon/ for the latest version.)

[Russ] D. Russell and G. T. Gangemi Sr., Chapter 10 ("TEMPEST") in "Computer Security Basics", ISBN 0-937175-71-4, 1991.

[Schn] B. Schneier, "Applied Cryptography", John Wiley & Sons, Inc., New York, 1994.

[SDNS3] U.S. Department of Defense, National Security Agency, "Secure Data Network Systems, Security Protocol 3 (SP3)", document SDN.301, Revision 1.5, 15 May 1989.

[SDNS4] ---, ---, "Security Protocol 4 (SP4)", document SDN.401, Revision 1.2, 12 Jul 1988.

[SDNS7] ---, ---, "Secure data Network System, Message Security Protocol (MSP)", document SDN.701, Revision 4.0, 7 Jun 1996, with Corrections to Message Security Protocol, SDN.701, Rev 4.0", 96-06-07, 30 Aug, 1996.

[SET1] MasterCard and Visa, "SET Secure Electronic Transaction Specification, Book 1: Business Description", ver. 1.0, 31 May 1997.

[SET2] ---, "SET Secure Electronic Transaction Specification, Book 2: Programmer's Guide", ver. 1.0, 31 May 1997.

[Stei] J. Steiner, C. Neuman, and J. Schiller, "Kerberos: An Authentication Service for Open Network Systems" in "Usenix Conference Proceedings", Feb 1988.

[X400] International Telecommunications Union--Telecommunication Standardization Sector (formerly "CCITT"), Recommendation X.400, "Message Handling Services: Message Handling System and Service Overview".

[X500] ---, Recommendation X.500, "Information Technology--Open Systems Interconnection--The Directory: Overview of Concepts, Models, and Services". (Equivalent to ISO 9594-1.)

[X501] ---, Recommendation X.501, "Information Technology--Open Systems Interconnection--The Directory: Models".

[X509] ---, Recommendation X.509, "Information Technology--Open Systems Interconnection--The Directory: Authentication Framework". (Equivalent to ISO 9594-8.)

[X519] ---, Recommendation X.519, "Information Technology--Open Systems Interconnection--The Directory: Protocol Specifications".

[X520] ---, Recommendation X.520, "Information Technology--Open Systems Interconnection--The Directory: Selected Attribute Types".

[X680] ---, Recommendation X.680, "Information Technology--Abstract Syntax Notation One (ASN.1)--Specification of Basic Notation", 15 Nov 1994. (Equivalent to ISO/IEC 8824-1.)

[X690] ---, Recommendation X.690, "Information Technology--ASN.1 Encoding Rules--Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", 15 Nov 1994. (Equivalent to ISO/IEC 8825-1.)

5. Security Considerations

This document only defines security terms and recommends how to use them. It does not describe in detail the vulnerabilities of, threats to, or mechanisms that protect specific Internet protocols.

6. Acknowledgments

Pat Cain, Mike Kong, and Charles Lynn provided meticulous comments on an early draft.

7. Author's Address

Please address all comments to:

Robert W. Shirey
EMail: rshirey@bbn.com
Phone: +1 (703) 284-4641
Fax: +1 (703) 284-2766

GTE / BBN Technologies
Suite 1200, Mail Stop 30/12B2
1300 Seventeenth Street North
Arlington, VA 22209-3801 USA

8. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.