SECURITY IN OPEN DISTRIBUTED PROCESSING

Charles Siuda

Ascom Systems Ltd.
CH-3000 Bern, Switzerland

ABSTRACT

This paper describes two main aspects of security in open distributed processing: Embedment of security capabilities in reference to the OSI Reference Model and mapping of application layer components onto implementations in end-systems. The paper is based on a strategic commitment to the adoption of existing and evolving international standards. Therefore, the work is based on the security architecture (OSI 7498-2) and on the security concept described in ECMA TR/46 - Security in Open Systems - a Security Framework. This framework proposes a set of security facilities which are the building blocks for security services for use in the OSI application layer. One of the main targets of this paper is to show how security services can be embedded in the OSI communication environment. Two new types of common Application Service Element (ASE) are proposed to provide the security services in the application layer: the security information ASE and the security control ASE. The X.400 message handling system has been chosen as an example for securing a productive application.

I. INTRODUCTION

The convergence in media communications and information technologies requires coordination and cooperation between separate organizations as well as within a single organization. Electronic trading, for example, leads to distributed systems spanning traders, customers and banks. This level of integration is much harder, since no single authority can control the entire activity of the system. Integration through open distributed processing will lead to heterogeneous systems containing a wide variety of computer and networking technologies, supplied by a multiplicity of vendors.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 249-266, 1990.

Providing security for computers and communications is quite complex. Security must be incorporated not only into the Open Systems Interconnection (OSI) framework to ensure interoperability and compatibility of equipment and services but also into the Open Distributed Processing (ODP) to ensure secure information processing activities in which discrete components of the overall processing activities may be located in more than one system at more than one location.

Many different security needs can be met by a common set of security services to be provided outside application processes. These services will affect the interactions between users and productive applications, and between productive applications and supportive applications. They will also affect the installation, maintenance and management of applications and of the underlying system. These services, security information, their interactions and their management constitute the scope of security in open distributed processing.

II EMBEDMENT OF SECURITY CAPABILITIES IN REFERENCE TO THE OSI REFERENCE MODEL

2.1 Overview

The basic assumption of this work is that all security functions are located above OSI layer 6, i.e. within the application layer and/or outside the OSI environment. Three approaches have been identified to define the security services in the application layer. The first approach is to define the security services within the scope of specific application service elements. The second approach is to define the security services within other common application service elements, for example within ACSE and ROSE. The third approach defines common application service elements for security services that are accessed by specific application service elements like FTAM, X.400 etc. The third approach seems to have more merits. Therefore, it has been selected as the basic concept for embedment of security services in the application layer.

The message handling applications have been chosen as an example for securing productive applications.

The following supportive applications constitute the high level support environment for the productive applications and for the users of these applications:

- security information provision,
- security control,
- systems management,
- directory.

Only the productive applications are visible to the human user, and are especially used by him.

The following application service elements are required in every set of ASEs:

- Association Control Service Element (ACSE)
- Remote Operations Service Element (ROSE)

Figure 1 shows the application layer components.

2.2 Application Layer Components for Security Systems

The application layer components proposed for security systems are located within the Application Entity (AE). An AE is represented by a set of communication capabilities, called Application Service Elements (ASE). An ASE is typically defined by its own service definition and protocol specification. The Association Control Service Element (ACSE) supports the establishment and release of an application association between a pair of AEs. The Remote Operations Service Element (ROSE) supports the request/reply paradigm of the abstract operations that occur at the ports in the abstract model. The AE contains also two additional functions:

- The Single Association Control Function (SACF) models the coordination of the interactions among the ASEs contained in the Single Association Object (SAO) and also models the coordination of their use of the presentation layer. The rules concerning these interactions are defined by the application - context of the application - association.
- The cryptographic support function provides cryptographic services used primarily by security-related ASEs and by other productive ASEs which need cryptopgraphic functions for their operations. The cryptographic support function provides users with the following cryptographic functions:
  - data confidentiality functions,
  - data integrity functions,

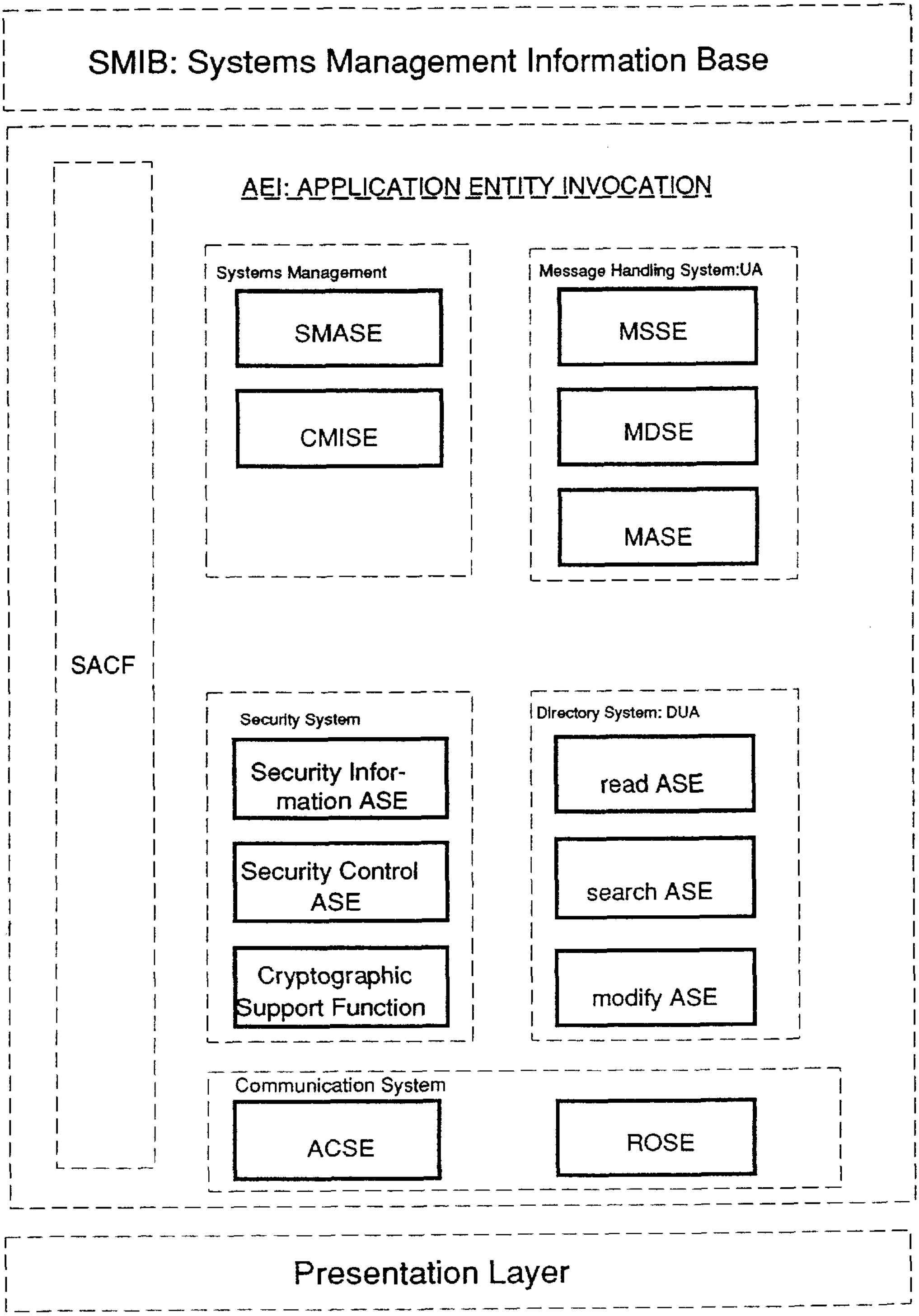

Figure 1- Application Layer Components

- data origin authentication,
- non-repudiation of origin,
- non-repudiation of receipt,
- authentication functions,
- key management functions.

The cryptographic support functions may also be used by systems management processes and directory access processes to support their cryptographic requirements.

2.2.1 Security-related ASEs

Security-related ASEs are a new type of more general ASEs in the application layer to provide the security services based on the ECMA security facilities described in ECMA TR46 and the application layer structure (ISO DP 9545).

There are two classes of security services that are directly and actively involved with implementing security policy:

- the security information providing class of service and
- the security control class of service.

The security information providing class of service provides security information, the security control class of service utilises security information. In accordance with these two classes of security service two security-related ASEs are proposed:

- the security information ASE, and
- the security control ASE

These ASEs may also be used by other productive ASEs.

a) Security Information ASE

The security information ASE provides two security services:

- the peer-entity authentication service and
- the security attribute service.

The peer-entity authentication service provides for the authentication of subjects e.g. human user's as well as active applications. Authentication requires the use of credentials to verify authentication information supplied by a subject. Depending on the trust relationships involved, different authentication mechanisms may be used. In general, authentication relies on an entity proving its identity by showing that it is in possession of some piece of secret information. Authentication is an end-to-end operation between the two entities concerned. The result of authentication is a mapping between a communicating entity (the subject) and a verified identity.

The security attribute service provides attributes for entities on presentation of the entity's authenticated identity. This service will also map attributes where required.

b) Security Control ASE

Security control has to do with information collection (e.g. reading a human user's credential), with information checking (as in access authorization) and with information transformation (as in exchanges between domains). Such information processing provides the basic operation of security control.

The security control ASE provides the following security control services:

- Subject sponsor service to support the interaction with human users.
- Secure association service to control the security aspects of associations between application processes.
- Authorization service to provide access control decisions.
- Interdomain service to provide the functionality for mapping policy elements between different domains.
- Cryptographic support service. This service is executed by the cryptographic support function.

2.2.2 System Management ASEs

2.2.2.1 Integration of Security Management into OSI Systems Management

OSI systems management is a set of activities that manage a communications environment conforming to open systems interconnection standards. Security management is used to monitor and control the operation of OSI security services and mechanisms in accordance with its security policy. Security management is the set of procedures used to manage the objects and attributes within the Systems Management Information Base (SMIB). These objects are similar to other objects which are managed by OSI management. What distinguishes security management from the other Specific Management Functional Areas (SMFAs) is the class of objects managed and not the operations used to manage them. For this reason, security management does not define its own directives for the use of Common Management Information Services (CMIS), but uses those already defined by other SMFAs. Thus, for example the directives used to configurate security objects and security attributes are exactly those which are defined by the configuration management SMFA. Therefore, security management is an integral part of OSI systems management.

2.2.2.2 Security Management Facilities

Security management provides the set of management facilities needed to operate on security objects so as to allow the implementation of the security policy. These facilities may be provided through the use of directives in other SMFAs which in turn use operations of CMIS. The facilities provided or used by security management are: security-related object management and security-related event and audit trail management.

a) The Security-related object management facility manages security-realted objects, attributes, states and relationships on a collection of open systems. It includes the facilities defined in configuration management (ISO-9595): object configuration, attribute management, state management and relationship management.

b) The security event and audit trail management facility is used to create and communicate security-related events, event logs and audit trails on a collection of open systems. The facilities required for this function are similar to those defined in fault management (ISO 9595): spontaneous event reporting, cumulative event gathering, event threshold alarm and management service control.

2.2.2.3 Communication Aspects of Security Management

Management processes perform the management activities in a distributed manner. The interactions which take place between management processes are abstracted in terms of directives issued by one processor to the other. The interactions between managing and agent processes are realized through the exchange of management information. This communication is accomplished using OSI protocols.

The Systems Management Application Service Element (SMASE) defines the semantics and abstract syntaxes of the information transferred as relevant to OSI management in Management Application Protocol Data Units (MAPDUs). The MAPDU is the OSI protocol realization of the abstract notation of directives exchanged between management application processes.

The communication service used by the SMASE may be provided by the Common Management Information Service Element (CMISE) or other ASEs such as Transaction Processing (TP). The use of CMISE also implies the presence of the Remote Operaton Service Element (ROSE) and other ASEs. CMISE specifies the service and procedures for transfer of Common Management Information Protocol Data Units (CMIPDUs). It provides a means for the exchange of information and commands for management purpose in a common manner.

2.2.3 Message Handling ASEs

Access to the Message Transfer System (MTS) abstract service is supported by three application service elements, each supporting a type of port between an MTS-user and the MTS in the abstract model.

The Message Submission Service Element (MSSE) supports the services of the submission-port; and the Message Delivery Service Element (MDSE) supports the services of the delivery-port; and the Message Administration Service Element (MASE) supports the services of the administration-port. Similarly, access to Message Store (MS) abstract service is supported by three application-service-elements: the MSSE supports the indirect-submission-port; the Message Retrieval Service Element (MRSE) supports the services of the retrieval-port; and the MASE supports the services of the administration-port.

These application service elements are in turn supported by other application service elements: The MSSE, MDSE, MRSE and MASE provide the mapping functions of the abstract-syntax notation of an abstract service onto the services provided by the ROSE.

2.2.4 Directory ASEs

The directory system stores information about objects in the real world which is provided, on request, to directory users to facilitate communication between objects. Users of the directory, including human user's and application processes, are represented by Directory User Agents (DUAs); these are application processes that enable users to read or modify information in the Directory Information Base (DIB). This information base consists of object entries which are distributed between several DSAs (Directory System Agents).

The DUA accesses the directory on behalf of the human user or of the application process. All directory services are requested and received by the DUA through access points, each of which corresponds to three different types of port. These ports define several directory operations which are used to read, modify, or search for entries in the directory information base.

The DUA connects to the directory via bind-operations (Remote Operations Service Element, ROSE) and requests directory services from the Directory System Agent (DSA) through the directory application service elements.

When a DUA is in a different open system from a DSA with which it is interacting, these interactions are supported by the Directory Access Protocol (DAP), which is an OSI application layer protocol. Similarly, when a pair of DSAs which are interacting are in different open systems, the interactions are supported by the Directory System Protocol (DSP).

Both the DAP and the DSP are protocols to provide communication between a pair of application processes.

The directory-specific ASEs (read ASE, search ASE, modify ASE) provide the mapping function of the abstract-syntax notation of the directory abstract-service onto the services provided by the ROSE.

The directory bind-operations are mapped onto the ACSE and the directory application service elements are mapped onto remote operation service elements, ROSE, as specified in the directory access protocols.

2.2.5 Mapping Security Facilities onto Security-related ASEs

Security in a distributed system requires the implementation of many different functions. These functions, which are modeled as security facilities, are described in ECMA TR/46 Security in Open Systems - a Security Framework. A short description of the security facilities is given in the table shown in Figure 2. These security facilities are used as building blocks of the proposed security-related ASEs. Figure 3 shows the mapping of the security facilities onto security-related ASEs.

Security Facility	Short Description
Subject Sponsor Facility	Intermediary between the security subject and the other security facilities.
Authentication Facility	Accepts and checks subject authentication information (subject credentials).
Association Management Facility	- Authorization for the two entities to communicate. - Assurance of the identity of both entities.
Security State Facility	Maintaines a view of the current security state of the system.
Security Attribute Management Facility	This facility manipulates the security attributes of subjects and objects.
Authorization Facility	Authorizes or denies requested accesses by subjects to objects.
Inter-domain Facility	Maps one domain's interpretation of security attributes into another domain's interpretation
Security Audit Facility	Receives and analyses event information from other security facilities.
Security Recovering Facility	Acts on information received from the audit facility.
Cryptographic Support Facility	Provides cryptographic services used by other security facilities and by productive services and applications to secure data in storage and transit.

Figure 2: Short description of ECMA security facilities

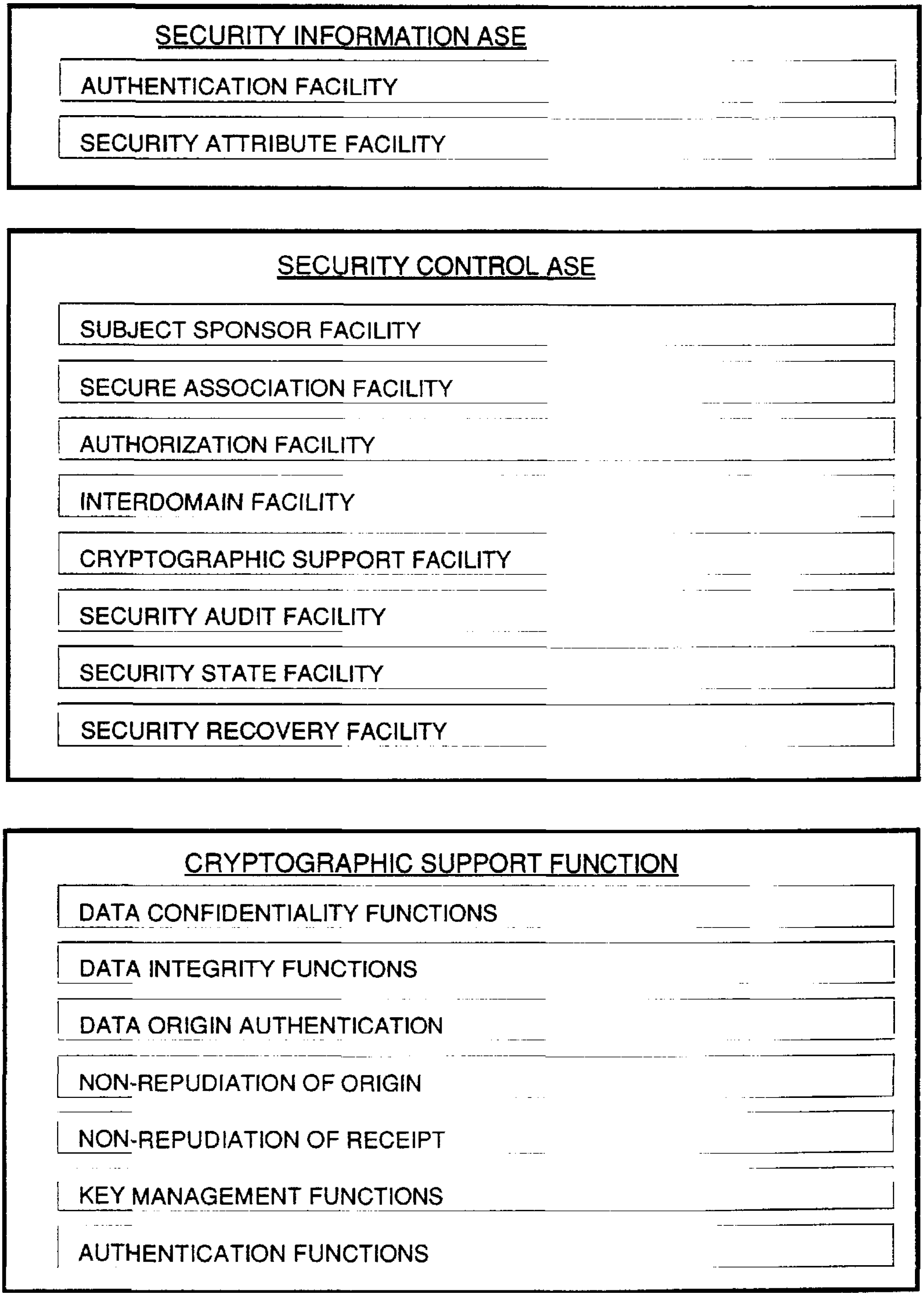

Figure 3- Mapping Security Facilities onto Security ASEs

III. MAPPING APPLICATION LAYER COMPONENTS ONTO IMPLEMENTATIONS IN END-SYSTEMS

3.1 Use of the Directory

The directory system stores information about objects in the real world (e.g. people, applications) which is provided, on request, to directory users to facilitate communication between objects. In general, the directory itself has no responsibility for the information placed in the directory. The directory is simply a repository for information. The directory assures the consistency of that information, making the appropriate updates in the distributed directory information base and the availability of that information.

3.1.1 The Directory Used as an Attribute Store

Each entry of the directory information base contains at least the following attributes:

- Common name which identifies the corresponding person, application process, application entity, etc.
- Public-key certificate which is used to authenticate two communicating parties.
- Security privilege attributes and security control attributes used in access control decision making.

3.1.2 The directory used as a Key Management System

Key management is achieved by using security features provided in the directory. The key management system is based on the use of public key cryptosystems. The X.509 authentication framework allows a user's public key to be stored in its directory entry. The directory provides a way to reliably link a name with a public key.

3.2 Client-Server Model of a Distributed Application

A distributed application consists of two parts. The part collocated with the user is referred to as the client entity, the remote part of the application as the server system. A client entity and a server system communicate over the network by means of an access protocol. In order to comply with the OSI Reference Model, the client and the server are considered application processes and are extended with Application Entities (AE). The AEs are parts of the application layer and contains sets of ASEs. The ASEs provide the communication functions, in accordance with the service definition, to the client and the server, and implement the access protocol. In doing so, an ASE may use services provided by other ASEs in the same AE, and by the presentation layer of the OSI Reference Model.

3.3 Mapping Application Layer Components onto Implementations in End-systems

Security service applications are real, possibly distributed applications, that can be named and registered for use in open systems. These applications consist of one or more elements that are distributed over a number of physical systems. These elements are referred to as logical servers. A single physical end-system may support one or more logical servers of different types. The application layer components to be mapped on implementations in end-systems are shown in Figure 1.

3.3.1 Mapping the Security Information ASE onto Supportive Servers

The security information ASE may be mapped directly onto supportive servers. Their function is to accept information, process it and return results; which is the classic action of a supportive server, which is called "security server". The data base of this server is embedded in the Directory System Agent (DSA).

3.3.2 Mapping the Security Control ASE onto End-system Components

The four kinds of services embedded in the security control ASE are: authorization services, interdomain services, secure association services and finally subject sponsor services. Secure association is a function that needs to be performed in each of the two end-systems involved in an association. A subject sponsor service maps to a local function in each end-system which is directly accessible to human users or external applications that need a subject sponsor as entry point into the secure distributed system. Authorization services and interdomain services may be mapped onto a local function in each end-system.

3.3.3 Mapping Directory ASEs onto End-system Components and Logical Servers

The directory user agent maps to a local function in each end-system which is directly accessible to human users. The directory system agent maps onto logical servers.

3.3.4 Mapping Message Handling System ASEs onto End-system Components and Servers

The User Agent (UA) maps to a local function in each end-system which is directly accessible to human users. The Message Transfer Agent (MTA) maps onto logical servers.

3.3.5 Mapping Communication ASEs onto End-system Components

The following communication ASEs are required in each set of ASEs:

- The Association Control Service Element (ACSE) supports the establishment and release of an application association between a pair of AEs.
- The ROSE supports the request/reply paradigm of the abstract operations.

Both ASEs are mapped to local functions in all user's end-systems and server end-systems.

3.4 User's End-system Components

The user's end-system components which are shown in Figure 4 can be grouped in five groups:

- security system,
- management system,
- message handling system,
- directory system,
- communication system.

The security system contains the security facilities which are the building blocks of the security system. The cryptographic support facility is implemented using hardware (the so-called crytographic processor). The subject sponsor facility is the intermediate between the human user and the rest of the security facilities.

The management system, which is located in the user's end-system contains the client part of the client/server management system. Each user's end-system can in principle initiate management operations. However these operations will only be available to application processes with the appropriate privilege attributes. The management system contains the following functional blocks:

- system security management,
- security service management,
- security mechanism management,
- security of OSI management.

The message handling system contains the User Agent (UA) and the Message Store (MS).

The directory system contains the Directory User Agent (DUA).

The communication system contains ACSE and ROSE.

3.5 Components of Servers

All types of server contain the communication system and the security system. The security server, the interdomain and audit server, the security state and recovery server contain in addition to the above described components the directory system agent, which is used as a data base for the servers. The message handling server contains the Message Transfer Agent (MTA). Figure 5 shows the components of a secure message handling system.

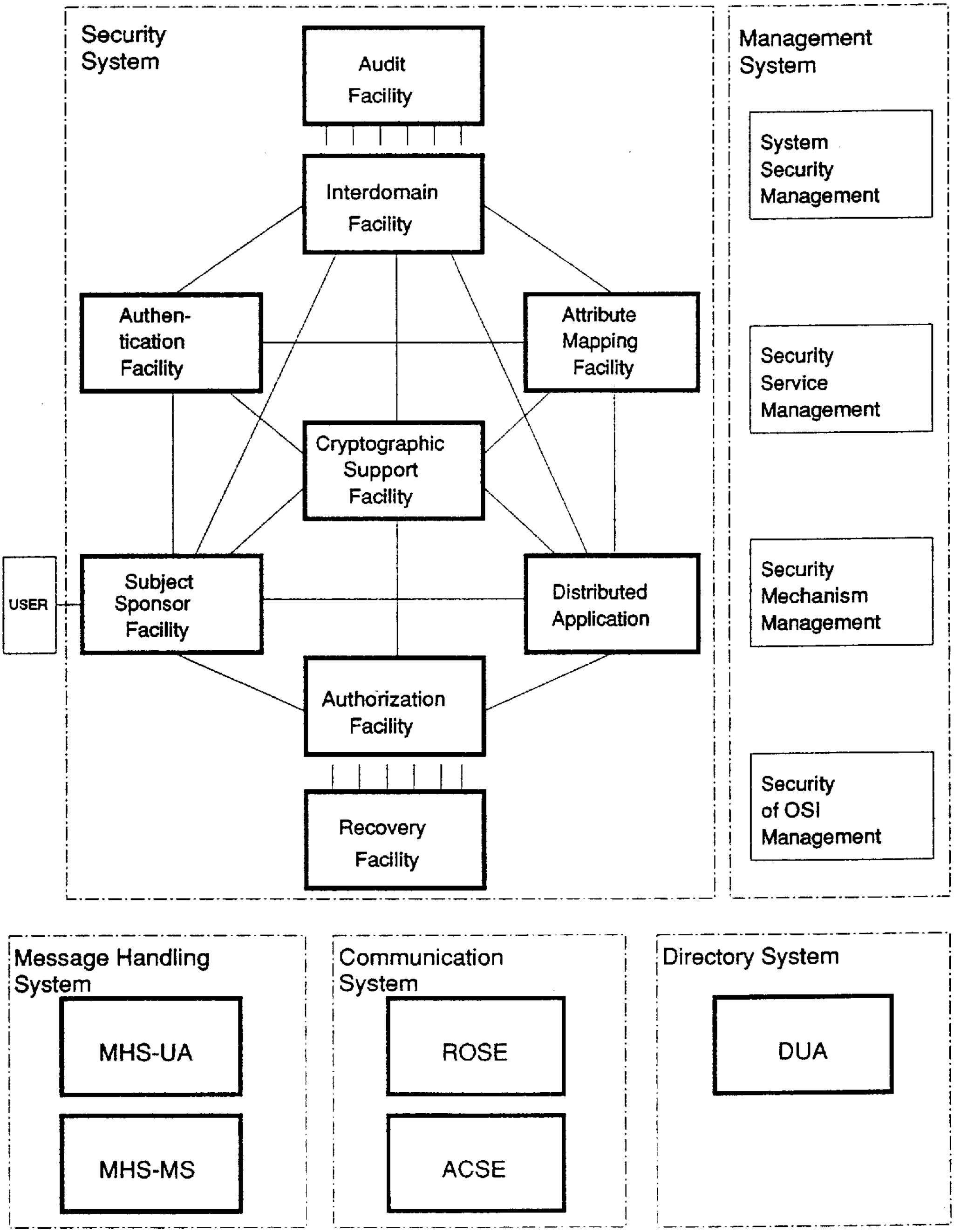

Figure 4- Components of user's end-system

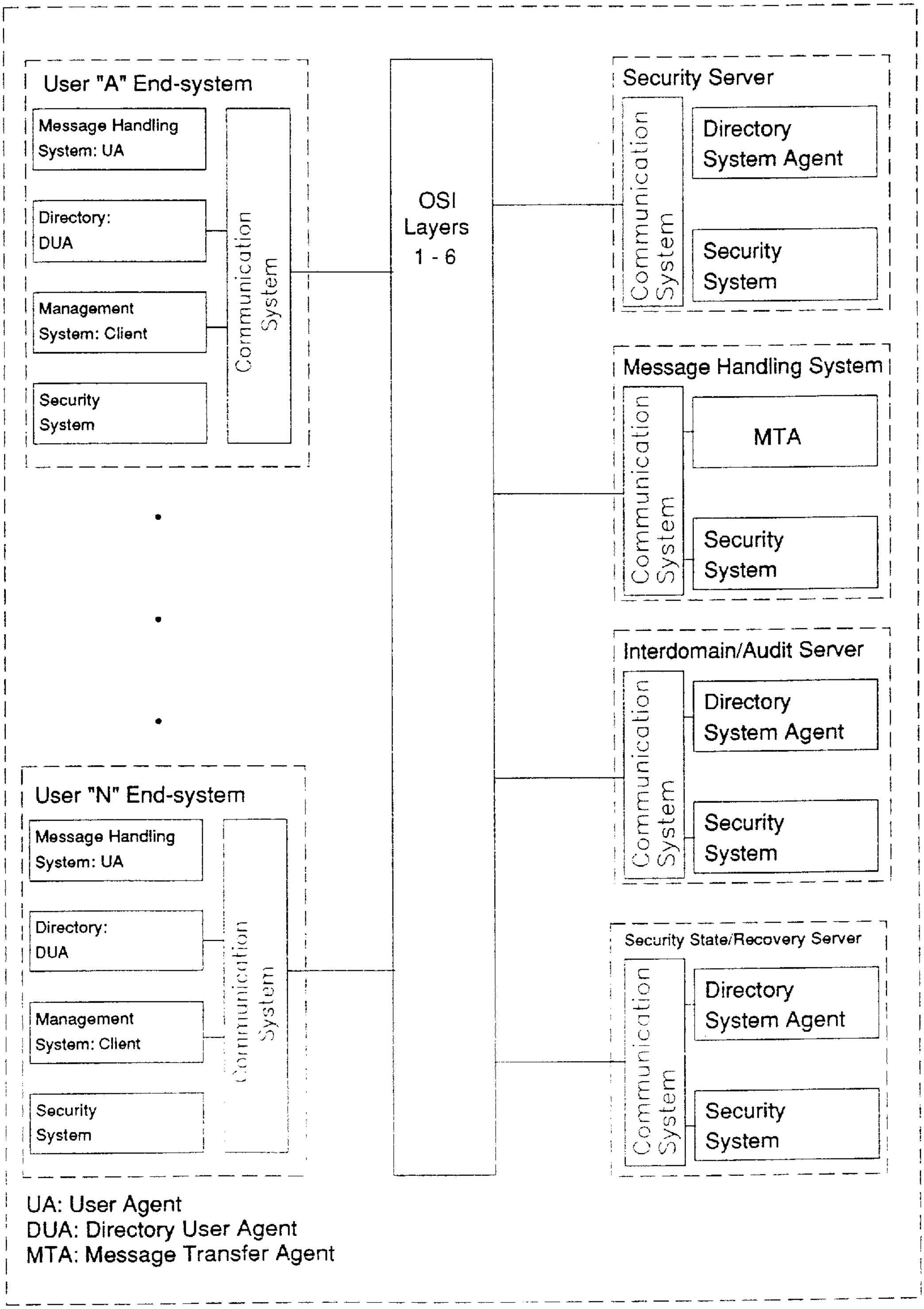

Figure 5- Secure Message Handling System

IV. CONCLUSIONS

This paper proposes two security-related ASEs in the OSI application layer as new common application-service elements to realize OSI secure communications. These proposed security-related ASEs provide a very simple interface to the user. The user only needs to indicate the general requirements for security function to be used. These security-related ASEs can be used for securing of existing and future OSI-specific applications.

Security in open distributed processing is very complex. The diamond with its great number of facets of brilliance should represent this complexity of security in open distributed processing. Each facet represents an element of this security system, and all the facets work together to reflect the structure of the underlying overall concept. This concept is a vision of the whole security system, implemented in hardware and software in an architecture which should provide maximum value to the users and is adaptable to meet user's future demands.

REFERENCES

(1) ECMA/TR42	Framework for Distributed Office Applications
(2) ECMA/TR46	Security in Open Systems - A Security Framework
(3) ECMA Standard XXX	Security in Open Systems - Data Elements and Service Definitions
(4) ISO 7498/2	Basic Reference Model, Security Architecture
(5) ISO 9545.1	Open System Interconnection, Application Layer Structure
(6) CCITT X.400	Message Handling System
(7) CCITT X.500	The Directory
(8) ISO/JTC1/SC21 N2688	Part 7: Security Management Service Definition