

Essay 10

Representative Organizations That Participate in Open Systems Security Standards Development

Harold J. Podell

This essay presents an introduction to representative organizations that participate in open systems security standards development. The reason we focus on open systems security standards is the international need to support secure electronic commerce and trade. Open systems standards, including security standards, support interoperability and security of business and government computer network communications. International agreements include a commitment of the standards organizations to support open systems security standards to achieve “brand independent” network configurations and interfaces. These agreements mean, in part, that large organizations will be gradually phasing out proprietary network protocols. These protocols could be replaced during the next 10 to 20 years with open systems standards and implementable solutions. Included in these solutions could be the evolution of the mobile office and new international ways to extend the concepts of electronic commerce and trade. The long-term trends for the development of open systems standards and software systems include supporting more effective business processes and communications, and meeting the needs of secure electronic commerce and trade.

We develop four interrelated issues to interpret current trends in the development of selected open systems standards. First, we introduce security standards as important economic, political, and cultural issues to support international electronic commerce and trade. Second, we present a conceptual view of open systems security standards relationships. Third, we briefly overview the

committee structure of the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Telecommunications Union-Telecommunications Standardization Sector (ITU-T) — formerly the International Telegraph and Telephone Consultative Committee (CCITT), and selected national and regional organizations. Our ISO/IEC and ITU-T focus is on the security standards responsibilities of the international committees and groups. Fourth, we overview ISO/IEC Joint Technical Committee 1 — Information Technology (JTC1) security standards activities. This overview highlights some of the security functions of three subcommittees doing security work: SC27 — Security Techniques; SC21 — Information Retrieval, Transfer, and Management for Open Systems Interconnection (OSI); and SC6 — Telecommunications and Information Exchange between Systems.

Open systems standards are necessary to support international commerce and trade and to assist computer and network companies in the process of marketing essentially the same secure product line in two or more countries. We anticipate that open systems security standards will eventually be more fully developed and products will be tested against the standards. There are important inputs to the development of these security standards. For example, questions remain regarding

- international commerce;
- architecture, which refers to the placement and relationships of certain functions, such as the required security services and mechanisms; and
- open systems.

The three leading organizations in the international standards community are the International Organization for Standardization, International Electrotechnical Commission, and International Telegraph and Telephone Consultative Committee (ISO, IEC, and ITU-T).

Open systems security standards may define the functionality and assurance necessary for a given set of security services. At the present time, functionality and assurance are the main focus of the security standards groups in ISO, IEC, and ITU-T, as well as national and regional organizations in the United States and Europe. Security criteria are examples of evolving international security standards activities that will consider assurance and functionality. National and regional contributions to the evolving international security criteria — Common Criteria (CC) — include the following:

- the draft US *Federal Criteria for Information Technology Security* (FC) [NIST92],
- the European *Information Technology Security Evaluation Criteria* (ITSEC) [ITSE91], and
- the Canadian *Trusted Computer Product Evaluation Criteria* (CTCPEC) [CANA92].

The CC is being developed under control of the Editorial Board (EB), which consists of members from North America and Europe. When the CC is ready, the EB will make it available to ISO Subcommittee (SC) 27, Working Group (WG) 3.

A wide variety of standards-promoting bodies interact in many ways with the international standards community. For example, the Open Software Foundation (OSF), which was formed in May 1988, develops core software technologies to support openness for the international Unix community. OSF has in excess of 200 international members that vary from commercial organizations to universities and government organizations. With respect to secure communications, OSF supports OSF/1. OSF/1 offers a variety of core (or “kernel”) services derived from the Mach operating system. In addition, a vendor association — X/OPEN — is dedicated to the creation of an internationally supported, vendor-independent Common Application Environment (CAE) based on industry standards.

Another example of a standards-promoting body is the European Computer Manufacturers Organization (ECMA). ECMA furnishes input to the standards developers at ISO, IEC, and ITU-T. Two technical committees (TCs) in ECMA concerned with security issues are TC29 — Office Document Architecture (ODA) Security, and TC36 — Security Evaluation Criteria and Open Systems Security.

One of the first official open systems security standards for the international community was the OSI Security Architecture (ISO 7498-2), which was voted on and agreed to by members of ISO [ISO89]. Many of the terms in this essay, such as security services and mechanisms, are derived from this architecture. ISO is the international umbrella organization of voluntary national standards organizations, such as the American National Standards Institute (ANSI), the British Standards Institute (BSI), and the Deutsches Institut für Normung (DIN). IEC is a companion organization that now participates by means of a joint technical committee (JTC1) with ISO in the joint development of open systems standards.

Other examples of open systems standards evolution include the development of a compatible or harmonized suite of standards. For example, ISO has issued a Digital Signature standard (ISO 9796) [ISO91a], and ISO/ITU-T has issued standards for Directory Security (X.509) [CCIT88c]. X.509 Secure Directory can be used with ITU-T X.400 and re-

lated Message Handling System (MHS) standards to support secure electronic communications. Through an ISO/ITU-T collaboration agreement, a ITU-T recommendation has the international status of an ISO standard. In addition, there are many draft open systems security standards in process.

An important issue is the gradual expansion of the scope of open systems security standards. The long-term trend is to evolve from open systems interconnection (OSI) (for example, ISO 7498-2, ITU-T X.400 MHS, and X.509 Secure Directory) to open systems (for example, ISO/IEC draft open systems frameworks, databases, and Open Distributed Processing (ODP)). This evolution is occurring, in part, because of the international demand for secure electronic commerce and trade. The initial focus on OSI — the network building blocks of information systems — is being supplemented with consideration of applications in the end systems (for example, hosts, workstations, or PCs).

Standards evolve, and the international community strives to develop a comprehensive suite of open systems standards harmonized with the national and regional efforts. Such standards are targeted to provide both functional standards and assurance criteria for business and commerce.

The international trend toward open systems has been augmented with a trend to adopt internetworking standards, such as Transmission Control Protocol (TCP) and Internet Protocol (IP) are Internet standards that approximately relate to OSI Layers 4 (Transport) and 3 (Network), respectively. Security standards are also being implemented in JTC1 and the Internet international communities. Examples include ITU-T X.509 for Secure Directory, and Internet RFCs (Request for Comments) 1421-4 for Privacy Enhanced Mail (PEM). Several nations, such as the United Kingdom and the United States, are updating their network guidance to reflect this trend to include open systems and internetworking standards.

At the time of writing, the international standards community has agreed to integrate the Internet standards process into JTC1. An agreement drafted between the Internet Architecture Board (IAB) and JTC1 appears to provide a high degree of standards autonomy to the Internet Engineering Task Force (IETF). IETF would be performing SC6 functions.

In addition, user- and market-led initiatives are being developed and coordinated by organizations such as X/OPEN, ECMA, and the World Federation of the Manufacturing Automation Protocol/Technical Office Protocol (MAP/TOP) Users Groups. MAP/TOP is an internationally accepted set of specifications for open communication based on ISO/OSI standards. MAP/TOP is produced by a standards consortium: the North American MAP/TOP Users Group. The secretariat for this group is the Corporation for Open Systems International (COS). International con-

tributions are utilized in the development of each version of MAP/TOP, such as MAP/TOP 3.0. The systems security versions have been officially accepted by the Australian, European, and Japanese users groups.

Our discussions in this essay are limited in scope and currency because of the magnitude of the international security standards processes. For supplemental information, we refer you to the publications from the organizations that are discussed. In addition, security standards committee and group assignments are gradually evolving in the representative organizations, such as ISO, IEC, and ITU-T. We are only sampling representative security activities from certain standards organizations. There are many national and regional standards organizations doing important work that we do not mention.

In developing the ISO, IEC, ITU-T, national, and regional perspectives for this essay, considerable review effort was provided by two internationally respected authorities: Marshall D. Abrams (US) and E. (Ted) J. Humphreys (UK). Their comments and insights have contributed to the accuracy and balance of the presentation. If there are any omissions or misinterpretations, they are the author's responsibility.

Economic, political, and cultural issues to support international electronic commerce and trade

Open systems security standards may be considered as economic, political, and cultural issues. We need the standards to support the international sale of information technology (IT) equipment and to support international electronic commerce and trade. An example of a current issue is the international marketability of IT equipment and systems. Until there are international agreements on interoperability and functionality for reciprocity of security evaluations of IT equipment and systems, hardware and software vendors face difficult investment and marketing decisions.

Internationally agreed upon profiles —International Standardized Profiles (ISPs) —are aimed at helping procurement agencies and software developers focus on those options that will support global inter-networking and functional selectivity. For example, an ISP may contain security features if one (or more) of the base standards to which it refers contains security features. However, with regard to certain functional and assurance aspects of a secure product, a hardware or software developer of a trusted or security enforcing operating system has to determine to submit the system for a security evaluation in one or more countries. This can become very costly if different nations use different security criteria and procedures for the evaluations.

Control of the security evaluation of products is also an economic, political, and cultural issue, because vendors and systems developers need creditability and marketability for their products and systems. Creditabil-

ity is the need to have a product or system evaluated and “approved” by an independent third party as secure for certain applications. Marketability is the ability to meet national, regional, and eventually international security criteria and standards that are required by the using organizations. Marketability can be enhanced through the construction and implementation of standards.

GOSIP for a particular nation is based, in part, on international standards. For example, the US GOSIP Federal Information Processing Standard (FIPS) is based on a profiled subset of the ISO and ITU-T international open systems standards, implementers’ agreements developed at the Open Systems Environment Implementors Workshop (OIW), and US federal government requirements. New versions of the GOSIP FIPS are produced as more open systems standards are agreed to. Open systems security standards can be considered for GOSIP as they are produced.

An international long-term goal is to develop an integrated set of open systems security standards for the interoperability of electronic commerce and trade. The open systems security standards development is occurring in parallel with and is related to the development of standards to support international commerce and trade, including marketability of IT equipment and systems. For example, substantial work is in process to fully develop open systems security standards that provide for peer-entity authentication, access control, and nonrepudiation. Business transactions supported by electronic commerce and trade require that the entities be securely identified at both ends — that is, they require authentication. Each business entity also requires that the data origin and receipt of electronic communications, such as business transactions, be verifiable — they require nonrepudiation.

Conceptual view of international open systems standards relationships

An overview of selected international open systems security standards relationships is presented to illustrate the complex interrelationships in open systems security standards development. In a sense, this discussion can serve as a “conceptual road map.” The purpose of this road map is to assist in your understanding of the conceptual relationships of several of the interrelated open systems security standards activities in ISO, IEC, and ITU-T. We provide several figures to assist in visualizing this road map. Another way of viewing the road map is as a scorecard. There is a saying, “You cannot tell the players without a scorecard.” More detailed taxonomies of open systems security standards are available elsewhere [HUMP92a, ITAE92b].

Open systems standards support international electronic commerce and trade as shown in Figure 1. Figure 1 shows that the Common Appli-

cation Environment (CAE) for distributed processing applications depends on an evolving set of open systems standards, such as those that support Electronic Data Interchange (EDI). This figure presents a conceptual view of security standards at a high level of abstraction. Figures 2 and 3 present two more detailed views of selected aspects of Figure 1. To visualize the three figures, first you look at the entire picture (Figure 1), then you zoom in on the second level of detail for distributed applications (Figure 2), and finally you zoom in on the third level of detail for architectures, frameworks, Models/Guidelines, and techniques (Figure 3). The horizontal rectangles in Figure 1 suggest the importance of layers in viewing security standards. The five vertical bars represent operational requirements necessary for successful implementation of distributed applications, such as open systems management.

The three layers in Figure 1 show that distributed applications can be viewed as a higher-layer process that depends on protocols in an intermediate layer. The intermediate-layer protocols support functions such as EDI, file transfer, and interactive or transaction processing (TP).

Key

Open sys. mgmt.: Open systems management

Conform. testing: Conformance testing and security evaluation criteria

Inter. documents: Interpretive documents (user guideline, design manuals, and so on)

Oper. procedures: Operating procedures

Figure 1. Conceptual overview of international computer and network security standards (source: E.J. Humphreys [HUMP90b]).

The example that we discuss is the evolving set of open systems standards, represented in Figure 1 as supporting EDI. These standards are ITU-T Recommendations X.400 Messaging and X.500 Directory. As mentioned, X.509 is the Recommendation for Secure Directory. X.400 is the Message Handling Service (MHS) series of standards that consists of

1. a user agent to enable users to create and read electronic mail;
2. a message transfer agent to furnish addressing, sending, and receiving services; and
3. a reliable transfer agent to provide routing and delivery services.

X.400 has been augmented to reflect the need for security. EDI security issues are presented in more detail in Essay 18.

Other distributed applications shown in Figure 1 include file transfer, interactive or transaction processing, remote operation, distributed processing, database applications, and communications management. Security enhancement of open system security services and protocols is necessary to support distributed applications.

Figure 2. Intermediate-level conceptual view of international computer and network security standards (Source: E.J. Humphreys [HUMP90b]).

Key

Auth.: Authentication techniques

Int.: Integrity techniques

Access: Access control

Non-R.: Nonrepudiation techniques

-----: Nested (hierarchical) relationships within the hierarchical categories: architectures, frameworks, Models/Guidelines, and techniques.

- - -: Interrelationships (nonhierarchical) within the hierarchical categories frameworks and techniques

Figure 3. Detailed conceptual view of international computer and network security standards (source: E.J. Humphreys [HUMP90b]).

In addition to the need for standards for distributed applications, there are five additional requirements, shown in Figure 1, which we referred to as vertical bars. These five additional requirements support the following operations:

1. interfaces;
2. open systems management;
3. conformance testing and security evaluation, certification, and accreditation;
4. interpretive documents (user guidelines, design manuals, and so on); and
5. operating procedures.

Conceptually, Figures 2 and 3 further illustrate the relationship of distributed processing applications to security architectures and supporting standards and draft standards. EDI and other distributed applications depend, in part, on an interrelated set of security architectures, frameworks, Models/Guidelines, and techniques. ISO, IEC, and ITU-T are working closely on developing the applicable open systems standards. See Essay 18 for further discussion of EDI message security.

We briefly define each of these terms, which represent a family of open systems standards and draft standards activities. First, as mentioned, security architectures refer to the placement and relationships of certain functions, such as the required security services and mechanisms. There are hierarchical relationships among the architectures. For example, the Open Systems Security Architecture could apply to database and/or other open systems architectures. The Open Systems Security Architecture covers the requirements for distributed applications and Open Distributed Processing (ODP). The Distributed Application Architecture is also supported by the OSI Security Architecture (ISO 7498-2) [ISO89]. This hierarchy has important implications. For example, as the original focus of OSI expands to include end systems, we need to supplement the OSI Security Architecture with an Open Systems Security Architecture.

In addition to the hierarchical relationships, there is a need for open systems management to integrate effective support for EDI processing. Open systems management interfaces with, relies on, and interacts with the set of architectures, frameworks, Guidelines, and techniques.

The architectures are supported by frameworks. Frameworks define generic solutions and ensure consistency in the security enhancements. As we have mentioned, a wide variety of frameworks is in process. These

address or will address authentication, access control, audit, nonrepudiation, confidentiality, integrity, and key management. The international standards responsibility for developing frameworks is primarily in a joint technical committee operated by ISO and IEC in collaboration with ITU-T.

An example of a framework is the Authentication Framework, which defines the basic concepts for authentication, identifies the possible classes of authentication mechanisms, and defines the services for these classes of authentication mechanisms [ISO91d]. The Authentication Framework identifies functional requirements for protocols to support these classes of authentication mechanisms and identifies general management requirements for authentication.

Models/Guidelines detail how and when mechanism and framework elements are combined. We briefly introduce the Models/Guidelines under development. Models/Guidelines are being developed by ISO/IEC Joint Technical Committee 1 — Information Technology (JTC1). The three subcommittees (SCs) that are doing the work are SC27 — Security Techniques; SC21 — Information Retrieval, Transfer, and Management for Open Systems Interconnection; and SC6 — Telecommunications and Information Exchange between Systems. Below, the entries in parentheses are the subcommittee (SC) and work group (WG) doing the specific work. There are Security Models/Guidelines in process for:

1. security mechanisms and techniques, for example, authentication (ISO/IEC 9798-1) and nonrepudiation (SC27);
2. Transaction Processing (TP) Security Model (SC21/WG5);
3. Generic Upper Layers Security (GULS) (SC21/WG8); and
4. Lower Layers Model/Guideline (SC6/WG4).

Security in the application and presentation layers is addressed in GULS. Security in the transport and network layers is the focus of the Lower Layers Model/Guideline.

Techniques and mechanisms are necessary to support the provision of open systems services and protocols. Techniques are the responsibility of Subcommittee 27 — Security Techniques (JTC1/SC27). Mechanisms are the methods to implement security services. In addition to responsibilities for security techniques, SC27 (WG3 — Security Evaluation Criteria) is involved in the development of a harmonized set of international security evaluation criteria.

The development of the Common Criteria (CC), originally expected to be complete in the spring of 1994, will use the WG3 draft criteria documents (Parts 1 through 3) as an initial framework. Specific inputs will include the ITSEC, CTCPEC, draft FC, and the comments received on all these documents.

Examples of techniques include the methods necessary to support authentication, data integrity, access control, and nonrepudiation. Techniques

are available in three broad categories: cryptographic, noncryptographic, and trusted or security enforcing functions. Important cryptographic techniques in addition to encipherment (encryption) are key management, digital signature, hash functions, zero knowledge techniques, and modes of operation. Digital signature is a mechanism that supports the business need for nonrepudiation and private communications. Public key cryptography is necessary for effective implementation of digital signature. Hash functions are used with digital signatures to reduce variable messages to unique fixed-length representations, such as a 128-bit message digest or “fingerprint.” A message digest is encrypted by a public key algorithm using a key to develop a digital signature. See Essay 15 on cryptography for further discussion.

Zero knowledge techniques can be used for authentication, where any exchange authentication information cannot be used to produce valid exchange authentication information. Further, a single verification of authentication information may be sufficient to verify exchange authentication information produced by different claimants. One example of a zero knowledge technique is a process to select from a set of “problems,” which the challenged entity must solve and combine together in such a way as to demonstrate ability to solve the problems without revealing exactly how.

Examples of noncryptographic techniques include the use of trusted third parties in networks to support nonrepudiation, audit, and accountability. In addition, availability can be considered as a noncryptographic technique (as well as one of the three aspects of IT security — protection against loss of confidentiality, integrity, and availability).

Another way of expressing the relationships necessary for successful standards development is to focus on the need for harmonization [HUMP89c]:

Open systems: The harmonisation of communications between computer systems to allow internetworking independently of the nature of the systems involved.

There is no one international standards organization that has produced a set of integrated computer and network and related security standards that meets the needs of international electronic commerce and trade. We have introduced several organizations that are working separately and together to develop the required architectures, frameworks, Models/Guidelines, and techniques.

An introduction to ISO, IEC, ITU-T, and related liaison organizations

ISO, IEC, ITU-T, and related liaison organizations are introduced to illustrate their roles in the open systems standards process. ISO and IEC are major umbrella organizations for national voluntary standards organizations, and ITU-T is an influential treaty standards organization.

Our focus in this essay for ISO and IEC is on Joint Technical Committee 1 — Information Technology (JTC1). More formally, this committee is referred to as ISO/IEC JTC1 — Information Technology (ISO/IEC JTC1). As mentioned, ANSI is the secretariat for JTC1, and other nations serve as the secretariats for the various subcommittees (SCs) and work groups (WGs).

Again, the three major SCs concerned with security are SC27 — Security Techniques; SC21 — Information Retrieval, Transfer, and Management for OSI; and SC6 — Telecommunications and Information Exchange between Systems. SC21 is responsible for all of the frameworks except for key management, which is being developed by SC27. SC6 is responsible for the OSI Lower Layers. Coordination with ITU-T Study Group VII (Data Communications Networks) is also maintained on the development of frameworks.

Certain ISO technical committees (TCs) focus on security in addition to their sectorial focus. For example, TC68 — Banking and Related Financial Services coordinates with JTC1 subcommittees on a wide variety of security standards pertaining to conventional (symmetric) and public key (asymmetric) cryptographic algorithms, such as “Key Management by Means of Asymmetric Algorithms” (ISO CD [Committee Draft] 11166) [ISO91b].

ITU-T has four classes of members. Administrative or full members can be any of the International Telecommunications Union’s approximately 160 member nations. A second class of full members consists of the Recognized Private Operating Agencies (RPOA), which are the international telecommunication services providers. Class three consists of the Scientific or Industrial Organizations (SIO). They provide a base of technical expertise but do not participate in the plenary sessions. The major international organizations constitute the fourth class of members. These organizations are invited to meetings to facilitate international coordination of standards development. ISO and IEC are examples of major international organizations. Not all standards organizations are included in this class.

ITU-T develops open systems recommendations or standards related to the OSI model. ITU-T also develops open systems and open systems security standards that will have a broader scope, such as applicability to EDI.

An important aspect of the trend toward open systems standards is that ITU-T has entered into formal agreements to harmonize its recommendations with the standards of ISO and IEC. A successful example is the ITU-T lead role in defining an approach to a Secure Directory (X.509) to support secure open systems communications [CCIT88c]. This directory can be conceptually viewed as a secure electronic telephone book to support computer communications.

ISO, IEC, and ITU-T, and Open Distributed Processing. An example of a long-term objective of the ISO, IEC, and ITU-T international cooperative efforts is their support of the development of Open Distributed Processing (ODP). ODP can be considered as including user requirements, conceptual design and specifications, software design and development, and infrastructure building blocks, as well as the realized components [CHAB90]. ODP systems will be developed as an aspect of open systems that pertains to distributed processing systems. Therefore, ODP systems will be users of communication data security services and distributed applications.

The planned ODP security architecture is considered by ISO/IEC JTC1/SC21 as a candidate for a set of security architectures to support open systems security [ISO91c]. This set has only one security architecture (ISO 7498-2) at present. Other possible security architectures could include a database security architecture.

JTC1 subcommittees. Many of the ISO/IEC JTC1 subcommittees and special working groups that focus on open systems issues are concerned, in varying degrees, with open systems security issues. The security and related activities of selected ISO/IEC JTC1 subcommittees are highlighted in this section.

Several ISO/IEC JTC1 subcommittees are briefly identified with some of their security responsibilities. SC6 — Telecommunications and Information Exchange between Systems has responsibilities for Open Systems Interconnection (OSI) security, such as the Lower Layers security guidelines, Network and Transport Layer security, and security protocols. SC17 — Identification and Credit Cards is responsible for integrated circuit (IC) card security. Examples include IC cards and IC-card communication protocols.

As mentioned, SC21 — Information Retrieval, Transfer, and Management for OSI is an active and well-known SC for security issues. Examples of responsibilities include OSI architecture (WG1) and management (WG4); specific application services, such as a preliminary TP security model (WG5); ODP (WG7); and Generic Upper Layer Security (GULS) (WG8).

Another SC is SC22 — Programming Languages, which focuses on the security interface for POSIX. POSIX is the Portable Operating System

Interface for Computer Environments for Unix-like operating systems and is sponsored by the Institute of Electrical and Electronics Engineers (IEEE). The US federal government's FIPS 151-1 specifies POSIX and is based on IEEE Standard 1003.1-1988. FIPS 151-1 makes certain optional capabilities mandatory for US federal procurements. ANSI approved IEEE Standard 1003.1-1988 on November 10, 1989. IEEE Standard 1003.1-1990 has been proposed as an international standard, ISO 9945-1. A rapidly growing number of US vendors claim conformance for their products. POSIX products are being delivered as part of US federal procurements.

As mentioned, one of the newer SCs is SC27 — Security Techniques. SC27/WG1 — Security Requirements, Services and Security Guidelines is responsible for a variety of documents including:

1. Glossary of IT Security Definitions,
2. Entity Authentication Mechanisms — General Model,
3. Key Management Framework,
4. Guideline for the Management of IT Security, and
5. Security Information Objects.

WG2 — Security Techniques and Mechanisms is responsible for a wide variety of documents pertaining to topics such as integrity, authentication, digital signature, hash functions, nonrepudiation, and key management.

Other ISO technical committees. In addition to JTC1, there are other ISO technical committees (TCs) that can have an impact on security. For example, both banking and EDI TCs have activities that may pertain to security. TC68 — Banking and Related Financial Services addresses a wide variety of banking security issues, which interface with JTC1 activities. The example we have introduced is “Key Management by Means of Asymmetric Algorithms Part 2: Approved Algorithms Using RSA Cryptosystem — CD 11166” [ISO91b]. We introduced this example in the earlier section “Introduction to ISO, IEC, ITU-T, and Related Liaison Organizations.” Our discussion pertained to the activities of TC68. The CD 11166 coordination is part of the responsibilities of SC2 — Operations and Procedures. Other security responsibilities of TC68 include SC6 — Financial Transaction Cards, Related Media and Operations. Two WGs that focus on security are WG6 — Security in Retail Banking and WG7 — Security Architecture of Banking Systems using the Integrated Circuit Card.

ITU-T study groups. There are several ITU-T study groups (SGs) that are actively concerned with security issues, such as those pertaining to ITU-T X.200, X.400, X.500, and distributed applications security. Examples of these SGs are presented. Security issues are included in paren-

theses after the study group name: (1) SG VII Q18 — Message Handling Systems (MHS framework and EDI security) and (2) SG VII Q19 — Framework for Support of Distributed Applications (OSI Security Architecture and frameworks, Generic Upper Layer Security (GULS), and security model for distributed applications). The frameworks and Security Models/Guidelines are coordinated as a joint work item with ISO/IEC.

Two other ITU-T SGs that work on security issues are (1) SG VII Q20 — Directory Systems (authentication-X.509 and access control) and (2) SG VIII Q28 — Security in Telematic Services. SG VIII Q28 is working on a Proposed Security Framework for Telematic Services.

United Nations/Economic Commission for Europe (UN/ECE). In addition to ITU-T, there is a second treaty international organization concerned with open systems security standards. This organization is called the United Nations/Economic Commission for Europe (UN/ECE). There are approximately 34 UN/ECE member states located in North America and Europe.

The UN/ECE was created by the Economic and Social Council of the United Nations. The Electronic Data Interchange (EDI) standards work is performed by UN/ECE Working Party 4 on Facilitation of International Trade Procedures (UN/ECE WP4). An example of a national representative is the US Department of Transportation. UN/ECE performs a standards function for EDI, which has produced a standard that is becoming the international standard — EDI for Administration, Commerce and Transport (EDIFACT).

Examples of security-related standards-promoting bodies. One view of the open systems security community at a given point in time is a structural view. An overview of selected European, international, and United States security-related standards-promoting bodies working on open systems security standards issues is presented. We discuss these organizations to illustrate some of the sources for many of the security standards ideas that are considered by JTC1 and ITU-T.

Selected European organizations. European standardization of information systems security is performed by three organizations that broadly correspond to ISO, IEC, and ITU-T, respectively:

1. Comité Européen de Normalization (CEN),
2. Comité Européen de Normalization Electrotechnique (CENELEC),
and
3. European Telecommunications Standards Institute (ETSI) [ITAE92b].

We use the term information systems security to include the security of IT systems, telecommunications, and other systems and services that handle information in electronic form.

Information systems security standardization in Europe is an evolving process that considers the experience of the European IT industry and users. The standardization process makes use of existing solutions and proposals, and is aimed at providing future solutions for new technical developments and market-driven requirements. Priority and preference are given to the adoption of international work items, with the intention of transposing the results into European Normen (ENs) (European Normal Standards) or European Norme Voransgaben (ENVs) (European Normal Prestandards) when appropriate. Provisions of two agreements are used — the Vienna Agreement and the ISO/CEN Cooperation Agreement. These standards may be supplemented by additional ENVs as necessary for European implementation.

The three official European organizations participating in the development of regional and international open systems security standards each represent important constituencies in the European Community (EC). CEN is concerned with the harmonization of standards for European ISO members. CENELEC is concerned with harmonization of standards for European IEC members. ETSI focuses on the harmonization of standards for the European ITU-T members. ETSI was created as a result of the activities of the European Conference of Postal and Telecommunications Administrations (CEPT) to produce standards for European telecommunications.

The CEN/CENELEC/ETSI Information Technology Steering Committee (ITSTC) established the Information Technology Advisory Expert Group on Information Systems Security (ITAEGV) in 1991. ITAEGV is developing a framework for future European IT security standards [ITAE92b] from a baseline document, *Taxonomy of Security Standardisation* [HUMP92a]. The baseline document was prepared by an earlier ad hoc group under the secretariat of CEN. The work of ITAEGV is to update this taxonomy, taking into account recent developments in the fast-changing world of information systems security.

A life-cycle orientation is used for the ITAEGV framework. Therefore, the classification scheme of information systems security standards reflects life-cycle phases. Briefly, the scheme covers:

1. S0, Architecture and Modeling;
2. S1, System Design;
3. S2, System Development and Implementation; and
4. S3, System Operational Aspects.

The framework includes a directory of standards that are placed in these classifications.

Our discussion of European security standards uses the ITAEGV work as of the time of writing. Since this process is ongoing, we suggest that the reader refer to the current version of ITAEGV work for the most up-to-date report on progress in European IT security standards. In addition, since ITAEGV makes extensive use of IT security standards prepared at the international level, current versions of JTC1 International Standards (ISs) and Draft International Standards (DISs) can be reviewed for additional up-to-date references.

We briefly discuss the three European standards bodies — CEN, CENELEC, and ETSI — and two standards-promoting bodies — the European Workshop for Open Systems (EWOS) and ECMA. Eighteen member countries of the European Community (EC) and the European Free Trade Association (EFTA) are the European countries that may participate in CEN and CENELEC. CEN and CENELEC are responsible for the drafting and ratification of harmonized European standards — ENs and ENVs. Further, there are proposed ENVs (prENVs).

Membership in ETSI is open to any organization that demonstrates an interest in European telecommunications standardization. At the time of writing, there were almost 300 members — manufacturers, telecommunications operators, administrations, and users. ETSI produces European Telecommunication Standards (ETSS) and Interim Telecommunication Standards (I-ETSS), corresponding to ENs and ENVs, respectively. ETSI also produces technical reports (ETRs) and performance specifications. For example, ETSI products pertain to certain aspects of the Special Mobile Services Group (GSM) pan-European digital cellular telephone system.

The European Workshop for Open Systems (EWOS) was established primarily to provide an open international forum to develop worldwide harmonized profiles and associated test specifications for open systems. EWOS is a standards-promoting body working in the forefront of standardization, building technical consensus, and directly contributing to CEN, CENELEC, ETSI, and ISO. EWOS was established by the main European IT supplier and user organizations with the support of CEN, CENELEC, ETSI, and the European Commission. Functional profiles are developed by EWOS to assist in utilizing OSI standards. In addition, EWOS works in collaboration with ETSI to develop profiles, such as X.400 [STRA92]. When these documents reach EN status, based on balloting, they can be considered stable.

EWOS participates in the development of International Standardized Profiles (ISPs) in collaboration with the North American regional workshop — the Open Systems Environment Implementors Workshop (OIW) — and the Pacific Rim-Asia Oceanic Workshop (AOW). AOW participation includes representatives from Japan, Korea, China, and Australia. As mentioned, ISPs are aimed at helping procurement agencies and software developers focus on those options that will support global in-

ternetworking and functional selectivity. In general, the specification of an ISP having security features has two distinct parts, one concerned with security-related functions and one concerned with other functions. A security subprofile specification is the specification of a distinct set of security-related functions in an ISP. An ISP may have one or more security subprofiles. ISPs are useful in effectively shortening the time it takes for certain standards to reach their final draft stage.

To assist in international collaboration, EWOS has established a Regional Workshop Coordinating Committee (RWS-CC) with OIW and AOW. The RWS-CC seeks to coordinate developments, acknowledging that worldwide interoperability requires worldwide harmonized implementation specifications. These specifications are to be approved at the ISO/IEC JTC1 level. Mechanisms are also being developed to ensure that only harmonized results are submitted for approval by JTC1 as International Standardized Profiles.

As mentioned, ECMA is also a standards-promoting body that furnishes input to the standards developers at ISO, IEC, and ITU-T. Two technical committees in ECMA that address security issues are TC29 — Office Document Architecture (ODA) Security and TC36. The latter includes the work of two technical groups: one for security evaluation criteria and one for open systems security (the former TC32 was merged into TC36).

Selected US-based organizations. In this section we introduce five US-based organizations. Our first organization is the American National Standards Institute (ANSI), which is a voluntary organization for developing industrial standards. Participation is open to interested and qualified parties, including government agencies. As mentioned, ANSI is the US member of ISO and the secretariat for ISO/IEC JTC1. ANSI coordinates with many organizations, such as the US National Institute of Standards and Technology (NIST). Many ANSI standards are also NIST Federal Information Processing Standards (FIPS). In certain cases, NIST and ANSI standards are also ISO standards.

Our second organization is one of the international regional organizations that promote the acceptance of standards-based open systems products. The organization is the Corporation for Open Systems International (COS) [WALT91]. COS is a US-based organization with approximately 55 international members from several countries, such as Canada, the United Kingdom, and Germany. COS has been active in contributing to the creation of ISPs. Another COS contribution has been in effecting the development of several OSI and ISDN standard test systems, such as those for electronic mail, file transfer access and management, network management, packet switching, and Ethernet. In addition, COS created the first certification process for open systems standards-based products and services — the COS Mark Program. COS

also assisted in the development of the US GOSIP by sharing its COS Mark Program testing and registration process and procedures with NIST. As mentioned, COS also provides the secretariat for the North American MAP/TOP Users Group.

The Computer and Business Equipment Manufacturers Association (CBEMA) is our third organization. CBEMA is a US-based regional organization that provides technical assistance to ANSI. CBEMA is the US Technical Advisory Group (TAG) to JTC1 and the secretariat to the ANSI Accredited Standards Committee X3 — Information Processing Systems.

Fourth, we mention a US-based international professional organization that has worked with ANSI on security-related draft standards. The Institute of Electrical and Electronic Engineers is an ANSI-accredited standards organization. For example, the IEEE developed a draft standard IEEE 802.10 SILS (Standard for Interoperable LAN [Local Area Network] Security).

Our last US-based organization is the Open Systems Environment Implementors Workshop (OIW), which is a regional organization that participates in various aspects of security profiles and implementers' agreements activities. The IEEE and NIST are the cosponsors of OIW. OIW is the US regional equivalent of EWOS and, as mentioned, works closely with EWOS and AOW in RWS-CC. An objective of this cooperation is to achieve consensus on proposed International Standardized Profiles.

Selected overview of ISO/IEC JTC1 security standards activities

We provide an overview of selected security-related work in ISO/IEC to illustrate the nature of several of the activities that pertain to open systems security standards. Our focus in this section is on the security standards activities of Joint Technical Committee 1 — Information Technology (JTC1) [ISO91c, ITAE92b]. We present selected aspects of the security activities of SC27, SC21, and SC6 to illustrate the type of activity. Although in subsequent sections we do not discuss the security activities of SC18 — Text and Office Systems, we should mention them here. SC18 is working on X.400 MHS, X.435 EDI, and Office Document Architecture (ODA). These standards are important components of interoperability necessary to support electronic trade and commerce.

Selected security activities of SC27. First, we discuss several security activities of SC27. The scope of SC27 is identification of generic requirements, development of standards for security services, development of security guidelines, development of security techniques and mechanisms, and the standardization of security evaluation criteria. This work sup-

ports a wide variety of security standardization needs reflecting a typical development cycle:

1. requirements and policy,
2. security services and applications,
3. security mechanisms and techniques,
4. security elements,
5. security management techniques,
6. guidelines, and
7. quality and evaluation of design.

For example, the following types of work are in process:

1. requirements and policy, for example, for medical and transport informatics security, and hyper/multimedia systems (in liaison with SC18);
2. services, for example, Open EDI;
3. mechanisms and techniques — digital signature, authentication, integrity, and so on;
4. data elements and objects; and
5. security management, for example, key management.

SC27 is also working on guidelines, for example, for the management of IT security. In addition, other guidelines work includes development of a Glossary of IT Security Technology and guidelines on the use and application of Trusted Third Party (TTP) services.

The SC27 work on evaluation criteria includes security evaluation methodologies. A European example of a contribution to the state of the art in evaluation methodologies is the *Information Technology Security Evaluation Manual* (ITSEM) [ITSE92]. Inputs to SC27 for evaluation criteria include European work on ITSEC, Canadian work on CTCPEC, and North American work on the *Federal Criteria for Information Technology Security* (FC). In addition, there is a variety of interregional coordination, such as close coordination among work on CTCPEC and FC and the ITSEC activity.

Recent SC27 work items for the development of security evaluation criteria include a multipart standard: Part 1, “Model”; Part 2, “Functionality Classes”; and Part 3, “Assurance.” As mentioned, these three parts are used as an initial framework for the development of the Common Criteria (CC).

Selected security activities of SC21. Subcommittee 21 — Information Retrieval, Transfer and Management for OSI works on security standards, and in collaboration with ITU-T Study Group VII (SG VII) — Data Communications Networks, on architecture, frameworks, services and

protocols. This work includes OSI Security Architecture, Open Systems Security Frameworks, and ODP. SC21 work on services and protocols includes:

1. Generic Upper Layer Security (GULS) (Layers 6 & 7, Abstract Syntax Notation 1 (ASN.1)),
2. Association Control Service Element (ACSE) authentication,
3. Remote Operations Service Element (ROSE),
4. TP, and
5. File Transfer and Access Management (FTAM) security.

In addition, SC21 work on applications/management and interfaces includes X.500 security and OSI management.

SC21 is perhaps best known for early work on OSI security. The result was the first SC21 security standard on security architecture (ISO 7498-2). While the earlier focus of SC21 was on OSI security, today much of its work addresses the needs of open systems security. The requirement for an open systems focus could result in consideration of more comprehensive security architectures, since the current security architecture concentrates on OSI issues.

Security architectures: SC21. As mentioned, the OSI Security Architecture developed by SC21 provides the fundamental description of security services and related mechanisms for the OSI Basic Reference Model. In addition, the security architecture presents tables that define the positions in the ISO seven-layer model where the security services and related mechanisms could be provided. Examples of our security definitions that we derive from the OSI Security Architecture include the following terms for security services: authentication, access control, non-repudiation, integrity, and confidentiality.

Other architectures may be defined, as indicated in our conceptual discussion; however, to date there are no other architectures. SC21 is considering the need to develop broader architectures and their appropriate scopes.

Security frameworks: SC21, SC27. Each of the security frameworks documents in ISO/IEC is being developed or will be developed by SC21, except for key management, which is being addressed by SC27 — Security Techniques. Security frameworks are being developed to address the application of the security services in open systems. The term open systems is interpreted to include databases, distributed applications, Open Distributed Processing (ODP), and OSI. One reason for the frameworks is to provide a vehicle for defining the means of protection for systems and objects within systems as well as the interactions between systems. Frameworks use available information technology knowledge as a base-

line. For example, the access control framework relies on object-oriented technology. The frameworks do not focus on methodology for constructing systems and mechanisms for implementing security services.

As mentioned, frameworks define generic solutions to ensure consistency in security enhancements. Frameworks do not provide protocol elements. Rather, they address data elements and sequences of operations used for specific security services. Security services may apply to the activities of the communicating systems and their representatives or entities. In addition, security services apply to the data managed and exchanged by systems. The access control scope of the frameworks may interface with but not include any data elements that are application specific or associated only with local internal access of a system.

As discussed, the security frameworks being developed are authentication, access control, nonrepudiation, integrity, confidentiality, audit, and key management (SC27). These frameworks are being developed for the five security services and audit and key management.

Security Models/Guidelines: SC21, SC6. As mentioned, Security Models/Guidelines define the details concerning how and when mechanism and framework elements are combined. Security Models/Guidelines provide architectural representations for the development of application-independent security services and protocols. In addition, Security Models/Guidelines provide for the utilization of security services and protocols to meet security requirements for many types of applications. At the time of writing, examples of Security Models/Guidelines being developed include the OSI Upper (SC21 — GULS) and Lower Layers (SC6) Security Models/Guidelines.

Generic Upper Layer Security (GULS) is concerned with providing details for the security aspects of communication in the upper layers of OSI. These aspects of communication pertain to the positioning and the interrelations between security services and the Presentation and Application Layers. This Model/Guideline also describes the way security transformation functions — such as encryption (encipherment) and security checkvalue functions — are processed for the Presentation and Application Layers. In addition, the Model/Guideline presents a concept of security exchange and provides for overview discussions of entity authentication, data origin authentication, association access control, resource access control, nonrepudiation, integrity, and confidentiality. GULS also discusses the concepts of a security policy and security state.

The Lower Layers Security Model/Guideline (SC6) is concerned with providing details for the security aspects of communication in the lower layers of OSI (for example, the Network and Transport Layers). SC6 (Telecommunications and Information Exchange between Systems) is focusing on security interactions within the lower layers and between the upper and lower layers. This Model/Guideline also describes the

general security requirements for management across the lower layers to provide various types and levels of security.

Security in data management standards: SC21. A variety of data management standards is being developed to address many of the inter-related aspects of security in data management. For example, the Reference Model of Data Management (ISO DIS 10032) presents access control as a set of privileges. This reference model also provides an architectural Model/Guideline of access control, which considers access control data in a manner related to database data. The Model/Guideline presents a standardized approach to access control as a technical objective related to the standardization of data management. No other security service is supported within the scope of data management.

Another example is the Information Resource Dictionary System (IRDS), which is presented in IS (Information Standard) 10027. This document is a framework used to control and document the information resources in an enterprise. Control is provided for limiting access to data in the Information Resource Dictionary (IRD). The IRDS describes the type of data that could be used to control access.

Two other examples are the Remote Database Access (RDA) service and the Database Language SQL (Structured Query Language). The RDA (ISO CD [Committee Draft] 9579-1) provides for a terminal to have interactive access to a remote database. General-purpose support is presented in RDA. This support should be considered as a baseline when using “specialization” standards, such as SQL (ISO CD 9579-2).

In RDA, each user has to be identified as a valid user of the resource so the remote data resource can be opened and accessed. Important security attributes, such as user identity and authorization identity in the request/indication service primitives, are carried by RDA. A dialogue will be set up with a remote node if the user and authorization identities are valid. Certain functions are not performed by RDA, such as dictating the format or meaning of the security attributes.

The last example of a data management standard that we discuss is Database Language SQL (ISO 9075). Database Language SQL presents the logical structures and associated basic operations required for a SQL database. Users of SQL data or services are identified within SQL; however, the implementation specifics are defined outside the SQL environment. SQL “Catalogs” are used to group SQL data entities. These data entities are controlled by implementation specifics outside SQL.

SQL controls the user entities and “Catalogs.” Other SQL entities are created and owned by SQL users. The access privileges for the other entities are under the control of the creating user. This control may be delegated to the entities of other SQL users. The ability to grant privileges on an object is included in the set of privileges that may be delegated.

Security in OSI management: SC21. A variety of ISO documents relate to OSI management standards. Three are highlighted in this section:

1. *OSI Systems Management* (ISO 10164), which has many parts in various stages of draft and approval;
2. *Common Management Information Service (CMIS) Access Control* (ISO 9595 and ISO 9595/PDAM); and
3. *Directory Authentication Framework* (ISO 9594-8; ITU-T X.509).

In the first example, *OSI Systems Management* (ISO 10164) presents an OSI security management overview that pertains to the security management functions. The relationships are given for the security management functions, the OSI Reference Model, and the Audit Framework. Other aspects of OSI security management are being developed: *Security Alarm Reporting Function* (ISO 10164-5), *Security Audit Trail Function* (ISO 10164-8), and *Objects and Attributes in Access Control* (ISO CD 10164-9).

The second example is *Common Management Information Service (CMIS) Access Control* (ISO 9595 and ISO 9595/PDAM). The access control parameters pertaining to ISO 9595/PDAM are A-associate, M-get, M-set, M-action, M-create, and M-delete.

We conclude with the third example, *Directory Authentication Framework* (ISO 9594-8, which is technically aligned with ITU-T X.509). The *Directory Authentication Framework* presents the basis for strong authentication essential for electronic commerce and trade. A certificate, which is described in this recommendation, may be conceptually considered as an “electronic envelope.” The certificate is “sealed” cryptographically with a public key algorithm and the private key of a trusted third party in the network — the Certificate Authority. Conceptually, we can visualize that each certificate is a digital envelope that contains a digital “letter” with the identification of an authorized user in the network — the user’s public key.

More formally, the certificate may be considered as a security token protected by integrity and data origin authentication security services. The mechanism that provides this protection uses public key cryptography, such as RSA (Rivest, Shamir, and Adleman).

There is also a Directory Access Control Model developed for general use for access control of directory information (ISO 9594-1,2,3,4/PDAM1). This provides hooks to facilitate control of directory access. Amendments to parts 3 and 4 of the Directory Access Control draft document enable the use of external access control to supplement the access control in part 2.

Security in OSI applications: SC21. There are many provisions for OSI in a variety of applications. We highlight seven examples:

1. File Transfer, Access, and Management (FTAM);
2. TP;
3. Terminal Management (TM);
4. Security Exchange Association Control Element (ASE);
5. Association Control Service Element (ACSE) authentication;
6. Presentation Layer confidentiality
7. Presentation Layer cryptographic techniques.

Examples of work in OSI applications include an amendment to ISO 8571 to evaluate the applicable authentication and access control requirements for FTAM. A similar development has occurred in TP security. There is work to develop amendments to OSI (DIS 10026, parts 1, 2, and 3) that will focus on evaluation of the appropriate mechanisms to provide security services. The security services that are being considered include authentication, access control, confidentiality, integrity, and nonrepudiation. Other considerations related to security services include auditing, “management,” (access right) revocation, replay (protection), (prevention of the) denial of service, reliability, and traffic control confidentiality. The scope of these considerations includes TP resources and application entities.

There is a TM model (ISO CD 10184-1); however, there is no assessment of the security relevance of the TM model. Generic Upper Layers Security (GULS) is proposed as a multipart standard. Generic facilities are proposed to be defined to provide security services in OSI applications. Included in the proposal are a definition of the service and a protocol associated with the Security Exchange Service Element.

ACSE Authentication Service and Protocol is defined in an information standard addendum (ISO 8649/AMI, ISO 8650/AMI). An A-associate request and confirmation are defined in a field in the amendment. This field may contain arbitrary authentication information. Included in this example is work to determine conditions for ACSE authentication. The conditions are related to the applicable cryptographic mechanisms for use with ACSE authentication.

The Connection Oriented Presentation Service and Protocol (ISO 8822 and 8823) is being amended to provide confidentiality and integrity security services. Some of the security architecture (ISO 7498-2) connection-oriented security services are provided in Presentation Layer cryptographic techniques. The procedures and Presentation Layer protocol necessary to implement a set of security services are presented. The selected security services are peer entity authentication, connection confidentiality, selective field confidentiality, connection integrity, and selective field connection integrity.

Open Distributed Processing (ODP) security. The Reference Model of Open Distributed Processing (RM-ODP) contains six “aspects” of distributed systems (part II). Work is progressing on the RM-ODP (part I) to present the use and organization of security in distributed systems. The requirements to support security will be defined for specific systems (part II).

Summary

In this essay we have developed four interrelated issues concerning representative organizations that participate in open systems security standards development. Our discussions have included identification of the economic, political, and cultural needs for standards to support international electronic commerce and trade. We presented a conceptual view of open systems security standards relationships. Then we over-viewed the committee structure of the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Telecommunications Union-Telecommunications Standardization Sector (ITU-T), and selected national and regional organizations.

Our ISO/IEC and ITU-T focus was on the security standards work responsibilities of the international committees and groups. We presented a selected overview of ISO/IEC Joint Technical Committee 1 — Information Technology (JTC1). This overview included highlights of the security functions of three subcommittees: SC27 — Security Techniques; SC21 — Information Retrieval, Transfer, and Management for Open Systems Interconnection; and SC6 — Telecommunications and Information Exchange between Systems.