Section 2: Terminology and General Requirements

2.1 Conventions

2.1.1 Editorial Conventions

2.2 Definitions

2.2.1 Terminology

For the purposes of this guide, the following definitions apply:

2.2.1.1 implementation defined: An indication that the implementation shall define and document the requirements for correct program constructs and correct data of a value or behavior [ISO 9945-1 {B1}].

2.2.1.2 may: An indication of an optional feature [ISO 9945-1 {B1}].

With respect to implementations, the word *may* is to be interpreted as an optional feature that is not required in this guide, but can be provided. With respect to Strictly Conforming Applications, the word *may* means that the optional feature shall not be used.

2.2.1.3 shall: An indication of a requirement on the implementation or on Strictly Conforming Applications, where appropriate [ISO 9945-1 {B1}].

2.2.1.4 should:

(1) With respect to implementations, an indication of an implementation recommendation, but not a requirement [ISO 9945-1 {B1}].

(2) With respect to applications, an indication of a recommended programming practice for applications and a requirement for Strictly Conforming

Applications [ISO 9945-1 {B1}].

2.2.1.5 supported: A condition regarding optional functionality.

Certain functionality in this standard is optional, but the interfaces to that functionality are always required. If the functionality is *supported*, the interfaces work as specified by this standard (except that they do not return the error condition indicated for the unsupported case). If the functionality is not *supported*, the interface shall always return the indication specified for this situation [ISO 9945-1 {B1}].

2.2.1.6 system documentation: All documentation provided with an implementation, except the conformance document [ISO 9945-1 {B1}].

Electronically distributed documents for an implementation are considered part of the system documentation.

2.2.1.7 undefined: An indication that this guide imposes no portability requirements on an application's use of an indeterminate value or its behavior with erroneous program constructs or erroneous data [ISO 9945-1 {B1}].

Implementations (or other standards) may specify the result of using that value or causing that behavior. An application using such behaviors is using extensions, as defined in

2.2.1.8 unspecified: An indication that this standard imposes no portability requirements on applications for correct program constructs or correct data regarding a value or behavior [ISO 9945-1 {B1}].

Implementations (or other standards) may specify the result of using that value or causing that behavior. An application requiring a specific behavior, rather than tolerating any behavior when using that functionality, is using extensions, as defined in

2.2.2 General Terms

The definitions listed below are an inital list derived from various sources (as marked). These are intended to be a starting point. There is an exercise to make them internally consistent, and also consistent with their use within this document. Not all the definitions will be retained and some will require adding.

For the purposes of this Guide, the following definitions apply:

2.2.2.1 access control The prevention of unauthorised use of a resource including the prevention of use of a resource in an unauthorised manner.[ISO 7498-2:1989]

2.2.2.2 access control certificate ADI in the form of a security certificate[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.3 access control decision function (ADF) A specialised function that makes access control decisions by applying access control policy rules to a requested action, ACI (of initiators, targets, actions, or that retained from prior actions), and the context in which the request is made.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.4 access control decision information (ADI) The portion (possibly all) of the ACI made available to the ADF in making a particular access control decision.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.5 access control enforcement function (AEF) A specialized function that is part of the access path between an initiator and a target on each access that enforces the decisions made by the ADF.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.6 access control information (ACI) Any information used for access control purposes, including contextual information.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.7 access control list A list of entities, together with their access rights which are authorised to have access to a resource.[ISO 7498-2:1989]

2.2.2.8 access control policy The set of rules that define the conditions under which an access may take place.[IS0/IEC CD 10181-3 Oct 1991]

2.2.2.9 accountability The property that ensures that the actions of an entity may be traced to that entity.[ISO 7498-2:1989]

2.2.2.10 action The operations and operands that form part of an attempted access.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.11 action access control decision information (action ADI) Action decision information associated with the action.[ISO/IEC CD 10181-3 Oct 1991] For example authentication information sent by a client to a server, such as a DCE PAC.

2.2.2.12 active threat The threat of a deliberate unauthorised change to the state of the system.

NOTE: Examples of security-relevant active threats may be: modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorised entity and denial of service.[ISO 7498- 2:1989]

2.2.2.13 alarm collector function A function that collects the security alarm messages, translates them into security alarm records, and writes them to the security alarm log.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.14 alarm examiner function A function that interfaces with a security alarm administrator.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.15 application programming interface (API) The interface between the application software and the application platform, across which all services are provided.

The application programming interface is primarily in support of application portability, but system and application interoperability are also supported by a communication API.[POSIX.0/D15 Jun 1992]

2.2.2.16 assertion Explicit statement in a system security policy that security measures in one security domain constitute an adequate basis for security measures (or lack of them) in another.[CESG Memorandum No.1 Issue 1.2 Oct 1992]

2.2.2.17 association-security-state The collection of information that is relevant to the control of communications security for a particular application-association.[ISO/IEC DIS 10745 May 1992]

2.2.2.18 asymmetric authentication method Method for demonstrating knowledge of a secret, in which not all authentication information is shared by both entities.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.19 audit See Security Audit[ISO 7498-2:1989]

2.2.2.20 audit authority The manager responsible for defining those aspects of a security policy applicable to maintaining a security audit.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.21 audit event detector function A function that detects the occurance of security-relevant events. This function is normally an inherent part of the functionality implementing the event.

2.2.2.22 audit recorder function A function that records the security-relevant messages in a security audit trail.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.23 audit trail See Security Audit Trail[ISO 7498-2:1989]

2.2.2.24 audit trail analyser function A function that checks a security audit trail in order to produce, if appropriate, security alarm messages.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.25 audit trail archiver function A function that archives a part of the security audit trail.[ISO/IEC CD 10181- 7 Aug 1992]

2.2.2.26 audit trail collector function A function that collects individual audit trail records into a security audit trail.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.27 audit trail examiner function A function that builds security reports out of one or more security audit trails.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.28 audit trail provider function A function that provides security audit trails according to some criteria.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.29 authenticated identity An identity of a principal that has been assured through authentication.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.30 authentication See data origin authentication, and peer entity authentication. [ISO 7498-2:1989]

2.2.2.31 authentication certificate Authentication information in the form of a security certificate which may be used to assure the identity of an entity guaranteed by an authentication authority.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.32 authentication exchange A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.33 authentication information (AI) Information used to establish the validity of a claimed identity.[ISO 7498- 2:1989]

2.2.2.34 authentication initiator The entity which starts an authentication exchange.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.35 authorisation The granting of rights, which includes the granting of access based on access rights.[ISO 7498-2:1989]

2.2.2.36 authorisation policy A set of rules, part of an access control policy, by which access by security subjects to security objects is granted or denied. An authorisation policy may be defined in terms of access control lists, capabilities or attributes assigned to security subjects, security objects or both.[ECMA TR/46 Jul

1988]

2.2.2.37 availability The property of being accessible and usable upon demand by an authorised entity.[ISO 7498-2:1989]

2.2.2.38 capability A token used as an identifier for a resource such that possession of the token confers access rights for the resource.[ISO 7498-2:1989]

2.2.2.39 ciphertext Data produced through the use of encipherment. The semantic content of the resulting data is not available.

NOTE: Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.[ISO 7498-2:1989]

2.2.2.40 claim authentication information (claim AI) Information used by a claimant to generate exchange AI needed to authenticate a principal.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.41 claimant An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.42 cleartext Intelligible data, the semantic content of which is available.[ISO 7498- 2:1989]

2.2.2.43 confidentiality The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.[ISO 7498-2:1989]

2.2.2.44 contextual information Information derived from the context in which an access is made (for example, time of day).[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.45 corporate security policy The set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organisation.[ITSEC Ver 1.2 1991]

2.2.2.46 countermeasure See Security Measure.[]

2.2.2.47 credentials Data that is transferred to establish the claimed identity of an entity.[ISO 7498-2:1989]

2.2.2.48 cryptanalysis The analysis of a cryptographic system and its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.[ISO 7498- 2:1989]

2.2.2.49 cryptographic checkvalue Information that is derived by performing a cryptographic transformation (see cryptography) on a data unit.

NOTE: The derivation of the checkvalue may be performed in one or more steps and is a result of a mathematical function of the key and data unit. It is usually used to check the integrity of a data unit.[ISO 7498-2:1989]

2.2.2.50 cryptography The discipline that embodies principles, means, and the methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.

NOTE: The choice of cryptography mechanism determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or methods is cryptanalysis.[ISO 7498-2:1989]

2.2.2.51 data integrity The property that data has not been altered or destroyed in an unauthorised manner.[ISO 7498-2:1989]

2.2.2.52 data origin authentication

2.2.2.53 decipherment The reversal of a corresponding reversible encipherment.[ISO 7498-2:1989]

2.2.2.54 decryption See decipherment.[ISO 7498-2:1989]

2.2.2.55 denial of service The prevention of authorised access to resources or the delaying of time-critical operations.[ISO 7498-2:1989]

2.2.2.56 digital fingerprint A characteristic of a data item, such as a cryptographic checkvalue or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that possesses the same characteristics.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.57 digital signature Data appended to, or a cryptographic transformation (see cryptography) 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 for example, by the recipient.[ISO 7498-2:1989]

2.2.2.58 discretionary access control Methods of restricting access to objects or other resources based primarily on the instructions of arbitrary unprivileged users.[FC Ver 1.0 Dec 1992]

2.2.2.59 distributed application A set of information processing resources distributed over one or more open systems which provides a well defined set of functionality to (human) users, to assist a given (office) task.[ECMA TR/46 Jul 1988]

2.2.2.60 encapsulated subsystem A collection of procedures and data objects that is protected in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the encapsulated subsystem and that those procedures may be called only at designated domain entry points. Encapsulated subsystem, protected subsystem, and protected mechanisms of the TCB are terms that may be used interchangeably.[FC Ver 1.0 Dec 1992]

2.2.2.61 encipherment The cryptographic transformation of data (see cryptography) to produce ciphertext.

NOTE: Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed. Such encipherment may be called a one-way-function or cryptochecksum.[ISO 7498-2:1989]

2.2.2.62 encryption See encipherment.[ISO 7498-2:1989]

2.2.2.63 end-to-end encipherment Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (See also link-by-link encipherment.)[ISO 7498-2:1989]

2.2.2.64 exchange authentication information (exchange AI) Information exchanged between a claimant and a verifier during the process of authenticating a principal.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.65 identity-based security policy A security policy based on the identities or attributes of users, a group of users, or entities acting on behalf of the users and the resources or targets being accessed.[ISO 7498-2:1989]

2.2.2.66 distinguishing identifier Data that unambiguously distinguishes an entity in the authentication process. Such an identifier shall be unambiguous at least within a security domain.[ISO/IEC DIS 10182-2]

2.2.2.67 initiator An entity (for example, human user or computer based entity) that attempts to access other entities.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.68 initiator access control decision information (initiator ADI) ADI associated with the initiator.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.69 initiator access control information (initiator ACI) Access control information relating to the initiator.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.70 integrity See Data Integrity.[ISO 7498-2:1989]

2.2.2.71 key A sequence of symbols that controls the operations of encipherment and decipherment.[ISO 7498-2:1989]

2.2.2.72 key management The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.[ISO 7498-2:1989]

2.2.2.73 masquerade The unauthorised pretence by an entity to be a different entity. [ISO 7498-2:1989]

2.2.2.74 non-discretionary access control Means of restricting access to objects based largely on administrative actions.[FC Ver 1.0 Dec 1992]

2.2.2.75 off-line authentication certificate A particular form of authentication information binding an entity to a cryptographic key, certified by a trusted authority, which may be used for authentication without directly interacting with the authority.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.76 on-line authentication certificate A particular form of authentication information,certified by a trusted authority, which may be used for authentication following direct interaction with the authority[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.77 organisational security policy Set of laws, rules, and practices that regulate how an organisation manages, protects, and distributes sensitive information.[FC Ver 1.0 Dec 1992]

2.2.2.78 password Confidential authentication information, usually composed of a string of characters.[ISO 7498-2:1989]

2.2.2.79 peer-entity authentication The corroboration that a peer entity in an association is the one claimed.[ISO 7498-2:1989]

2.2.2.80 physical security The measures used to provide physical protection of resources against deliberate and accidental threats.[ISO 7498-2:1989]

2.2.2.81 policy See: security policy.[ISO 7498-2:1989]

2.2.2.82 principal An entity whose identity can be authenticated.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.83 privacy 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.

NOTE: because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.[ISO 7498-2:1989]

2.2.2.84 private key A key used in an asymmetric algorithm. Possession of this key is restricted, usually to only one entity.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.85 public key The key, used in an asymmetric algorithm, that is publicly available.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.86 repudiation Denial by one of the entities involved in a communication of having participated in all or part of the communication.[ISO 7498-2:1989]

2.2.2.87 rule-based security policy A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.[ISO 7498-2:1989]

2.2.2.88 seal A cryptographic checkvalue that supports integrity but does not protect against forgery by the recipient (that is, it does not support non-repudiation). When a seal is associated with a data element, that data element is "sealed".

2.2.2.89 secret key In a symmetric cryptographic algorithm the key shared between two entities.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.90 secure interaction policy The common aspects of the security policies in effect at each of the communicating application-processes.[ISO/IEC DIS 10745 May 1992]

2.2.2.91 security architecture A high level description of the structure of a system, with security functions assigned to components within this structure.[CESG Memorandum No.1 Issue 1.2 Oct 1992]

2.2.2.92 security attribute A security attribute is a piece of security information which is associated with an entity in a distributed system.[ECMA-138 Dec 1989]

2.2.2.93 security audit An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security and to recommend any indicated changes in control, policy and procedures.[ISO 7498-2:1989]

2.2.2.94 security audit message A message generated following the occurrence of an auditable security-related event.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.95 security audit record A single record in a security audit trail corresponding to a single security- related event.[ISO/IEC CD 10181-7 aug 1992]

2.2.2.96 security audit trail Data collected and potentially used to facilitate a security audit.[ISO 7498- 2:1989]

2.2.2.97 security auditor An individual or a process allowed to have access to the security audit trail and to build audit reports.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.98 security certificate A set of security-relevant data from an issuing security authority that is protected by integrity and data origin authentication , and includes an indication of a time period of validity.

NOTE: All certificates are deemed to be security certificates (see the relevant definitions in 7498-2). The term "security certificate" is adopted in order to avoid terminology conflicts with [X.509 | ISO 9594- 8] (i.e. the directory authentication standard).[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.99 security domain A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy, administered by the security authority, for the specified activities.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.100 security event manager An individual or process allowed to specify and manage the events which may generate a security message and to establish the action(s) to be taken for each security message type.[ISO/IEC CD 10181-7 Aug 1992]

2.2.2.101 security label The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

NOTE: The marking may be explicit or implicit.[ISO 7498-2:1989]

2.2.2.102 security policy The set of criteria for the provision of security services (see also identity-based and rule-based security policy.)

NOTE: A complete security policy necessarily addresses many concerns that are outside the scope of

OSI.[ISO 7498-2:1989]

2.2.2.103 security service A service which may be invoked directly or indirectly by functions within a system that ensures adequate security of the system or of data transfers between components of the system or with other systems.

2.2.2.104 security state State information that is held in an open system and which is required for the provision of OSI security services.[ISO/IEC DIS 10745 May 1992]

2.2.2.105 security token A set of security-relevant data that is protected by integrity and data origin authentication from a source that is not considered a security authority.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.106 sensitivity The characteristic of a resource that implies its value or importance, and may include its vulnerability.[ISO 7498-2:1989]

2.2.2.107 separation The concept of keeping information of different security classes apart in a system.

NOTE: Separation may be implemented by temporal, physical, logical or cryptographic techniques.[CESG Memorandum No.1 Issue 1.2 Oct 1992]

2.2.2.108 signature See digital signature.[ISO 7498-2:1989]

2.2.2.109 strength of mechanism An aspect of the assessment of the effectiveness of a security mechanism, namely the ability of the security mechanism to withstand direct attack against deficiencies in its underlying algorithms, principles and properties.[ITSEC Ver 1.2 1991]

2.2.2.110 symmetric authentication method Method for demonstrating knowledge of a secret, in which both entities share common authentication information.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.111 system security function A capability of an open system to perform security-related processing.[ISO/IEC DIS 10745 May 1992]

2.2.2.112 target An entity to which access may be attempted.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.113 target access control decision information (target ADI) ADI associated with the target.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.114 target access control information (target ACI) Access control information relating to the target.[ISO/IEC CD 10181-3 Oct 1991]

2.2.2.115 threat A potential violation of security.[ISO 7498-2:1989]

An action or event that might prejudice security.[ITSEC Ver 1.2 1991]

2.2.2.116 traffic analysis The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency).[ISO 7498-2:1989]

2.2.2.117 traffic flow confidentiality A confidentiality service to protect against traffic analysis.[ISO 7498- 2:1989]

2.2.2.118 traffic padding The generation of spurious instances of communication, spurious data units and/or spurious data within data units.[ISO 7498-2:1989]

2.2.2.119 trap door A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g., special "random" key sequence at a terminal).[TCSEC Dec 1985]

2.2.2.120 trojan horse Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allow unauthorised collection, falsification or destruction of data. [NSTISSI 4009][FC Ver 1.0 Dec 1992]

2.2.2.121 trust A relationship between two elements, a set of activities and a security policy in which element X trusts element Y if and only if X has confidence that Y behaves in a well defined way (with respect to the activities) that does not violate the given security policy.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.122 trusted computing base (TCB) The totality of protection mechanisms within an IT system, including hardware, firmware, software and data, the combination of which is responsible for enforcing the security policy.

2.2.2.123 trusted functionality That which is perceived to be correct with respect to some criteria, for example, as established by a security policy.[ISO 7498-2:1989]

2.2.2.124 trusted path Mechanism by which a person using a terminal can communicate directly with the TCB. [NSTISSI 4009]

NOTE: Trusted path can only be activated by the person or the TCB and cannot be imitated by untrusted software.[FC Ver 1.0 Dec 1992]

2.2.2.125 trusted third party A security authority or its agent, trusted by other entities with respect to security-related activities.[ISO/IEC CD 10181-1:Dec 1992]

2.2.2.126 verification authentication information (verification AI) Information used by a verifier to verify an identity claimed through exchange AI.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.127 verifier An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.[ISO/IEC DIS 10181-2 Jul 1991]

2.2.2.128 virus Self replicating, malicious program segment that attaches itself to an application or other executable system component and leaves no external signs of its presence. [NSTISSI 4009][FC Ver 1.0 Dec 1992]

2.2.2.129 vulnerability Weakness in an information system or components (for example, system security procedures, hardware design, internal controls) that could be exploited to produce an information-related misfortune.[FC Ver 1.0 Dec 1992]