2. Security Architecture(s) for Open Systems

Two related efforts have set the stage for the development of security standards in Open Systems. The first of these, ISO 7498-2, provides an architecture for security in Open Systems Interconnection, that is communications between open systems. The second, developed by the *European Computer Manufacturers Association (ECMA)*, addresses the somewhat broader scope of overall open systems. Both efforts are essentially architectural and neither have yet resulted in specific final protocol standards.

NSA and NIST, in cooperation with industry, have sponsored the development of the *Secure Data Network System (SDNS)*, a set of protocols which operate in the general framework of Open Systems Interconnection protocol standards. They augment the OSI protocols to provide needed security services, and are expected to provide the basis for specific OSI security protocol standards.

2.1 Open Systems Interconnection (OSI)

A security architecture for OSI and a set of protocols that implements a part of that architecture have been defined. They should serve as the basis for specific International Standard security protocols.

2.1.1 ISO 7498-2, Security Architecture

The one generally accepted standard in security for open systems is ISO 7498-2-1988 *Security Architecture*, Part 2 of ISO 7498, *Open Systems Interconnection - Basic Reference Model*. ISO 7498 provides a reference model for communications between open systems (the well known *OSI Reference Model*) and ISO 7498-2 covers communications security for OSI protocols, but not the more general problem of security in open systems (including processing and storage, etc. as well as communications).

The OSI Reference Model seven layer communications protocol stack is illustrated in figure 1 [OSI 7498]. In the model the protocols are defined on a peer protocol to peer protocol basis. The vertical interfaces between layers are logical service primitives, that are never observed directly; the only external observation possible is of peer entity to peer entity communications.

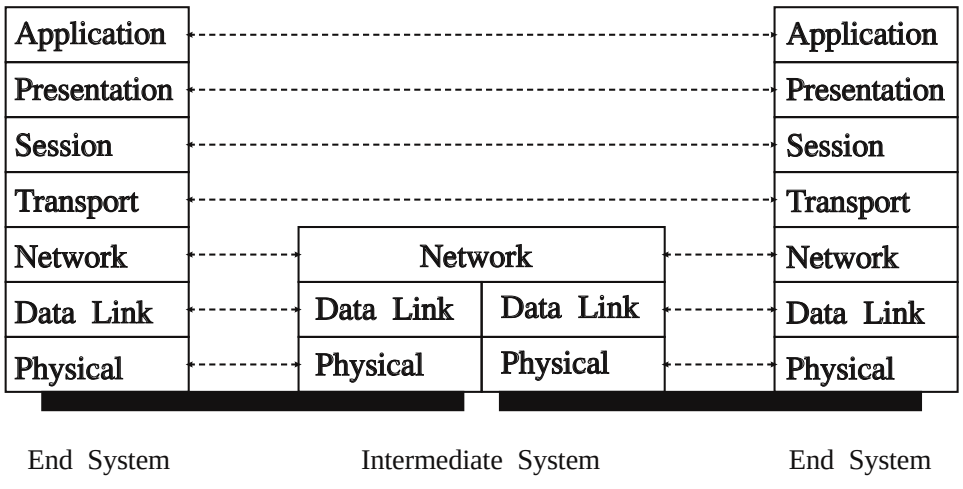


Figure 1 - Open Systems Interconnection Reference Model.

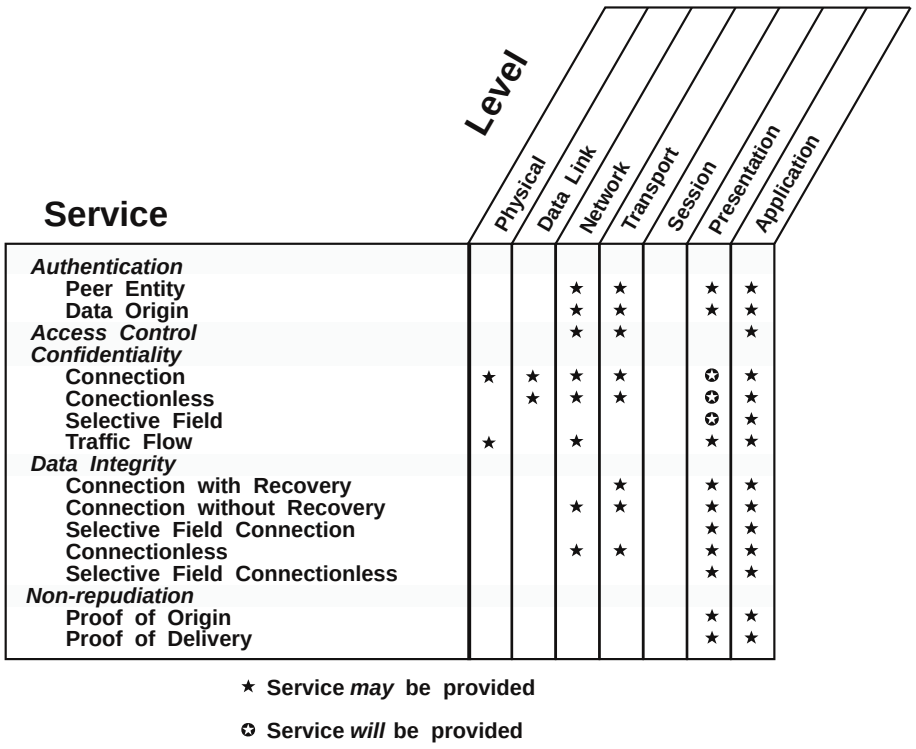
The *Protocol Data Unit (PDU)* of each layer or sub layer is encapsulated in the PDU of the lower layer. That is, when transmitting user data, each layer protocol entity applies a header and trailer to the data delivered by the layer above and may also subdivide the higher PDU into several of its own PDUs. When receiving, each layer strips its headers and trailers and reassembles any subdivided PDUs before passing them up. Layers may be divided into sublayers (this is most common at the lower three layers, which are conventionally divided into a total of as many as seven sublayers), and the sublayers act with peer sublayers similarly to layer protocols. According to 7498-2, the security services which may be provided at each layer are either peer entity to other peer entity at that layer, or refer to the protocol entity immediately above.

ISO 7498-2 defines five basic security services for secure open systems communication. They are:

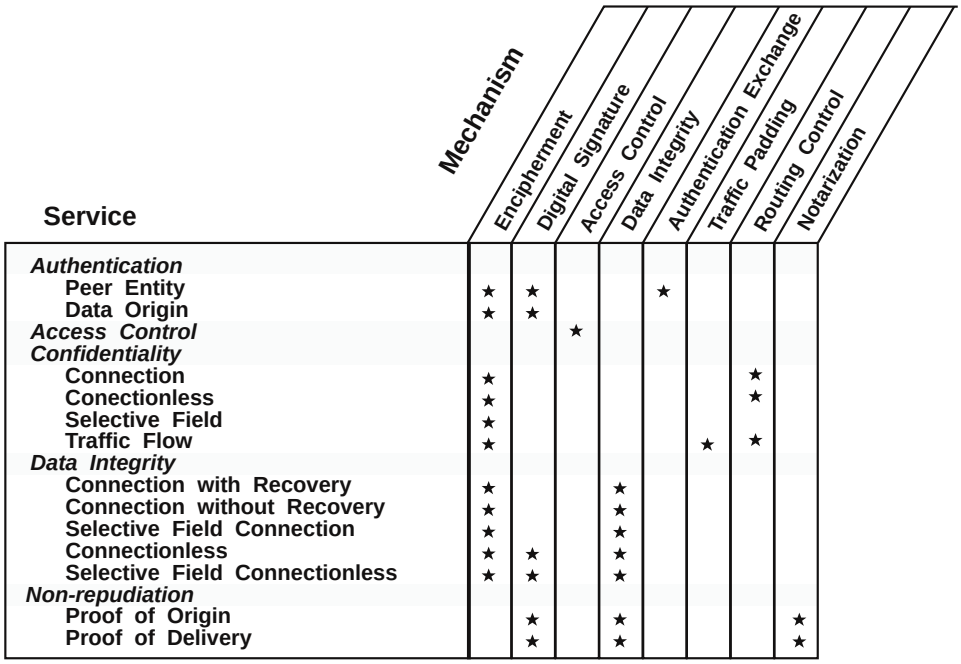
- *Authentication*. This service basically provides a reliable answer to the question, with whom am I communicating? Authentication services are provided by an (N)-layer entity to the (N+1)-layer entity above it. *Peer entity* authentication, when provided by an (N)-layer entity, corroborates that the remote (N+1)-layer is the claimed entity. *Data origin* authentication is provided by a (N)-layer entity to the (N+1)-layer entity above and corroborates that the source of the data is the claimed peer to the (N+1)-layer entity.
- *Access Control*. This service controls access to the resources which may be accessed via OSI communications as well as to the communications themselves. It relies upon the authentication service to reliably identify the entity seeking access.
- *Data Confidentiality*. This service protects data from unauthorized disclosure. All user data may be protected or fields may be selectively protected. *Traffic flow confidentiality* may also be provided, protecting the information which may be derived from a traffic analysis.
- *Data Integrity*. This service guarantees the integrity of data. It protects against the modification, insertion, deletion or replay of data. The integrity service may provide for recovery from integrity faults, or it may simply detect them. It may protect all data or only selected fields.
- *Non-repudiation.* This service prevents the parties to a communication from denying that they sent or received it, or disputing its contents. It may provide either *proof of origin* or *proof of delivery*.

To implement the services, ISO 7498-2 defines eight mechanisms. They are:

- *Encipherment*. This refers to cryptographic technology. Two classes of encipherment are defined, *symmetric* (*i. e.*, secret key), and *Asymmetric* (*i. e.*, public key).
- *Digital Signature*. A digital signature can only be produced using the private information of the signer. Therefore it can be proven that only the holder of that private information could have originated the signature. Asymmetric key encipherment is used to produce the signature.
- *Access Control*. Access control mechanisms control access of authenticated entities to resources. They may be based upon access control information bases, authentication information, capabilities, security labels, the time of attempted access, the rout of attempted access, and the duration of access.
- *Data Integrity* Data Integrity is broken into the integrity of a single PDU (*connectionless integrity*) and of the sequence of PDUs (*connection integrity*). The usual



(a) Security Services by OSI Level



(b) OSI Security Services & Mechanisms

Figure 2 - Security Services, OSI Levels and Mechanisms.

means of ensuring the integrity of a single PDU is a checkvalue which is a function of all the data in the PDU. The checkvalue may then be enciphered to prevent its alteration. The sequence of PDUs may be ensured by sequence numbering, time stamping or cryptographic chaining.

– *Authentication Exchange.* This is used to authenticate protocol entities. Passwords and cryptographic techniques, with suitable handshakes provide either unilateral or mutual authentication.

– *Traffic Padding*. Observation of traffic patterns, even when enciphered, may yield information to an intruder. This mechanism may be used to confound the analysis of traffic patterns.

– *Routing Control*. Routes can be chosen so as to use only secure links.

– *Notarization*. This mechanism is used to assure that communications cannot be repudiated.

ISO 7498-2 defines the appropriate protocol layers for each security service and the mechanisms which may be used to implement them. Figure 2(a) illustrates the assignment of services to layers while figure 2(3) shows the mechanisms used by each service.

2.1.2 Secure Data Network System (SDNS)

SDNS provides an architecture and several protocols which are overlayed on the OSI communications protocol stack. The SDNS protocols all work in a somewhat similar fashion by encapsulating *Protocol Data Units (PDUs)* in a "security envelope" as illustrated in figure 3. A protected header for the protocol is appended in front of the PDU. The protected header optionally contains security labels, sequence numbers, NSAP addresses, or CLNP headers, depending upon the specific protocol. An Integrity Check Value (ICV) is computed from the protected header and the PDU and added behind the PDU. The PDU, the protected header and the ICV are optionally encrypted. A clear header is then appended in front of the protected header. The primary function of the clear header is to identify the key used.

SDNS defines two somewhat similar protocols, one, *Security Protocol 4 (SP4)* [SDN.401], at the bottom of the Transport Layer and the other, *Security Protocol 3 (SP3)* [SDN.301], at the top of the Network Layer. Two variants of SP4 and four variants of SP3 are defined as summarized in table 1.

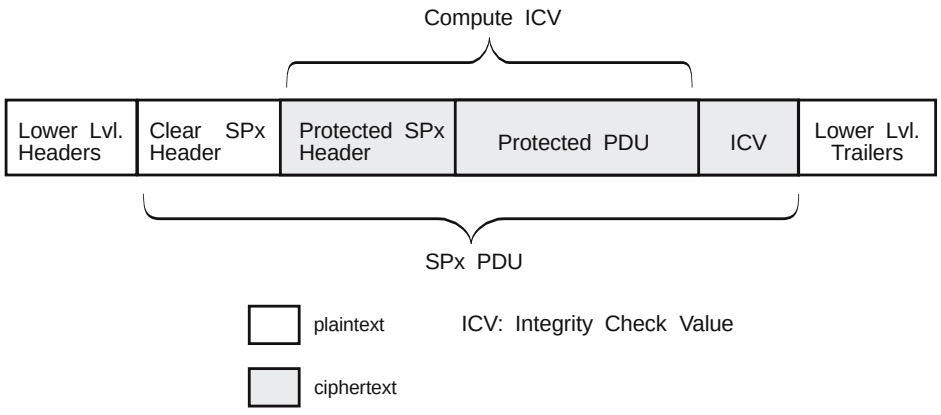


Figure 3 - SP3 and SP4 Security Encapsulation.

SP4 implements two modes, while SP3 implements four. Each mode logically fits into the OSI protocol stack in a somewhat different position. Figure 4 attempts to distinguish each of the modes by their location in the OSI protocol stack. By definition a layer 4 protocol operates from end system to end system. SP4C is a sublayer near the bottom of the transport layer. A separate security association with a separate key is formed for each transport connection, even when the transport connections are between the same transport entities., facilitating multilevel security.

SP4E and SP3N are between the transport and network layers. They are simple protocols and could be applied between almost any network and transport layer protocols, however they depend for connection integrity upon the services of the transport layer above them. When TP4 is used above SP3E, then the integrity of the TP4 protocol fields are protected, and, since TP4 provides connection error detection and recovery, the combination prevents most replay, deletion and insertion attacks. All connections between the same pair of end systems are protected by the same keys.

SP3A, SP3I and SP3D may operate from end system to end system, end system to intermediate system or intermediate system to intermediate system. SP3A is at the very top of the network layer. It includes source and destination NSAP addresses in the protected header. SP3I lies

Table 1 - SP3 and SP4 Protocols

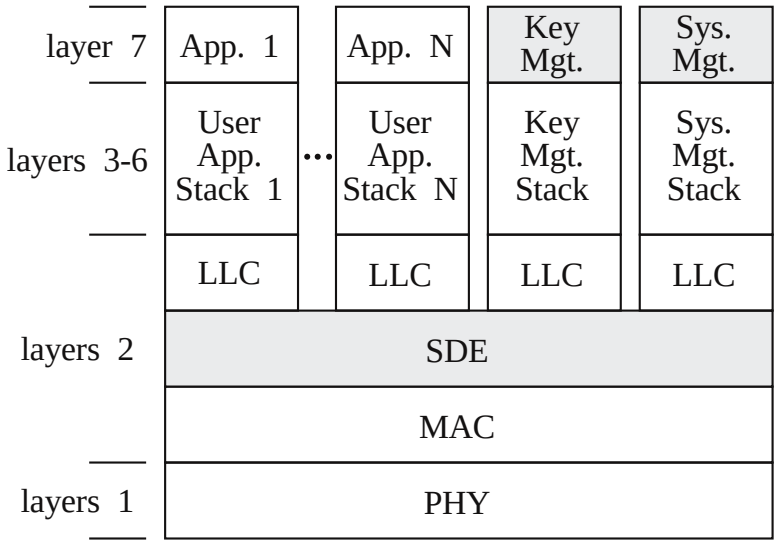
Protocol	Description
SP4C	Provides connection oriented security services with a key per transport connection. Is closely integrated with the ISO 8073 connection oriented Transport protocol. Includes full connection integrity and prevents modification, replay, insertion and deletions. Confidentiality and security labels are optional.
SP4E	Provides connectionless security services with a key per transport entity pair. Supports connectionless integrity and prevents modification of Transport Protocol Data Units. Security labels and confidentiality are optional. Provides a simple encapsulation of Transport PDUs; any protection against replay, insertion and deletion depends upon services of the Transport layer above.
SP3N	Used only in end systems and is identical to SP4E.
SP3A	Provides connectionless integrity, optional user data confidentiality, and optional security labels. Protects end system OSI *Network Service Access Point (NSAP)* addresses in the secure header. Encapsulates complete *Network Service Data Units (NSDUs)*. Used in end systems or intermediate systems.
SP3I	Services similar to SP3A but Protects *Connectionless Network Protocol (CLNP)* headers in the secure header. Encapsulates entire NSDUs or fragments.
SP3D	Similar to SP3I except that DoD IP formats and rules are used.

below the CLNP network sublayer, and includes the CLNP header in the protected header. SP3D is similar to SP3I except that it lies below the DoD IP protocol.

An Access Control Specification and a Key Management protocol are also under development for SDNS as application processes. The Key Management protocol can provide key management for cryptography in SP3 and SP4.

Either SP3 or SP4 may be applied to communications which use ISDN, however even SP3 is above the highest layer that is ordinarily considered an integral part of the ISDN, the *X.25* [ISO 8208, CCITT recommendation X.25] *Subnetwork Access Protocol (SNAcP)*. Every variant of SP3 is either intended for end systems, or explicitly associated with a specific *SubNetwork Independent Convergence Protocol (SNICP)* computer packet protocol (OSI NSAPs, CLNP or DoD TCP/IP). None provides a general X.25 solution which could be included in any X.25 ISDN intermediate system or packet handler and be used whatever the higher layer protocol.

In addition, application layer work is under way to add needed security features to the X.400/ISO 8505-1 Message Handling System (MHS) and the X.500/ISO DIS 9594 Directory Services standards. The SDNS extensions to MHS will provide for message confidentiality, integrity, data origin authentication access control and non-repudiation with proof of origin and signed receipt requests. In general the SDNS Directory extensions do not require new protocols (Directory Access Control may be the exception), rather they provide new Directory attributes to support security.



LLC: Logical Link Control
SDE: Secure Data Exchange Protocol
MAC: Medium Access Control (CSMA/CD, token ring, etc.)
PHY: PHYsical level

Figure 4 - SILS Protocols for LANs.

In the *Local Area Network (LAN)* arena, IEEE 802.10 is developing a *Standard for Interoperable Local Area Network (LAN) Security (SILS)*, [P802.10]. LANs are broadcast networks, with particular security concerns, including secure broadcast messages. SILS, which is illustrated in figure 4, will include three standards:

– *Secure Data Exchange (SDE)*, a Data Link layer protocol providing Confidentiality, Integrity, Data Origin Authentication and Access Control services. Note that ISO 7498-2 specifies only Confidentiality and Traffic Flow Confidentiality at layer 2.

– *Key Management Protocol*, a layer 7 function which supports SDE.

– *System/Security Management*, which is a layer 7 set of services used to manage the security protocols.

Figure 5 illustrates the combination of the various SDNS, application security and SILS protocols, and their relationship to ISDN. The SDNS protocols are expected to serve as the basis for international standards development to provide standards for security in OSI. Although working prototypes of SP3 and SP4 protocols exist, the international standards work is still at an early stage, and the protocols can be expected to evolve considerably before they are adopted as International Standards. It appears likely that SP4 or its ISO standard successor protocol will be widely used to ensure secure communications between open computer systems. When ISDN is

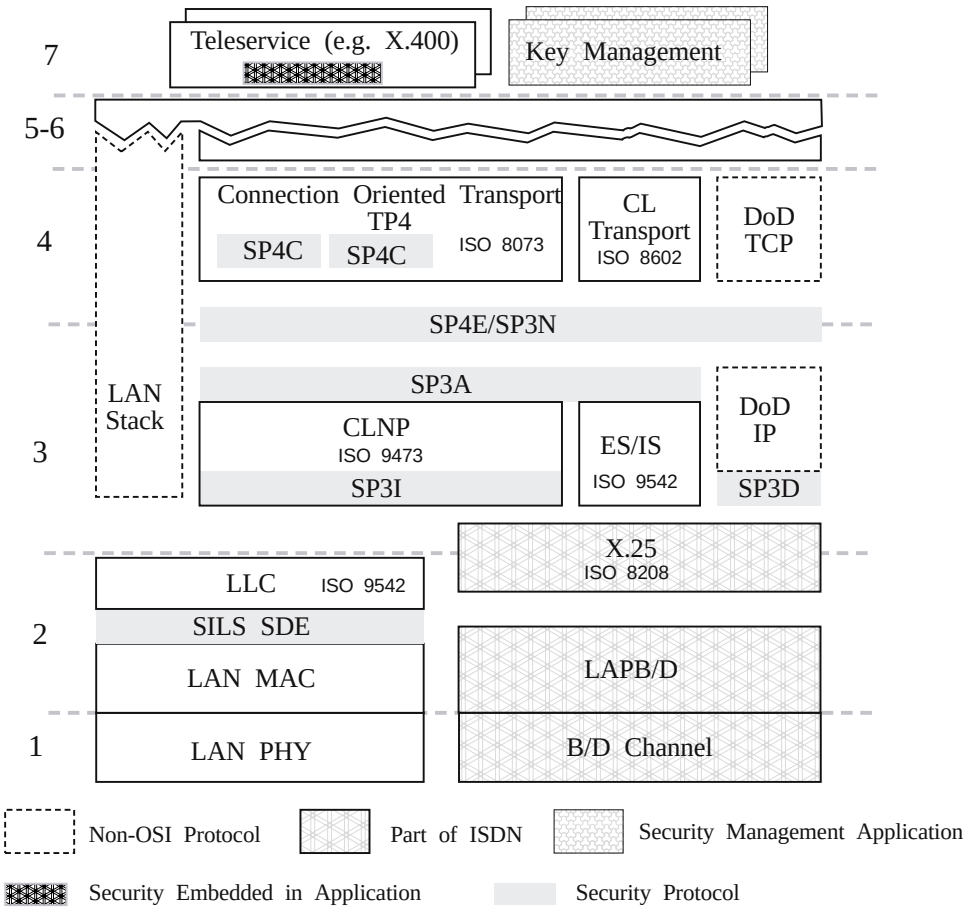


Figure 5 - SDNS and SILS Security Protocols.

used to provide a Data Link or Network Layer services for OSI communications, then SP4 or the equivalent standard protocol can ensure end to end confidentiality and integrity.

2.2 ECMA Security Architecture

Two documents produced by ECMA, ECMA TR/46, *Security in Open Systems a Security Framework*, and ECMA 138 *Security in Open Systems Data Elements and Service Definitions*, describe an approach to security in the context of complete open systems, rather than just communications. However, the ECMA model deals primarily with only two of the five security services defined in ISO 7498-2: Authentication and Access Control.

ECMA adapts an object orientated client-server model of security interactions. Figure 6 illustrates the ECMA object model and its relation to security services. In this model a human user interacts with an initiator (client) object which operates on a target (server) object. In the object orientated model, data is contained within the object and both applications and data are objects. The security services mediate between the human user and the objects in the system and they mediate between the objects themselves in accordance with the security policy of the system.

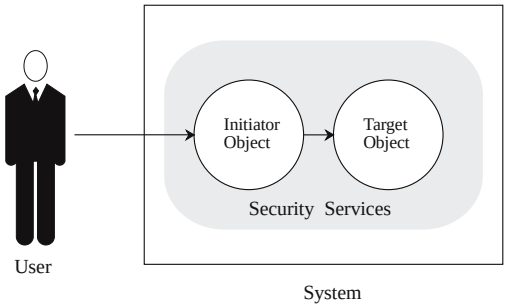


Figure 6 - Object Oriented Security Model.

Four classes of security services are defined by ECMA:

- Security Information Providing
- Security Control
- Security Monitor
- Other

Three Security Information Providing services are defined which provide trusted security information:

a. **Authentication Service.** Both human users and objects require authentication before they are allowed access to other objects, and objects may be authenticated before they are accessed.

b. **Security Attribute Service.** An attribute is an item of information associated with a user or an object. An attribute associated with a user or an initiator is a *Privilege Attribute*, while an attribute associated with a target object is a *Control Object*.

c. **Interdomain Service.** This service provides for mapping Security Attributes between domains, and for the sealing of identities and attributes by a Security Authority recognized in the target domain.

Three Security Control services are defined, which use attributes to control access to objects:

a. **Authorization Service.** The authorization service controls access to objects based upon the initiator and target Security Attributes.

b. **Secure Association Service.** In a distributed system this service has a component in each end-system, which associates a target and an initiator.

c. **Subject Sponsor Service.** The Subject Sponsor is the trusted facility that acts for any remote subject, particularly a human user, and arranges for the subjects authentication and access privileges to the objects it requires.

Two Security Monitor services are defined to maintain the integrity of the security system:

a. **Security Recovery Service.** The Security Recovery Service is an integral component of the other services. When the security of the system is threatened or violate, then recovery is required.

b. **Security Audit Information Collection Service.** This service collects audit information, the nature and analysis of which are dependent on the security policy.

Other Security Services may be required to support specific mechanisms and security policy requirements. They may include a Notary Service, a Key Management Service, a Data Flow Control Service and a Labelling Service, none of which are described in the ECMA standard.

The Security Services, in turn are supported by eight Security Facilities:

a. **Authentication Facility.**

b. **Attribute Management Facility.**

c. **Association Management Facility.**

d. **Inter Domain Facility.**

e. **Authorization Facility.**

f. **Audit Facility.**

g. **Recovery Facility.**

h. **Cryptographic Support**

In each case except for Recovery, the facility is implemented in the corresponding service. The Recovery Facility is contained in each of the services, and each service contains an authorization facility, which provides the access control for the management of the service. The Audit and Cryptographic Support facilities are optionally contained in all of the services.

The ECMA standards define the concept of a security domain, as a set of entities subject to a single security policy and a single security administration. They further recognize that security domains may be separate peers, or there may be a domain to sub-domain relationship. Each sub-domain is treated as a separate autonomous domain unless it is useful or necessary to con-

sider it as a sub-domain. The Interdomain Service provides for secure interworking between objects in different domains.

Distributed systems require that initiator privileges be transferred via communications protocols. The ECMA Data Elements and Service Definitions also defines a *Privilege Attribute Certificate (PAC)*. PACs state the privileges of an object and are bound together under the seal of the Authority which issues them. They must be protected against undetected modification, use by the wrong initiator, use against the wrong target, use outside stated constraints, or use by the right initiator for the wrong purpose.

ECMA 138 addresses security in distributed systems, in contrast to ISO 9478-2, which addresses only communications security. Unfortunately, the terminology of the two are not consistent. ISO defines five security services, and discusses them in terms of the mechanisms which may be used to implement the services and the layer of the ISO model where they may appropriately be implemented. ECMA defines eight rather different security services and eight security facilities they contain. However the focus of ECMA corresponds to the ISO Authentication and Access Control Services. In this document references to security services will follow the ISO model, unless otherwise stated. We will, however, adopt the concepts of security domains, the interdomain facility, and PACs from ECMA.