Essay 18

Electronic Data Interchange (EDI) Messaging Security

Ted Humphreys

The modern economy and the future wealth and prosperity of industry and commerce rely increasingly on the exchange of data and information, in electronic form, between business partners. The speed and reliability of the information exchanged coupled with the spread in the distributed use and application of IT are increasingly affecting the competitiveness of businesses and international trade. Electronic information exchanged in this way is growing in volume because of the increasing number of business partners that may be involved (suppliers, customers, manufacturers, bankers, carriers, and so on) and the numerous documents that need to be exchanged.

The performance of the system handling these documents can significantly affect the economy and future prosperity of a business. The ability to process and exchange trade data as quickly as possible allows stocks to be reduced at a profitable rate, helps cut financial costs, and gives firms such as this an additional competitive edge by improving the service offered to their customers. In addition to the speed, the flexibility in responding to customers' changing needs and desires adds value to the service being offered and creates better commercial relationships.

In response to the need for effective and efficient solutions to handle this way of doing business, Electronic Data Interchange (EDI) offers substantial advantages and opportunities. The EDI approach has been identified as the most important user base of open networks and likely to create one of the most fundamental changes in the way that future business is carried out. EDI is starting to be used in a growing number of market sectors, in a wide range of user applications. The use of EDI trading systems is underpinned in many respects by the need for security, and it is the use of commercially reasonable security features for EDI that will bring about its long-term success.

This essay looks at a particularly important aspect of EDI — the security of EDI messages. In particular, it focuses on the secure communica-

tions of EDI messages. To start with, some introductory material is presented that views security in the context of Open-EDI.

Security and the Open-EDI conceptual model

There have been many attempts over the years to understand the security requirements for EDI. One of the most important efforts is described in the European report "Security in Open Networks" [SOGI89]. This report, commonly referred to as the SOGITS Report, confirmed the business need for EDI security. It identified EDI as the most important and demanding use of open networks, and, through an extensive survey covering 59 organizations in 12 countries in Europe, it reinforced the need for a range of solutions addressing several key areas of technical work. Since the publication of this report, several other European and international initiatives have contributed to the progression of work in a number of areas.

One particular important activity involved the JTC1 special working group, which was responsible for the Open-EDI Conceptual Model [JTC191], and its successor JTC1/WG3, which will take forward the Open-EDI work within JTC1. Figure 1 is a high-level view of security that might be used in the development of an Open-EDI Security Model, set beside the JTC1 Open-EDI Conceptual Model as a point of reference [HUMP92b].

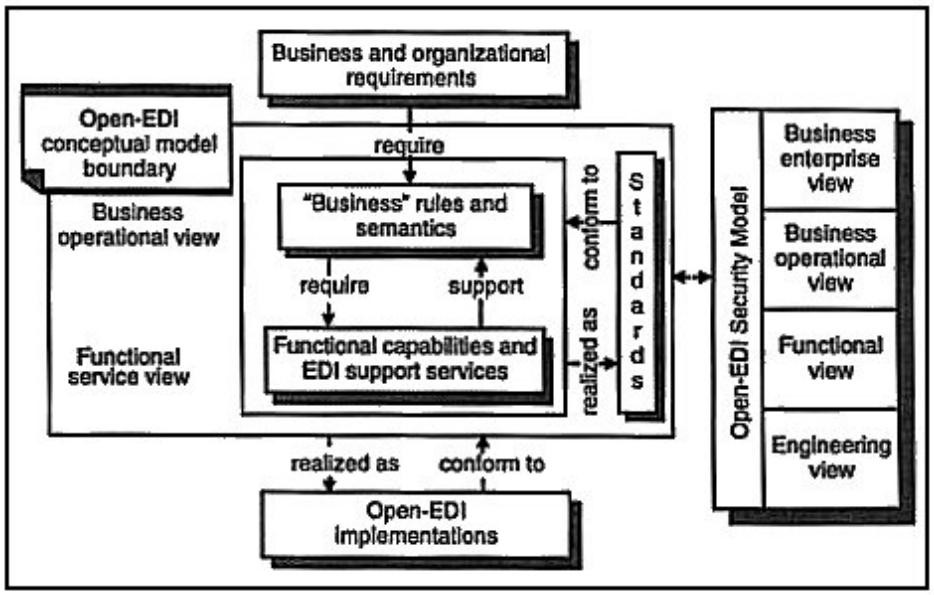

Figure 1. Security and Open-EDI.

The various views in the security model reflect a different aspect and definition of security. Figure 2 illustrates this security model in more detail, reflecting this progressive flow of security definition and specification of business requirements.

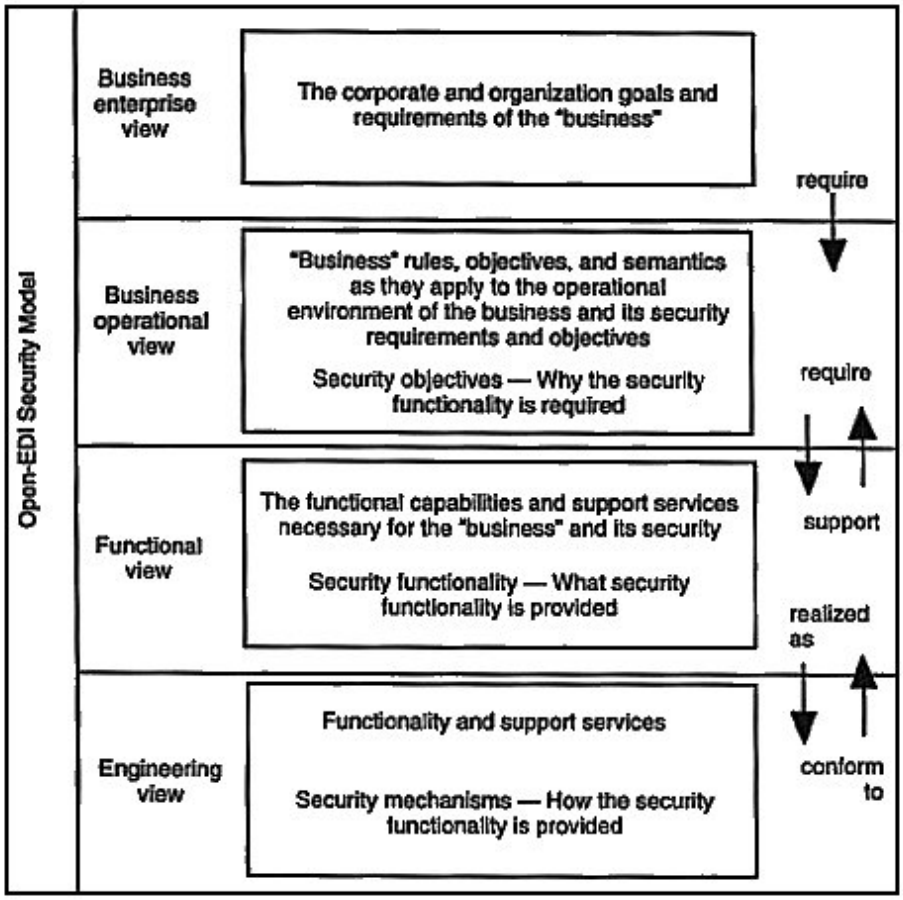

Figure 2. Open-EDI Security Model.

At the highest level, the enterprise view, security is expressed in terms of corporate policy and overall business strategy. At the next level down, such business policy and strategy are expressed in terms of specific security objectives as reflected in the operational environment in which the business is placed and operates.

At the functional level, the security objectives of the business are then specified in terms of a set of security functions to support the operational requirements for security. Finally, at the last level, the security functions are realized in terms of security mechanisms implemented in systems, products, and services. This model recognizes the need to be able to support a "complete" business activity and its security requirements — that is, a business activity involving several parties and numerous interlinked EDI transactions reflecting real-world activities.

Open-EDI is driven by electronic integration among enterprises and requires both simple and complex security solutions, depending on the nature of the business and the needs of different business scenarios [HUMP92b].

EDI security requirements

The SOGITS Report [SOGI89] considered the needs of users and suppliers of EDI-based systems across a wide range of applications, including corporate trading systems, financial systems, import/export systems, cargo handling systems, computer-aided acquisition and logistics (CALS), CAD/CAM (computer-aided design/computer-aided manufacturing), procurement and stores, and so on. IT and communications systems that are associated with the use of EDI will have a wide range of security requirements commensurate with the nature and value of the business using the system. These requirements can range from very broad, in the case of a sensitive commercial business exchange (where the integrity, confidentiality, and availability of the EDI information being exchanged are critical to the business mission), to a more basic form of requirement, which might be the data integrity of a regular shipment order.

Users of EDI trading systems include government departments (for example, Custom and Excise), manufacturing industries (including the car industry, aerospace industry, chemical industry, and electronics industry), finance, and insurance. In most areas of application, the three major risks to EDI messages are:

- loss of integrity (that is, alteration, modification, or destruction), for example, important for payment services; sensitive information (including medical records and personnel records); critical processes; commercial designs, specifications, and manufacturing processes (for example, in the case of CAD/CAM);
- loss of confidentiality (that is, copied, seen, or heard by unauthorized persons), for example, important for sensitive information (including medical records and personnel records) and for intellectual property, commercial designs, specifications, and manufacturing processes (for example, in CAD/CAM); and

- nonavailability (that is, not accessible when needed), for example, important for "just-in-time" situations and for 24-hour trading, production automation, critical processes, and so on.

There are many customer benefits and demands for EDI. As a result, there is a growing demand for a set of commercially reasonable security solutions. Priority must be given to a standardized approach to EDI security if the long-term benefits of EDI to the business environment are to be achieved.

The current trend to obtaining the more substantive business opportunities through the use of EDI will be through a standardized approach leading to a secure Open-EDI environment.

The essence of EDI messaging security

One must assume that EDI may be used across a wide-ranging messaging continuum covering different types of network services and various value-added application platforms. This range of communications provision will reflect a need for different levels and types of security to protect these EDI messages. The EDI components chain and the emerging EDI enabling technologies to support this chain are migrating the proprietary/direct-link type of offering to the Open-EDI approach based on international standards.

EDI security appears at several interrelated stages of system technology:

- the user/application interface,
- EDI applications and value-added services,
- the processing (both batch and interactive) and storage of EDI messages, and
- the communication of these messages in an open systems environment.

The basic security objectives that may need to be met at each stage are those of authentication and integrity, nonrepudiation, access control, availability, audit, and accountability. These objectives will need to be satisfied by both logical and legal controls and procedures, which are supported by a range of technologies, tools, and standards.

Current assertions about the security of EDI messages being handled at and between these various stages are often based on a level of "trust" in the increasingly complex systems that handle such messages, and the rules of engagement agreed to between messaging partners. It is therefore imperative that both the logical and legal aspects of EDI security are dealt with hand in hand. These two aspects of EDI security need to work with each other to provide the right levels of overall trust and protection

to EDI messages and interchanges. The rest of this essay looks at secure messaging for EDI.

Secure messaging standards

The standards industry has tackled many aspects of EDI security. In particular, the most important work in this area concerns EDI messaging based on the use of International Message Handling Standards [CCIT88a], [CCIT90]. The scope of this work covers secure message transfer, which provides the benefits of secure messaging to a wide range of distributed applications such as EDI.

Protection in an EDI messaging environment is essentially concerned with the nonrepudiable submission, delivery, and receipt of messages in a way that preserves the integrity, confidentiality, and availability of the messages being communicated. The current messaging standards provide the means of applying security mechanisms to meet different types of security objectives and levels of security. A brief introduction to the most important standards in this area follows.

X.400 message handling systems (1988)

CCITT, in its 1988 version of the X.400 recommendations for message handling (and the corresponding ISO 10021 equivalent standard), has made major extensions to the Message Transfer System (MTS) to provide for secure messaging [CCIT88a].

The 1988 X.400 standard allows the provision of different types and levels of security service independent of the type of message being transferred. Applying security mechanisms to the MTS ensures that the benefits of secure messaging are obtained independent of the content type of the message. For some content types, additional security mechanisms may be defined in the content-type protocol. The security specified in this standard thus provides for secure message transfer services and distributed interworking in support of applications such as electronic mail and EDI, as illustrated in Figure 3.

The security model used to specify the security features of the 1988 standard is based on a threat assessment of an assumed messaging environment. This assessment considers the main threats to be associated with the unauthorized access to the messaging system, threats to the message itself, and intramessage threats. Table 1 shows an example threat/security service scenario that might be covered by this model.

This table of threats and services is an indicative example rather than a definitive list. The designer of a secure messaging system would need to determine which threats are actually present and applicable to the messaging environment under consideration and which of these can be countered by the X.400 security services available. In essence, the de-

signer will need to develop a technical security policy for the messaging environment.

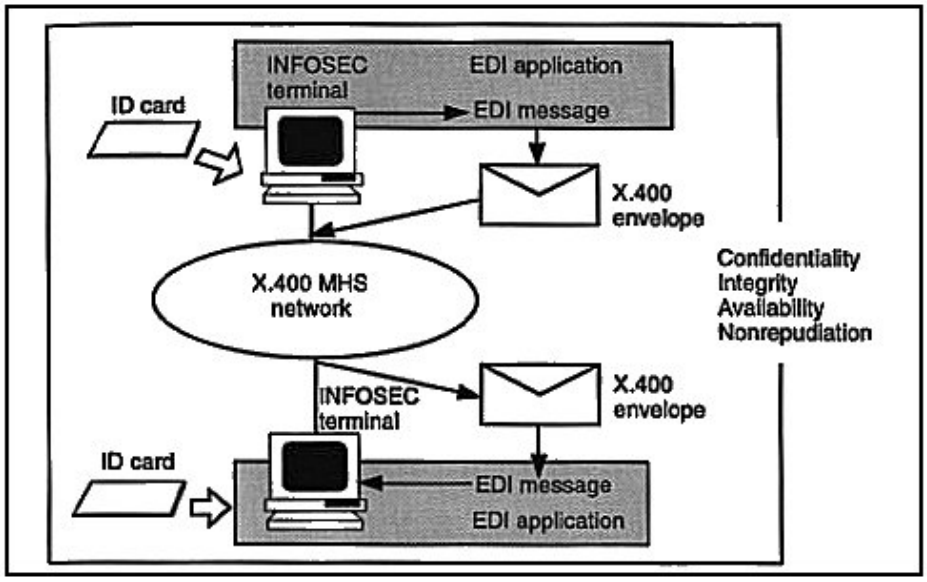

Figure 3. Secure EDI and X.400.

Table 1. Threats and services.

Threat	Examples	Security Services
Masquerade	Impersonation, false claims/acknowledgments	Authentication
Unauthorized message modification	Modify, delete, destroy messages	Integrity
Repudiation	Denial of origin, submission, or delivery of a message	Nonrepudiation
Leakage of information	Unauthorized release of message contents	Confidentiality

The security services defined in X.400 provide the link between the security requirements and objectives as described in a security policy, and the security mechanisms (for example, digital signatures) and management controls (for example, for the management of public keys) to satisfy these requirements. The 1988 X.400 recommendations specify the following security services:

- Authentication. Message origin authentication, peer entity authentication, probe/report origin authentication, proof of submission, and proof of delivery.
- Integrity. Connection, content, and message sequence integrity.
- Nonrepudiation. Nonrepudiation of delivery, of origin, and of submission.
- Confidentiality. Connection, content, and message flow confidentiality.
- Security content.
- Message security labeling.

Each of these security services can be implemented by one or more types of security mechanism, to satisfy the requirements of many different messaging applications needing different levels of security. In implementing these security measures and controls, the level of assurance at which these must be applied and maintained will need to be considered. In the case concerning the use of cryptographic mechanisms, it might be a question of the strength of mechanism and the mode of operation being used.

X.435 EDI messaging (1992)

Since the introduction of the 1988 X.400 standard, CCITT has been working on a series of recommendations, referred to as the X.435 series for secure EDI messaging. X.435 will use the X.400 security mechanisms in addition to some EDI-specific security measures not defined in the X.400 standard.

This standard will thus provide a security messaging capability for EDI applications, supporting the use of a range of EDI message formats currently being standardized, such as EDI for Administration, Commerce, and Trade (EDIFACT), American National Standards Institute ANSI/X12, and United Nations Trade Document 1 (UN/TD 1).

The basic security features being progressed by the X.435 EDI messaging standards work, in addition to the 1988 X.400 security features, include the following:

- *EDI Messaging (EDIM) responsibility authentication.* Proof of transfer, retrieval, and EDI notification.

- *Nonrepudiation of EDIM responsibility.* EDI notification, retrieval, transfer, and content.

In addition, work has started on:

- message store extensions (including control of delivery, user security management, and audit),
- message transfer audit, and
- other enhanced security management controls.

Figure 4 illustrates the concepts relating to the proof services offered by X.400 and X.435.

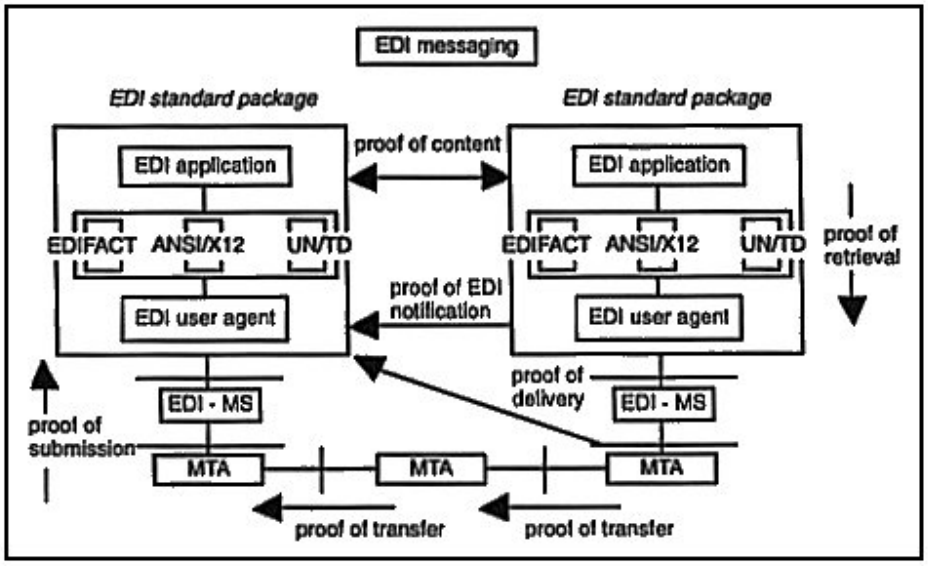

Figure 4. EDI security and proofs. The solid lines perpendicular to flow lines indicate EDIM responsibility transfer boundaries. MTA: message transfer agent; MS: message store.

The practical realization of this might typically be a standard EDI software package containing EDI application software, various format options (for example, EDIFACT), and an EDI user agent. The standard package could be modified to incorporate the necessary security controls to provide the capability of implementing a number of proof services, and possibly other services. In addition, security could be offered at the mes-

sage transfer level via the message transfer agents to provide a secure transfer medium.

X.500 directory systems (1988)

CCITT and ISO/IEC incorporated into their 1988 X.500 series of directory system standards [CCIT88c] an "Authentication Framework" (X.509) that defines mechanisms and protocols for entity authentication. These mechanisms are based on the use of public key technology, digital signatures, and the introduction of various public key elements such as certificates and tokens. Other publications [ANSI92a, b] are applicable to the financial sector.

The X.509 standard also introduces the concept of a Certification Authority (CA) through which users are identified, registered, and then issued their public key certificate(s). The use and application of the X.509 certificates and the concept of Certification Authorities (CAs) are a natural complement to the distributed nature of the X.500 directory system approach and to the provision of publicly available information services. It can be shown that this natural duality also holds between the X.509 technology and the provision of a number of EDI security features. The X.509 standard when implemented will constitute a secure naming and routing process in a multidomain messaging environment. In addition, a number of the security services specified in X.400 can be implemented using the X.509 technology (certificate, token, and digital signature). These security services include user identification, content integrity, and various nonrepudiation/proof services, for example, proof of delivery.

X.509 technology can provide a distributed use of authentication, thus allowing secure distributed processing of EDI transactions and greater security of trading partner connectivity. Although the X.509 technology is not the only solution to the provision and implementation of X.400 and consequently EDI security, it is certainly one of the most effective and the most practical. The distributed nature of messaging and in particular EDI messaging makes the X.509 technology a natural partner for secure trading across distributed environments. Figure 5 shows the future EDI use of the X.500 directory system.

The X.509 technology is able to play a major part in the realization of a number of these services, in particular, the provision of nonrepudiation services, the responsibility authentication options, and the various authentication and integrity services. However, other methods for providing these services are also available; these include the use of symmetric encipherment techniques, message authentication codes (MACs), and manipulation detection codes (MDCs). The work of ISO/IEC JTC1/SC27 "Security Techniques" and ANSI X12 in this area provides some excellent examples.

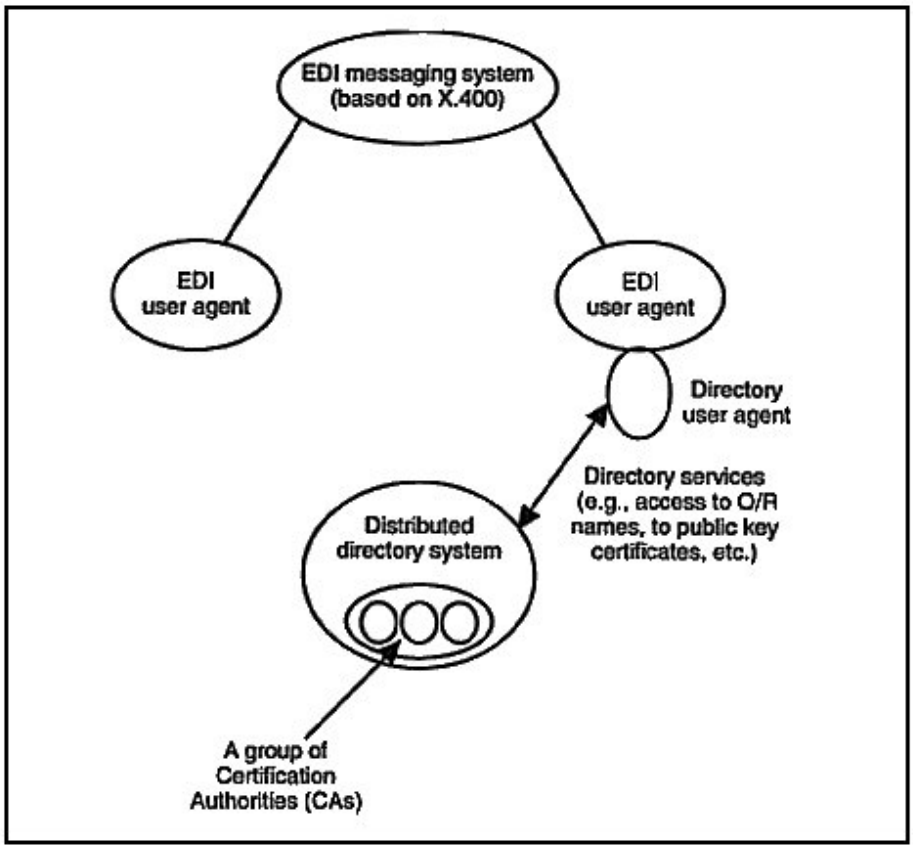

Figure 5. X.500 and EDI security (O/R: organizational/residential).

Nonrepudiation, responsibility, and proof

One of the important features of EDI messaging is that of nonrepudiation, which provides some level of proof or evidence that an EDI message has been sent or has been delivered. For example, nonrepudiation of delivery provides the originator of the message with proof that a message has been delivered, and this proof should hold up against any attempt by the recipient(s) to deny receiving the message or its content.

Both the X.400 and X.435 standards allow for a number of different elements of service to be available in order to provide a wide range of non-

repudiation services. Some of the important elements of nonrepudiation are shown in Figure 6.

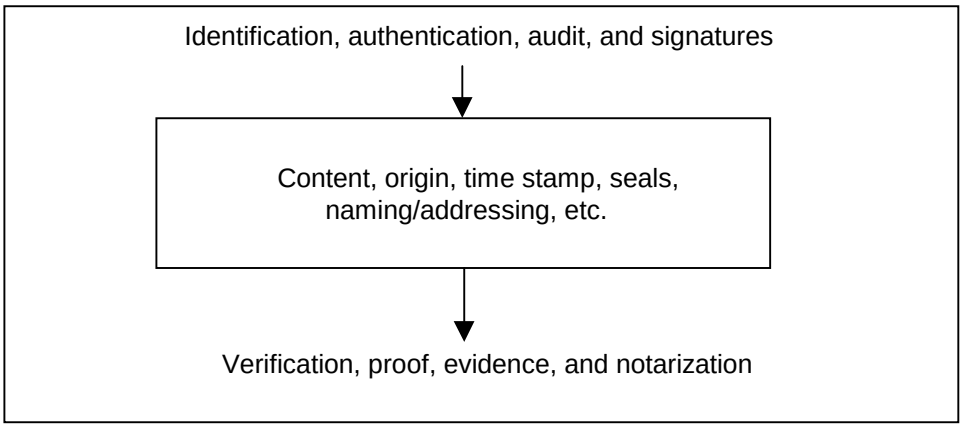

Figure 6. EDI and nonrepudiation.

Current standards [CCIT88a] introduce the concept of a "responsibility transfer boundary" and provide specification for the provision of several "responsibility" security services. The basic idea behind this concept is to transfer responsibility of certain aspects of a message, as it passes from one component of the EDI messaging systems to another component.

For example, after transferring an EDI message through the network of message transfer agents into the EDI message store (EDI-MS), the end system EDI user agent will at some point in time retrieve this message from the EDI-MS. By providing a proof of retrieval message, responsibility for that message now rests with the EDI user agent [SC2792].

Other security standards work

There are a number of other activities of relevance and support to the provision of secure EDI messaging [ITAE92b].

ISO/IEC JTC1/WG3 Open-EDI. WG3 is responsible for the coordination and development of Open-EDI standards. WG3 provides a coordination function across JTC1 and is also involved in liaison and collaboration with most of the major groups outside JTC1 that are also active in EDI work.

ISO/IEC JTC1/SC21 OSI Architecture, Management and Upper Layers. SC21 is involved in a number security projects related to OSI

and open systems. In particular, with respect to EDI, it is involved in the development of a nonrepudiation framework and X.500 directory security.

ISO/IEC JTC1/SC27 Security Techniques. SC27 is responsible for the development of a wide range of security techniques for information processing systems. These techniques include digital signatures, data integrity techniques, authentication mechanisms, and nonrepudiation techniques. SC27/WG1 is particularly interested in the requirements and development of security services for Open-EDI based systems.

ANSI. ANSI X.12 has been considering several areas of EDI security, in particular, covering work on management of transaction sets, security structures, and key management.

This work includes:

- X12.58 "Draft Standard for the Trial Use for Managing EDI Security Structures,"
- X12.42 "Draft Standard for the Trial Use of Managing EDI Cryptographic Service Message Transaction Sets," and
- "Guideline for Implementing X12.42 and X12.58."

This work uses other ANSI standards, such as X.9.9 on MACs (Message Authentication Codes), X.3.92 (Data Encryption Algorithm), and X.9.17 (Key Management Using Symmetric Key Techniques).

ANSI is also working on the following two sets of signature standards for the financial services industry:

- X9.30-199X:
  Part 1: The Digital Signature Algorithm (DSA)
  Part 2: The Secure Hash Algorithm (SHA)
  Part 3: Certificate Management for DSA
  Part 4: Management of Symmetric Algorithm Keys Using Irreversible Cryptography

- X9.31-199X:
  Part 1: The RSA Signature Algorithm
  Part 2: Hash Algorithms
  Part 3: Certificate Management for RSA
  Part 4: Management of Symmetric Algorithm Keys Using RSA

Public domain standards. There are a number of de facto standards [RSAD91] for public key techniques, some of them based on X.509, which are applicable to the implementation of secure EDI messaging. These standards include the following:

- PKCS No. 1 “RSA Standard,”
- PKCS No. 6 “Extended-Certificate Syntax Standard,”
- PKCS No. 7 “Cryptographic Message Syntax Standard,” and
- PKCS No. 8 “Private Key Information Syntax Standard.”

EDIFACT Security Framework. The Western Europe EDIFACT Board (WE/EB) has a Security Group MD4.B that has developed a Security Framework for EDIFACT. This framework considers end-to-end security requirements for EDI systems for use in interchanges between corporations and banks.

The approach taken in this framework is one of combining existing standards and implementations specifically for EDIFACT interchanges, and is closely aligned with the ANSI X.12.58. It also uses some of the X.509 technology (the Directory Systems Authentication Framework), in particular, for key management.

TEDIS. The European initiative TEDIS (Trade EDI Systems) is a program of work sponsored by the European Commission. This program looks at three aspects of EDI systems: telecommunications, security, and legal. The aim of TEDIS security is to protect the EDI message itself and to stimulate the definition, development, and adoption of technical standards to ensure the security of EDI messages in a multicompany environment. A secondary aim of the TEDIS program is to coordinate the development of procedures and methods specific to the management auditing and control that are linked to the establishment and use of a secure EDI system.

The TEDIS program has been considering an EDI Agreement Model, which also includes security as a conditional feature. One of the results of TEDIS was the development of a report on Digital Signatures for EDIFACT, which is currently being considered by the UN/EDIFACT Working Group and by SC27. Another result is a report on Trusted Third Party Services [TEDI91].

Summary

This essay has mainly concentrated on X.400, X.435, and X.500 standards, and their use in EDI messaging. The X.400 technology provides a basis upon which secure trading systems can be developed which would satisfy a high percentage of the market requirements, in particular, for international trade and wide-area regional trade.

It is probably one of the most significant steps in achieving a secure Open-EDI environment. However, this is just part of the solution, albeit a very important part. There are still issues to be dealt with in providing secure distributed systems technology in such a way that all barriers (for

example, technical, administrative, and international) are removed to allow the introduction of a fully integrated Open-EDI environment.

This standards-driven technology cuts across many multidisciplined areas: from work on CAEs (common application environments), open systems management, and distributed applications to work on techniques, services, and protocol building. It is a standards technology that is targeted toward the future integration of the current set of services and applications, together with the introduction of additional ones to meet the future needs of a wide range of distributed business environments.

This essay has considered some of the aspects of international security standards as they apply to the provision of secure EDI messaging. In particular, the use of the 1988 X.400 message handling system standards has been the basis for this overview.

The X.400 1988 standard, together with the X.500 directory systems standard and the X.435 EDI messaging standard, form an internationally agreed upon basis of future secure EDI technology and secure EDI messaging environments.

Other EDI-related security standards that are of relevance and support include:

1. the work of ANSI X.12 on EDI security structures [ANSI91a-c],
2. the WE/EB EDIFACT group on security,
3. the European TEDIS program, and
4. ISO/IEC JTC1/SC27 on security techniques, for example, digital signatures and authentication mechanisms, and the requirements for security.

Conclusions

There is no doubt that the growing trend toward open systems will see an ever-increasing requirement to achieve the right levels of business confidence and assurance in these systems [SOGI89, HUMP90a, BLAT90]. EDI is the growing business technology of the 1990s. It is a key change dynamic to business development. It is the baseline for improving business performance and efficiency, building new markets, and expanding old ones — and it allows the introduction of new business opportunities. It is a technology that has support from government, industry, finance, and commerce.

The SOGITS Report [SOGI89] confirmed the business need for EDI security. It identified EDI as the most important and demanding use of open networks and through an extensive survey reinforced the need for a standards program addressing several key areas of technical work.

This report provides valuable insight into the practical needs of users for trading system security. It identifies not only the need for technical

and quality standards for EDI security but also the need for urgent consideration to be given to the legal aspects of these electronic solutions. It emphasizes the need for work on practical standards for EDI security, third-party services (directories, notaries, and so on), messaging gateways for multidomain communications, techniques for nonrepudiation, audit, and authentication — and the need for additional legislation.

There is a growing need for "interconnectivity platforms" using the concept of "one-stop shopping" to enable users to deal with only one business intermediary rather than a complex network of them.

The long-term EDI architecture will be based on international standards technology offered by X.400 (1988 and 1992) and X.500. It should provide a common messaging technology package to support different applications and future additional tailored services. It should also support a range of security policies and the provision of security for different application needs and at different levels of protection. In addition, it will need to aim to complement the X12 and EDIFACT work.

This architecture, based on internationally agreed upon standards, will provide the business platform and connectivity for future secure distributed trading.

Related work

There is also work going on considering APIs (application programming interfaces) for EDI messaging (for example, X/Open) and for generic security services (for example, Trusted Systems Interoperability Group TSIG). In addition, there is work going on in other areas of the open systems security standardization program that potentially supports the introduction of secure end-to-end EDI solutions (SC21 work, ECMA work, and so on).

There are also other groups in Europe considering other types of solutions for EDI security (for example, based on the use of FTAM) and mixed solutions (for example, the French ETEBAC 5 system, which uses ANSI and ISO/CCITT X.509 solutions). Some consideration is being given to the development of solutions for interactive EDI (for which there is a growing market).