

© British Standards Institution. No part of this publication may be photocopied or otherwise reproduced without the prior permission in writing of BSI

Draft for Development

Open Systems Interconnection: security architecture (ISO 7498/PDAD 2)

Interconnexion de systèmes ouverts: Architecture de protection

Verbindung offener Systeme: Aufbau des Datensicherungssystems

Contents	BS page	BS Page
National foreword	2	
Committees responsible	Back cover	
Draft for Development		
0 Introduction	3	
1 Scope and field of application	4	
2 References	5	
3 Definitions	6	
4 Notation	11	
5 General description of security services and mechanisms	12	
5.1 Overview	12	
5.2 Specific security services	12	
5.3 Specific security mechanisms	14	
5.4 Pervasive security mechanisms	18	
5.5 Summary matrix of security services and mechanisms	20	
6 The relationship of services, mechanisms and layers	21	
6.1 Security layering principles	21	
6.2 Model of invocation, management and use of (N)-protected services	21	
7 Placement of security services and mechanisms	28	
7.1 Physical Layer	28	
7.2 Data Link Layer	29	
7.3 Network Layer	29	
7.4 Transport Layer	31	
7.5 Session Layer		32
7.6 Presentation Layer		32
7.7 Application Layer		33
7.8 Summary matrix of security services and layers		36
8 Security management		37
8.1 General		37
8.2 Authentication management		38
8.3 Access control management		38
8.4 Key management		38
8.5 Security audit trails and event handling		39
Annexes		
A Background information on security in OSI		41
B Justification for security service and mechanisms placement in section 7		54
C Choice of position of encipherment for applications		59
Figures		
1 Direct signature scheme		51
2 Arbitrated signature scheme		51
Tables		
<i>Untitled</i>		20
<i>Untitled</i>		36

This publication is not to be regarded as a British Standard. It is being issued in the Draft for Development series of publications and is of a provisional nature because the subject matter is in the process of ongoing development within the International Standards Committee (ISO/TC 97/SC21 Information Retrieval, Transfer and Management for Open Systems Interconnection).

It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

A review of this Draft for Development will be carried out

not later than two years after its publication. Notification of the start of the review period, with a request for the submission of comments from users of this Draft for Development will be made in an announcement in the appropriate issue of *BSI News*. Observations which it is felt should receive attention before the official call for comments will be welcomed.

According to the replies received, the responsible BSI Committee will judge whether the Draft for Development can be converted into a British Standard or what other action should be taken.

DD 148: 1986

National foreword

This Draft for Development has been prepared under the direction of the Office and Information Standards Committee. The primary objective of this Draft for Development is to give advance guidance to product and systems designers concerned with security architecture for Open Systems Interconnection (OSI).

The text of the Draft for Development is identical with the proposed Draft Addendum ISO 7498/PDAD 2 (reference ISO/TC 97/SC 21 N 931) issued January 1986 by the International Organization for Standardization (ISO).

For ease of reproduction the ISO text has been reproduced unchanged.

The UK has actively participated through BSI Technical Committee IST/21 in the development of the ISO Draft Addendum. The Technical Committee will review any agreed amendments or addenda to the ISO text and will, where appropriate, update the text of this Draft for Development by means of an amendment or revision. When the ISO draft reaches an appropriate level of agreement and stability, this Draft for Development may be converted to a British Standard.

This Draft for Development contains the text of one of the set of Draft Addenda to the Basic Reference Model for Open Systems Interconnection (BS 6568):

ISO 7498/DAD 1 Connectionless-mode transmission (DD 125)

ISO 7498/PDAD 2 Security architecture (DD 148)

ISO 7498/PDAD 3 Naming and addressing (DD 149)

A brochure giving details of existing and projected British Standards publications for Open Systems Interconnection (OSI), data communications, database and computer graphics may be obtained from the Sales Department, BSI, Linford Wood, Milton Keynes, MK14 6LE, at no charge. Press releases for new British Standard publications in these areas will be issued to the computing press, and details of all new publications will be recorded in full in *BSI News*.

Terminology and conventions. The text of the proposed Draft Addendum has been approved as suitable for publication as a Draft for Development without deviation. Some terminology and certain conventions are not identical with those used in Drafts for Development; attention is drawn especially to the following.

Wherever the word 'Addendum' appears, referring to this Draft for Development, it should be read as 'Draft for Development'.

Cross-reference

International standard Corresponding British Standard

ISO 7498-1984	BS 6568 : 1984 Description of basic reference model for open systems interconnection (Identical)
ISO 7498/DAD 1	DD 125 : 1986 * Basic reference model for Open Systems Interconnection: connectionless mode transmission (ISO 7498 DAD 1 rev) (Identical)
ISO/DP 8648	DD 135 : 1985 Open Systems Interconnection: internal organization of the network layer (ISO/DP 8648.2) (Identical)
ISO/DIS 8822 †	DD 101 : 1986 * Open Systems Interconnection: connection-orientated presentation service definition (ISO/DIS 8822) (Identical)

At the time of publication of this Draft for Development, SC16 N 1953, to which reference is made in the text, has not yet reached Draft Proposal stage nor has it been issued as a Draft for Development.

* In preparation.

† Referred to as ISO/DP in the text.

0 Introduction

IS 7498 describes the Basic Reference Model for Open Systems Interconnection. That International Standard establishes a framework for coordinating the development of existing and future standards for the interconnection of systems.

The objective of OSI is to permit the interconnection of heterogeneous computer systems so that useful communication between application processes may be achieved. At various times, security controls must be established in order to protect the information exchanged between the application processes. Such controls should make the cost of obtaining or modifying data greater than the potential value of obtaining or modifying the data.

This addendum defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required. The addendum establishes, within the framework of the Reference Model, guidelines and constraints to improve existing standards or to develop new standards in the context of OSI in order to allow secure communications.

Note - This addendum extends the Basic Reference Model to cover security aspects which are general architectural elements of communications protocols, but which are not discussed in the Basic Reference Model (see Note 2 of section 5.1 of IS 7498).

[ISO page 1]

Documents

This publication is a Draft for Development and is therefore not to be regarded as a British Standard. See page 1

1 Scope and Field of Application

This Addendum to IS 7498, the Basic Reference Model for Open Systems Interconnection:

- a) provides a general description of security services and of related mechanisms, which may be provided by layers of the Reference Model; and
- b) defines the positions within the Reference Model where the services and mechanisms may be provided.

The Addendum adds to the concepts and principles defined in the International Standard; it does not modify them. The Addendum does not specify services and protocols for OSI. It is not an implementation specification, nor is it a basis for appraising the conformance of actual implementations.

This addendum extends the field of application of IS 7498, to cover secure communications between open systems.

OSI security functions are concerned only with those visible aspects of a communications path which permit end systems to achieve the secure transfer of information between them. OSI Security is not concerned with security measures needed in end systems, installations and organizations except where these have implications on the choice and position of security services visible in OSI. These latter aspects of security may be standardized but not within the scope of OSI standards.

[ISO page 2]

This publication is a Draft for Development and is therefore not to be regarded as a British Standard. See page 1.

2 References

- 2.1 IS 7498 Information Processing Systems - Open Systems Interconnection -Basic Reference Model
- 2.2 SC16 N1953 OSI Management Framework
- 2.3 IS 7498/DAD1 Addendum to 7498 Covering Connectionless-Mode Transmission.
- 2.4 DP 8648 Internal Organization of the Network Layer.
- 2.5 DP 8822 Connection-Oriented Presentation Service Definition.

[ISO page 3]

This publication is a Draft for Development and is therefore not to be regarded as a British Standard. See page 1.

Documents
Document Sharing Hub

3 Definitions

3.1 This Addendum builds on concepts developed in IS 7498 and makes use of the following terms defined in that standard:

- a) (N)-connection;
- b) (N)-data-transmission;
- c) (N)-entity;
- d) (N)-layer;
- e) open system;
- f) peer entities;
- g) (N)-protocol;
- h) (N)-protocol-data-unit;
- k) (N)-relay;
- m) routing;
- n) sequencing;
- p) (N)-service;
- q) (N)-service-data-unit;
- r) (N)-user-data;
- s) subnetwork;
- t) OSI resource; and
- u) transfer syntax.

3.2 This addendum uses the following terms drawn from the respective ISO documents:

Connectionless Mode Transmission	(IS 7498/DAD1)
End system	(DP 8648)
Internetwork	(DP 8648)
Subnetwork access	(DP 8648)
Relay and routing	(DP 8648)
UNITDATA	(IS 7498/DAD1)
Presentation context	(DP 8822)

3.3 For the purpose of this Addendum, the following definitions also apply:

3.3.1 **access control list:** A list of entities, together with their access rights, which are authorized to have access to a resource.

3.3.2 **accountability:** The property that ensures that an entity may be held responsible for its actions so that its violations or attempted violations of system security may be traced uniquely to it.

3.3.3 **active threat:** The threat of an unauthorized 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 authorized entity and denial of service.

3.3.4 **asset:** Anything which has value.

Note - Assets may include functions, devices, software, data, resources, and systems.

3.3.5 **audit:** See Security Audit.

3.3.6 **audit trail:** See Security Audit Trail.

3.3.7 **authentication:** See Data Origin Authentication, and Peer Entity Authentication.

Note - In this addendum, the term "Authentication" is not used in connection with data integrity; the term "Data Integrity" is used instead.

3.3.8 **authentication exchange:** a mechanism intended to ensure the identity of an entity by means of information exchange.

3.3.9 **authorization:** The granting or possession of rights.

3.3.10 **availability:** The property which requires the resources of an open system to be accessible and useable upon demand by an authorized entity.

3.3.11 **capability:** A token used as an identifier for a resource such that possession of the token confers access rights for the resource.

3.3.12 **channel:** An information transfer path.

3.3.13 **ciphertext:** Unintelligible data produced through the use of encipherment.

Note - Ciphertext may, itself, be input to encipherment, producing superenciphered output.

3.3.14 **cleartext:** Intelligible data that can be read or acted upon without the application of any decipherment.

3.3.15 **confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.3.16 **credentials:** Data passed from one entity to another which are used to establish the sending entity's access rights.

3.3.17 **cryptanalysis:** The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.

3.3.18 **cryptographic checkfunction:** Information which is derived by performing a cryptographic process on the data unit.

[ISO page 5]

Note - The derivation of the checkfunction may be performed in one or more steps and is a result of a mathematical function of the key and a data unit. It is usually used to check the integrity of a data unit.

3.3.19 cryptography: 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.

Note - Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

3.3.20 data integrity: The property that data has not been altered or destroyed in an unauthorized manner.

3.3.21 data origin authentication: The corroboration that the source of data received is as claimed.

3.3.22 decipherment: The reversal of a reversible encipherment.

3.3.23 denial of service: The prevention of authorized access to system assets or the delaying of time-critical operations.

3.3.24 digital signature: Data appended to, or a 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.

3.3.25 discretionary security: Those aspects of security policy which involve the provision of security services as a result of a request by an entity requiring an instance of communication.

3.3.26 encipherment: The transformation by cryptographic techniques (see cryptography) to produce ciphertext.

Note - Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

3.3.27 end-to-end encipherment: Encipherment of information 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.)

3.3.28 forgery: The fabrication or modification of information by an individual, entity or process and the claim that such information was received in a communication from another individual, entity or process.

3.3.29 integrity: See Data Integrity.

3.3.30 key: A sequence of symbols that controls the operations of encipherment and decipherment.

[ISO page 6]

3.3.31 key management: The generation, storage, secure distribution and application of encipherment keys in accordance with a security policy.

3.3.32 link-by-link encipherment: The individual application of encipherment to data on each link of a communications system. (See also end-to-end encipherment.)

Note - The implication of link-by-link encipherment is that data will be in cleartext form in relay entities.

3.3.33 mandatory security: The aspect of security policy insisted upon by system administrators, which require the provision of security services for one or more instances of communication.

3.3.34 manipulation detection: A mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally).

3.3.35 masquerade: The pretence by an entity to be a different entity in order to gain unauthorized access to resources.

3.3.36 notarization: The registration of data with a trusted third party that provides for future recourse to the data and assures accuracy concerning its characteristics such as content, origin, time and delivery of the data.

3.3.37 passive threats: Threats of unauthorized disclosure of information without changing the state of the system.

3.3.38 password: Confidential information, often composed of a string of characters, which may be used in the authentication of a user or resource and which may be used to identify a permitted mode of access.

3.3.39 peer-entity authentication: The corroboration that a peer entity in an association is the one claimed.

3.3.40 physical security: The measures used to provide physical protection of resources against malicious and accidental threats.

3.3.41 policy: See Security Policy.

3.3.42 privacy: The right to insist on adequate security of, and to define authorized users of, information or systems.

Note - Because this term relates to "rights" and these depend on legislation, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

3.3.43 repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.3.44 security audit trail: Data collected and potentially used to facilitate a security audit.

[ISO page 7]

3.3.45 security label: A sensitivity indicator which is permanently associated with protected data, processes, and/or other OSI resources, and which may be used in enforcing a security policy.

3.3.46 security policy: The set of rules for the provision of security services (see also discretionary security and mandatory security).

Note - A complete security policy will necessarily address many concerns which are outside of the scope of OSI.

3.3.47 security service: Services provided by one or more layers of communicating open systems which enhance the security of the systems and the data transfers taking place.

3.3.48 selective field protection: The protection of specific fields within a message which is to be transmitted.

3.3.49 sensitivity: The characteristic of a resource which implies its value or importance, and its vulnerability to accidental or deliberate threats.

3.3.50 signature: See digital signature.

3.3.51 threat: A potential violation of the security of the system.

3.3.52 traffic analysis: The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency).

3.3.53 traffic flow security: A confidentiality service to protect against traffic analysis.

3.3.54 traffic padding: The generation of spurious instances of communication, spurious data units and/or spurious data within data units.

3.3.55 trusted functionality: That which is perceived to be correct with respect to some criteria, e.g. as established by a security policy. The functionality shall neither fall short of nor exceed the criteria.

4 Notation

The layer notation used is the same as that defined in ISO 7498.

The term 'service' where not otherwise qualified, is used to refer to 'security service'.

The following abbreviations are used: OSI for Open Systems Interconnection; and SDU for Service Data Unit.

[ISO page 9]

5 General description of security services and mechanisms

5.1 Overview

The security features discussed below include various services and mechanisms which may be included in the OSI architecture and in implementations of the services and protocols of the architecture.

5.2 Security services

The following are considered to be the security services which can optionally be provided within the framework of the OSI Reference Model. Security services are provided through the use of security mechanisms which are detailed later.

5.2.1 Peer entity authentication

This service is provided at the establishment of, or during the data transfer phase of, a connection in order to provide confidence in the identity(s) of the entities connected. In other words, the entity is not attempting a masquerade or a replay of a previous connection.

Note - If peer entity authentication is required and the underlying service is connectionless, then a connection orientated service must first be provided over the connectionless service.

5.2.2 Access control

This service provides protection against unauthorized use of the resources accessible via OSI. This protection service can be applied in common to a group of entities (often referred to as a closed user group) or on an individual entity basis.

5.2.3 Data confidentiality

This service provides for the protection of data from unauthorized disclosure as described below.

5.2.3.1 Connection confidentiality

This provides confidentiality of all (N)-user-data on an (N)-connection.

Note - Depending on use and layer, it may not be appropriate to protect all data, e.g. expedited data or data in a connection request.

5.2.3.2 Connectionless confidentiality

This provides confidentiality of all (N)-user-data in a single connectionless (N)-SDU.

5.2.3.3 Selective field confidentiality

This provides confidentiality of selected fields with the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU.

5.2.3.4 Traffic flow security

This provides protection of the information which might be derived from observation of traffic flows.

5.2.4 Data integrity

This service counters active threats and it may take one of the following forms.

5.2.4.1 Connection integrity with recovery

This provides integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion or replay of any SDU of an entire SDU sequence (with recovery attempted).

5.2.4.2 Connection integrity without recovery

As for 5.2.4.1 but with no recovery attempted.

5.2.4.3 Selective field connection integrity

This provides integrity of selected fields transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.

5.2.4.4 Connectionless integrity

This provides integrity of a single connectionless SDU and may take the form of determination of whether a received SDU has been modified.

5.2.4.5 Selective field connectionless integrity

This provides integrity of selected fields within a single connectionless SDU and takes the form of determination of whether the selected fields have been modified.

5.2.5 Data origin authentication

This service, when provided by the (N)-layer, provides corroboration to the (N+1)-layer that the source of the data is the claimed peer entity.

5.2.6 Non-repudiation

This service may take one or both of two forms.

5.2.6.1 Non-repudiation, origin

The recipient of data is provided with proof of the origin of data which will protect against any attempt by the sender to falsely deny sending the data or its contents.

5.2.6.2 Non-repudiation, delivery

The sender is provided with proof of delivery of data such that the recipient cannot later deny receiving the data or its contents.

5.3 Specific security mechanisms

The following mechanisms may be incorporated into the (N)-layer in order to provide some of the services described in section 5.2 to the (N+1)-layer.

5.3.1 Encipherment

5.3.1.1 Encipherment can provide confidentiality of either data or traffic flow information and can complement a number of other security mechanisms as described in the following sections.

5.3.1.2 There are two general classifications of enciphering algorithm:

- a) Symmetric (e.g. secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice-versa; and
- b) Asymmetric (e.g. public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or vice-versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key".

5.3.1.3 The existence of an encipherment mechanism implies the use of a key management mechanism. The security architecture will determine the extent of isolation of protection achievable by the use of encipherment. The key management system will determine the extent of isolation actually achieved in practice in any given distributed system.

5.3.1.4 Some guidelines on key management methodologies are given in 8.4.

5.3.2 Digital signature mechanisms

These mechanisms define two procedures:

- a) signing a data unit; and
- b) verifying a signed data unit.

The first process uses information which is private (i.e., unique and confidential) to the signer. The second process uses procedures and information which are publicly available but from which the signer's private information cannot be deduced.

5.3.2.1 The signing process involves either an encipherment of the data unit or the production of a cryptographic checkfunction of the data unit, using the signer's private information as a private key.

5.3.2.2 The verification process involves using the public procedures and information to determine whether the signature was produced with the signer's private information.

5.3.2.3 The essential characteristic of the signature mechanism is that the signature can only be produced using the signer's private information. Thus when the signature is verified, it can subsequently be proven to any third party (e.g. a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

5.3.3 Access control mechanisms

5.3.3.1 These mechanisms use the authenticated identity of an entity or trusted information about the entity, (such as membership of a known set of entities or the capabilities or credentials of the entity) in order to determine and enforce the access rights of the entity. When the entity attempts to use an unauthorized resource the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm and/or forming part of an audit trail.

5.3.3.2 Access control mechanisms may, for example, be based on use of the following:

- a) access control information bases, where the access rights of authorized peer entities to resources are maintained. This information may be maintained by authorization centres or by the entity being accessed, and may be in the form of an access control list, or matrix, or hierarchical or distributed structure. This presupposes that peer entity authentication has been assured.
- b) Passwords, possession and subsequent presentation of which is evidence of the accessing entity's authorization.
- c) Capabilities, possession and subsequent presentation of which is evidence of the right to access the entity or resource defined by the capability.

Note - A capability should be unforgeable and should be conveyed in a trusted manner.

- d) Security labels, which when associated with an entity may be used to grant or deny access usually according to a security policy.

5.3.3.3 Access control mechanisms may be applied at either end of a communications association and/or at any intermediate entity.

Access controls involved at the origin or any intermediate entity are used to determine whether the sender is authorized to communicate with the recipient and/or to use the required communications resources.

The requirements of the access control mechanisms at the destination end of a connectionless data transmission must be known at the origin, and must be recorded in the Security Management Information Base (see 6.2 and 8.1).

5.3.4 Data integrity mechanisms

5.3.4.1 There are two aspects of data integrity: the integrity of a single data unit or field; and the integrity of a stream of data units or fields. In general, different mechanisms are used to provide the two types of integrity, although provision of the second without the first is not practical.

5.3.4.2 Determining the integrity of a single data unit involves two processes, one at the sending entity and one at the receiving entity. The sending entity appends to a data unit a quantity which is a function of the data itself. This quantity may be a block check code, other form of redundant information, or a cryptographic checkfunction and may itself be enciphered. The receiving entity generates a corresponding quantity and compares it with the received quantity to determine whether the data has been modified in transit. In appropriate layers of the architecture, detection of manipulation may lead to recovery action at that or a higher layer.

5.3.4.3 Protecting the integrity of a sequence of data units (i.e., protecting against misordering, losing, replaying and inserting or modifying data) requires additionally some form of sequence numbering and may also use time stamping.

5.3.5 Authentication exchange mechanism

5.3.5.1 Some of the techniques which may be applied to authentication exchanges are:

- a) Use of passwords - supplied by a sending entity and checked by the receiving entity;
- b) Cryptographic techniques; and
- c) Use of characteristics and/or possessions of the entity.

5.3.5.2 The mechanisms may be incorporated into the (N)-layer in order to provide peer entity authentication. If the mechanism does not succeed in authenticating the entity, this will result in rejection of the connection and possibly also cause an entry in the security audit trail and/or a report to a security management centre.

5.3.5.3 When cryptographic techniques are used, they may be combined with "hand-shaking" protocols to protect against replay (i.e., to ensure "liveness").

5.3.5.4 The choices of authentication exchange techniques will depend upon the circumstances in which they will be used. In many circumstances they will need to be used with:

- a) time stamping and synchronized clocks;
- b) two- and three-way handshakes (for unilateral and mutual authentication respectively); and
- c) non-repudiation services achieved by digital signature and/or notarization mechanisms.

5.3.6 Traffic padding mechanism

Traffic padding mechanisms can be used to provide various levels of protection against traffic analysis. This mechanism can be effective only if a confidentiality service is provided at the same layer or below.

5.3.7 Routing control mechanism

5.3.7.1 Routing control can be a security-relevant mechanism.

5.3.7.2 Routes can be chosen so as to use only physically secure networks or links.

5.3.7.3 End-systems may, on detection of persistent manipulation attacks, wish to instruct the network service provider to establish a connection via a different route.

5.3.7.4 Data carrying certain labels may be forbidden by the security policy to pass along certain routes. Also the initiator of a connection (or the sender of a connectionless data unit) may specify routing caveats requesting that specific sub-networks, links or relay entities be avoided.

5.3.8 Notarization mechanism

5.3.8.1 Properties about the data communicated between two or more entities, such as its integrity, origin, time and destination, can be assured by the provision of a notarization mechanism. The assurance is provided by a third party notary, which is trusted by the communicating entities, and which holds the necessary information to provide the required assurance in a testifiable manner. For the notarization

mechanism to be used, the notary requires a protected communications channel which can be trusted by each of the communicating entities. This channel may use digital signature, encipherment, and integrity mechanisms as appropriate to the service being provided by the notary. When such a notarization mechanism is invoked, the data is communicated between the communicating entities via the trusted channels and the notary.

5.4 Pervasive security mechanisms

This subsection describes a number of mechanisms. It is strongly recommended that they be present when any form of security is required and they may be essential when a high level of security is required. They are not specific to any particular service. Thus, in section 7, they are not explicitly described as being in any particular layer. Some of these pervasive security mechanisms can be regarded as aspects of security management (see also section 8).

5.4.1 Trusted functionality

5.4.1.1 Trusted functionality must be used to extend the scope of, or to establish the effectiveness of other security mechanisms. Any functionality which directly provides, or provides access to, security mechanisms, should be trustworthy.

5.4.1.2 The procedures used to ensure that trust may be placed in such hardware and software are outside the scope of this standard and in any case vary with the level of perceived threat and value of information to be protected.

5.4.1.3 Certification and verification procedures are, in general, costly and difficult to implement. The problems can be minimized by choosing an architecture which permits implementation of security functions in modules which can be made separate from, and protected from, non-security related functions.

5.4.2 Event detection and handling

5.4.2.1 The various security mechanisms may detect apparent violations of the security functions provided. The actions to be taken may include:

- a) recovery procedures;
- b) logging the event (in order to contribute to a security audit trail);
- c) local reporting of the event;
- d) remote reporting of the event (e.g. to a network control or security management centre); and
- e) unilateral disconnection.