Security and EDI

Autor(en): **Greevy, Orla**

Objekttyp: **Article**

Zeitschrift: **Technische Mitteilungen / Schweizerische Post-, Telefon- und Telegrafenbetriebe = Bulletin technique / Entreprise des postes, téléphones et télégraphes suisses = Bollettino tecnico / Azienda delle poste, dei telefoni e dei telegrafi svizzeri**

Band (Jahr): **72 (1994)**

Heft 2

PDF erstellt am: **11.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-874698

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Security and EDI

Orla GREEVY, Berne

1 Abstract

The increasing use of Electronic Data Interchange (EDI) in the marketplace has highlighted many aspects of existing commercial and legal practice which require adaptation. Likewise, the business world enforces its requirements on EDI, expecting it to offer the same level of confidence to its users as the paper system it is replacing. Many EDI systems in operation today are considered as closed systems. They are based on proprietary protocols and various message syntax standards, which have been developed to meet specific national and business requirements. These EDI systems are referred to as closed EDI systems and do not reflect the need for open trading between business sectors. The establishment of an 'open' EDI service is being promoted at international level. This trend emphasizes the need for a standardized, coherent approach to security within EDI. Security is a crucial component contributing to the success and expansion of an 'open' EDI service. Common security procedures and tools based on international standards and tailored to the commercial environment are vital if open EDI is to become reality in the business world.

The security requirements of EDI have influenced and accelerated the efforts of the international standards organizations such as CCITT and ISO in defining security services for open systems. Although the OSI standards for security limit the field of scope to the communications aspects of the EDI service, they identify security threats and countermeasures in the form of security mechanisms and functions which can be applied to the entire EDI system.

Due to the diversity of business applications requiring the EDI service, a standard security framework must be defined. This should be flexible enough to enable security policies specifying varying degrees of security to be enforced. Security policies reflect the sensitivity of the data involved in an EDI transaction. They also address the concept of security for the entire EDI service. Recognized international-level security policies are intended to satisfy legal requirements of international commercial trading being conducted over EDI.

As existing EDI systems are currently well established, the transition to EDI systems based on OSI standards will not be immediate. During the transitory phase, existing EDI service providers could enhance their existing EDI services with security functionality. Based on their experience, they could also play an important role in defining internationally acceptable security policies for EDI.

2 Introduction

Security is a major concern in information processing. Generally, security refers to a system of procedural, logical and physical measures aimed at prevention, detection and correction of certain types of misuse, together with the tools to install, operate and maintain these measures [18]. Due to the nature of the data involved in EDI, the security and confidentiality of an EDI service is a fundamental requirement.

The security of an EDI service may be discussed at two distinct, but closely related levels. At the abstract level, the security requirements for EDI are considered from the point of view of the legal and commercial world. This includes aspects such as the definition of trading agreements, which specify the degree of security required for legal acceptability. At a more detailed level, the possibilities for incorporating security features in a typical EDI system and its component parts are considered. The components of an EDI service include the application at an end system, the messaging syntax used to represent the trade data, and the communications network involved in the transmission.

The adoption of OSI standards for EDI will facilitate the overall requirement to provide a standardized approach to security for the EDI service. The OSI standards provide the framework for defining internationally acceptable methods of counteracting threats to security within EDI communications, and thus present electronic alternatives to the existing manual checks present in the paper-driven trading system. However, the need for defining standard security policies for the EDI service which extend beyond the communications aspects and which incorporate all aspects of the EDI service must be addressed.

In order to achieve a standard approach to security within EDI, it is necessary to define a means to provide standard security functions which act as generic building blocks to meet a wide range of security requirements. In recent years, efforts have been made at an international level to define an EDI service for open systems. As EDI is involved with message passing between distinct, geographically distributed applications, it has been recognized as an ideal layer-7 application, in ac-

cordance with the OSI reference model. The CCITT X.435 and F.435 recommendations published in 1990 define protocols and service elements specifically for the transmission of EDI messages in open systems [9, 10]. It is therefore appropriate to review the security services and mechanisms defined by the OSI standards, in particular those outlined in the X.800 recommendation [3]. The security requirements and service elements specific to EDI messaging as defined by the X.435 and F.435 recommendations are dealt with here.

A standard approach to security should accommodate the possibility to define varying security levels. Not all EDI applications require the high level of security as banking applications involved in the transmission of funds. Providing an application with unnecessary security increases the cost of data transfer and decreases its efficiency. This emphasizes the requirement for the definition of a security policy which consists of a set of rules, outlining the procedures and mechanisms to maintain the security of the system. Security policies should reflect the fact that the security requirements of a specific EDI application can vary, depending on the sensitivity of data involved.

Another important consideration is that the migration to OSI-based EDI systems will not be immediate. In the transition period, the EDI service will consist of a number of interconnected heterogeneous systems based on either proprietary or standardized protocols. The provision of standard security procedures under these circumstances could prove to be complicated. Standard security policies for EDI can, however, be defined independent of the underlying system. The VADS (value-added and data services) companies, who generally provide the EDI services in operation today, could extend their services to offer customers security features required by the commercial world. They could also play a deciding role in the definition of security policies when drawing up trading agreements between EDI partners. In addition, due to their neutral position in an EDI trading agreement, they could provide an audit service of EDI transactions, which is a basic legal requirement.

Security functionality may be provided as an embedded feature of the EDI service and also by distinct applications known as security support applications. These provide the necessary facilities to achieve a secure EDI service. It is desirable that such applications adhere to international standards. A typical supportive application would be a distributed directory service, which maintains a variety of information, including security attributes. The Directory Service, as defined in the CCITT X.500 recommendations, is examined briefly, to consider its ability to provide the necessary information and infrastructure to support and manage a secure EDI service.

3 *The Legal Requirements of an EDI Service*

The legal requirements for a secure EDI service identify many of the issues which must be addressed when defining security policies. The importance of security commercially has been a major driving force in promoting the work of the international standards bodies in the field of security. The CCITT X.400 recommendations, which were first published in 1984, did not include a definition of security features. The lack of security for X.400 messaging is considered unacceptable, if it is to provide the basis for commercial messaging applications such as EDI. This situation has been remedied, as the X.400 1988 standards have been extended and now identify security functionality for the Message Handling System (MHS). In addition, the increasing use of EDI has challenged the legal and commercial world to adapt and standardize their procedures to encompass electronic trading. At present, legal requirements for business and trade can vary from country to country. As EDI trading extends beyond national borders, it requires an international set of laws which outline the security measures necessary for electronic trading.

At the request of the European Commission, the International Chamber of Commerce (ICC), working through a joint committee which includes representatives of major intergovernmental and nongovernmental international organizations, has now produced a set of uniform rules of conduct for the interchange of trade data by teletransmission (UNICD). UNICD facilitates the use of EDI through a code of conduct accepted by the parties engaged in electronic interchange. The UNICD rules have been adopted by the United Nations Economic Commission for Europe and provide a basis for establishing acceptable business practices. While these rules form a useful basis, the TEDIS program is looking at the need for a model interchange agreement which trading partners can accept as a legal basis for their EDI implementation.

The basic legal requirements for EDI are the same as those of the paper system being replaced. The EDI service is required to reproduce the checks and customary controls that currently exist for manual systems. Such checks include:

- a contract of agreement between trading partners
- authentication of sender
- nonrepudiation of sender and receipt
- confidentiality of the EDI transaction
- logging and storing of data for audit by a third party

The legal acceptability of documents generated from electronically transmitted trade data must be established. Although EDI cannot transmit a hand-written signature, the service has the ability to incorporate mechanisms to electronically authenticate the source of the data transmitted and its correctness. Confidence in electronic security mechanisms, provided in a standardized manner, will eliminate demands for paper documents and establish the acceptance of computer records.

31 *Responsibility and Liability*

The issues of responsibility and liability can be considered within the scope of a secure EDI system. Because of the use of networks and computers, liability for errors, malfunction of software and theft or fraudulent use of data is uncertain. At present it is not defined to what extent a network operator or software producer would

be liable for loss of trading data or EDI service. As enterprises increase their reliance on EDI, it will become essential to define standards which include these issues within the scope of EDI transactions.

32 Auditing Electronic Transactions

Auditing of commercial transactions between companies is standard legal practice. This requires that sufficient details of EDI transactions be retained in electronic form to enable an audit to be carried out. International acceptance of such an audit demands the development of standards, stipulating what information must be retained for audit.

An audit trail logs activity in computer systems for management control purposes, but could also be used by auditors to verify figures in the accounts. The EDI transactions, which are now electronically represented, must be validated for their integrity by a third-party notarization company.

4 Standardization for Security and Open-EDI

The term Open-EDI is used to describe a globally accessible EDI service based on OSI standards. Commercial trading and legal requirements, outlined previously, require that standardization for a secure EDI service include many aspects which are considered beyond the scope of OSI standards. The Report on the Open-EDI Conceptual Model [12] tackles this task by defining Open-EDI as the electronic data interchange among autonomous parties, using public standards and aiming towards interoperability over time, business sectors and information technology systems. This study suggests a means of instantiating the exchanges of information between parties according to detailed, well-defined data exchange agreements and protocols. Such agreements are intended to inherently define specifically the level of security required for a particular EDI transaction.

The need for the provision of security within EDI has also been approached within the European community. The TEDIS program, which is responsible for supporting European user groups and organizations concerned with EDI, emphasizes the need for adequate security provision within EDI systems. In early 1989, the Directorate General XIII of the Commission of European Communities published the results of an extensive study on the security requirements of EDI users as part of this program. This study identified the following security threats, which it considered directly applicable to an EDI service:

- loss of service
- disclosure of information
- unauthorized network access by insiders
- unauthorized network access by outsiders

The study also outlined the security features which would be necessary to protect against these threats:

- user authentication
- message integrity
- confirmation of end-to-end delivery
- message confidentiality
- network service operational security
- auditability of EDI transactions
- network service harmonized security levels
- nonrepudiable confirmation of delivery and receipt of EDI messages

In addition to this study, TEDIS hosted a workshop on EDI security with the aim of examining how these basic security requirements for EDI security could be met [1]. An important underlying aim was to focus the attention of security specialists on the new situation being brought about by the increased use of EDI in the commercial world. The experts recognized the need to define security levels for the range of message types that might be carried over widespread interconnected EDI networks. As a result of this workshop, a model defining varying levels of security and reflecting the requirements of a secure EDI service was proposed. Each security level corresponds to specific message categories and their associated risks. The service level, for example, is intended to define the quality of an EDI service based on the security features available at that level. The aim of this 'levelled approach' is to achieve a cost-effective and standardized solution for a secure EDI service.

5 An Overview of Security Threats

The following sections describe a number of general threats to the security of an EDI system. In general, threats to security can be classified as accidental or deliberate. While much of the concern over data security relates to deliberate infiltration, the accidental disclosure of information can be equally serious.

51 Disclosure of Information

Organizations maintain valuable information on their computer systems. This information may be used by other parties in such a way as to damage the interest of the organization owning the information. Therefore, information must be protected against disclosure to unauthorzied internal and external sources.

52 Contamination of Information

Valuable information being transmitted between EDI trading partners may become worthless if it is corrupted with unauthorized information. It is therefore necessary that the EDI service can guarantee the integrity of information within the system.

53 Unauthorized use of Resources

Access to the resources of the EDI service should be restricted to users and user applications that have been authorized. Misuse and unauthorized use of resources may lead to destruction, modification and loss of integrity of information.

54 Repudiation of Information Flow

Repudiation of information flow involves denial of transmission or receipt of messages. Since EDI messages can carry vital details of a business transaction such as purchasing agreements or instructions for payment, the system should make it impossible for an EDI user to repudiate the transmission or receipt of an EDI message.

55 Denial of Service

Because of the increasing reliance by organizations on EDI to perform trading, loss of service may have a significant negative affect. Therefore, detection and prevention of denial of service must be considered as part of any security policy.

6 Security Countermeasures

Security facilities and security mechanisms act to counter threats within the EDI service. The term 'security facility' refers to a set of logically associated security functions [18]. Security facilities can exist as an inherent part of the EDI system, or they can be provided by distinct applications known as security support applications. These applications offer security functionality in the form of security services to the EDI application.

There is no single countermeasure that completely eliminates a security threat. Certain countermeasures are more effective against specific threats than others. However, the existing security mechanisms provide a good deterrent to many possible deliberate attempts to infiltrate an EDI system.

61 Cryptographic Techniques

Cryptography underlies many security facilities. Cryptographic techniques provide a mechanism for encipherment and decipherment of EDI messages. The EDI message is encoded prior to transmission, so that if the information is intercepted, it is not immediately intelligible. On reception, the message is decoded into its original form. This ensures a level of confidentiality and integrity of the EDI message during transmission.

Cryptographic algorithms may be described as symmetric or asymmetric. A symmetric algorithm is based on the knowledge of a single key, which is used for both encipherment and decipherment of the data. An asymmetric algorithm uses one key, referred to as the 'secret key' to encode the data, and another key, referred to as a 'public key' to decode it.

Cryptographic techniques provide a basis for digital signatures and encryption. For the purpose of encryption, the encoding key is made publicly accessible, while the decoding key is kept secret. In this way, a partner involved with transmitting a message can encode the message using the intended recipient's public key. The secret key is used to decode the message; therefore, only the intended recipient who is the sole possessor of the secret key can interpret the message. In the case of digital signatures, the converse is true. The decoding key is made public, and the encoding key is secret. This enables the recipient of a message to decode the message and be sure of the originator. *Encryption has the effect of digital signature.*

Cryptographic techniques can be used to counteract the following security threats:

- message stream observation
- traffic analysis
- repudiation
- masquerade
- unauthorized connection
- modification of messages

The use of cryptographic techniques for secure EDI messaging implies the availability of a service which enables encryption and decryption of messages. In addition, a facility to generate, manage, store and distribute cryptographic keys securely is also required.

62 Digital Signature Mechanisms

The term digital signature is used to indicate a particular technique which can be used to provide security services such as nonrepudiation and authentication. Digital signatures require the use of asymmetric cryptographic algorithms as outlined in the previous section. The essential characteristic of a digital-signature mechanism is that a signed data unit can only be created by the holder of the private key. This means that the sender of a 'digitally signed' message cannot deny having sent the message; therefore, it can be used to counteract the threat of nonrepudiation. The verification of a signature can be used to prove to a third party that only the unique holder of the private key could have produced the signature.

63 Access Control Mechanisms

These mechanisms enforce a policy of limiting access to a resource to only those who are authorized to use the resource. Access control mechanisms are usually implemented by means of passwording and access control lists, which define the level of access to a specific resource. A given entity may authenticate its identity, and this information is used to determine the capabilities or rights of that entity. Access control policies can be enforced at the end system where the EDI application resides, so that access to EDI information is restricted to those who are authorized. Access control policies form an integral part on the overall security policy for the EDI service. Access control mechanisms are also appropriate within the communications system.

Access control mechanisms may be based on use of one or more of the following:

- access control information bases, where access rights of peer entities are maintained
- authorization centers which maintain access control information

64 Data Integrity Mechanisms

Data integrity mechanisms outline a means of corruption detection. They can be used to provide the integrity of a single data unit or field or the integrity of a stream

of data units. Determining the integrity of a single data unit involves two processes, one at the sending entity and one at the receiving entity. The sending entity appends a value which is a function of the data itself. The receiving entity generates the corresponding value and compares it with the received value to determine whether the data has been modified in transit. Integrity of a single data unit does not protect against the replay of a single unit.

Data integrity for a stream of data units can be implemented by means of sequence numbers, thus protecting the data against misordering, loss of information, replaying and modification of the data.

65 Authentication Exchange Mechanisms

Entities gaining access to a distributed system will be authenticated before being allowed to interact with other entities, subject to an access control policy [18]. The entities that are accessed must also be authentic. Systems supporting user authentication must ensure the integrity and confidentiality of the credentials involved. A standard means of exchanging authentication between entities and users of the EDI system information is required. Provision of a secure method for exchanging keys is beyond the scope of the X.400 standards [11].

Authentication mechanisms provide a means for an entity to identify itself to another entity before it can interact with it. Authentication is also necessary during data transfer of EDI messages, so the recipient of a message can be sure that the sender is indeed who he claims to be.

66 Notarization Mechanisms

The notariziation mechanism is based on the concept of a trusted third party (a notary), who is responsible in ensuring certain properties about the information exchanged between two entities, such as origin, its integrity, or the time it was sent or received. The incorporation of notarization mechanisms in the EDI service will enable it to provide audit information and thus satisfy the legal requirement for commercial trading.

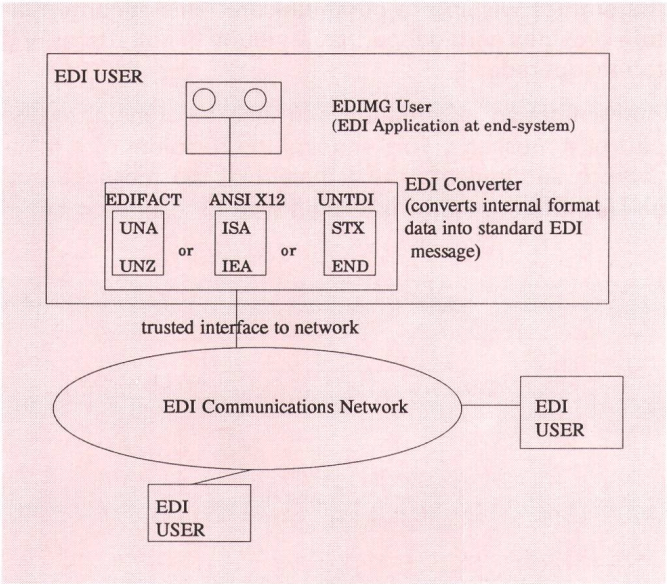

Fig. 1 Components of an EDI system

7 Security for EDI System Components

The following sections outline how the overall EDI system can be enhanced with security features based on the above-mentioned security mechanisms. The EDI system is decomposed into component elements *(fig. 1),* and each element is examined with the view to enhancing it with security functionality. The typical EDI system can be viewed as a distributed application consisting of the end system of an individual EDI trading partner, an EDI message syntax such as EDIFACT or ANSI X.12 which enables the coding interchanges according to predefined rules, EDI conversion and translation software which is responsible for the conversion of data from its internal representation at the end system to a predefined messaging syntax, and EDI communication software, such as that provided by the X.400 message-handling system environment.

71 End System Security

The OSI standards consider security of an end system involved in the EDI services as a local issue, as it does not affect the EDI-distributed application as a whole. However, if security is not guaranteed locally, then the measures adopted in the remainder of the system are irrelevant. The end system is considered as a trusted interface by the other elements of the distributed application. Standard security measures in the form of access control mechanisms can be incorporated into the end system, together with database security measures. Only then can the confidentiality and integrity of the system be guaranteed. *From the legal point of view, the security of the data maintained at the end system is just as important as when it is been transmitted over a network.* The requirement to prove the integrity of this data still exists. The overall security policy for the EDI service should satisfy legal and commercial requirements by specifying security mechanisms and a recognized standard security level enforced at the end system.

72 Security in EDI Message Standards

Message syntaxes used to encode EDI messages are defined independent of the communications network used to transmit these messages. Therefore, a secure EDI service can be provided by incorporating security features within the message syntax and would be applicable to both proprietary protocols and OSI *(fig. 2* and *3).* This discussion is based on EDIFACT message syntax, which has recently been endorsed by ISO [19] and has become the most widely accepted messaging standard for the exchange of data for EDI.

Protection of all or part of an EDI message can be included as an integral part of the information. Security information is being defined for EDIFACT and can occur within the message. This security information can be in

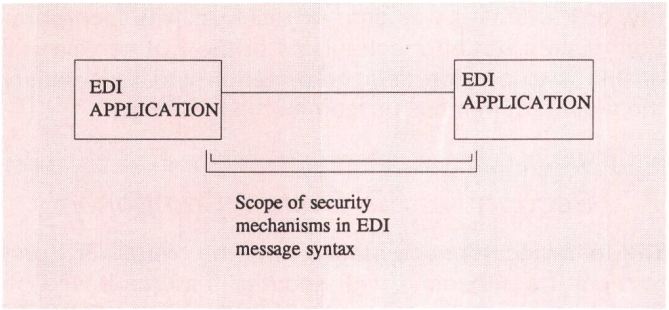

Fig. 2 The scope of security, when security is embedded in EDI message syntax

the form of a digital signature or integrity information. Thus it can provide a means to guarantee the integrity and authentication of the EDI message.

End-to-end security can be provided by means of an EDIFACT acknowledgement. The UNB interchange header segment of an EDIFACT message contains an acknowledgement request indicator, allowing the sender, A, to check if B, the recipient, has received and identified the start and end of an EDI message. B may perform detailed content verification. The interchange agreement can spell out the degree of checking which A can rely on when B sends back the acknowledgement.

The advantage in using security elements within the EDI message is that end-to-end security can be provided independent of the network being used to transmit the message. This has the obvious advantage in providing an interim solution to many EDI security problems, without having to wait for the EDI community to adopt the OSI-standard EDI systems.

73 Network Security

This discussion of network security concentrates on the security features defined in the OSI and CCITT standards document. The scope of network security is limited to providing security to messages while they are being transmitted or stored within the network component elements. The protocols used can include facilities to protect the data from network security threats such as nonrepudiation, eavesdropping and message integrity. Message authentication and encryption techniques are usually applied.

731 X.400 (88) Standards for Security in OSI

The X.400 (88) recommendations have been extended to define security features for messaging. These security features are provided by means of security services that counter potential threats to the Message Transfer Service (MTS). The security services are supported through use of the service elements in the MTS message envelope, referred to as the P1 envelope. The *Pedi* protocol for EDI messaging relies heavily on the service elements of the P1 envelope. Many of the security elements require encryption mechanisms.

A minimal knowledge of asymmetric public key encryption methods is required to understand how these security features are provided. A possible method used to provide message authentication and message integrity is described here *(fig. 4)*.

Originator

1. Apply a hash function to the content of the X.400 message. This reduces the number of bits of the X.400 message in such a way that all the original bits influence the outcome of the computation.
2. Encrypt the result of the hash function using asymmetric public key encryption by using the originators secret key.
3. Send the encrypted result of the hash function together with the message.

Recipient

1. Apply the hash function to the content of the message received.
2. Decrypt the encrypted result of the hash function, which was sent with the message using the originators public key.
3. Compare the results of the hashed X.400 message with the decrypted hashed message.

This method can be used to guarantee the integrity of the message and also to authenticate the originator of the message. It is also suitable to provide additional security features described in the following sections.

The security services defined by the CCITT recommendations are briefly described below.

The authentication service

The authentication requires authentication information comprising of locally stored information and data that is transferred to facilitate authentication.

Peer entitiy authentication is a service provided for use at the establishment of, or at any time during the data transfer phase of connection to confirm the identities of the entities wishing to communicate. This security feature provides confidence that an entity is not attempting to masquerade.

Authentication information can also be transmitted as part of a message. This enables the recipient of a message to authenticate the recipient of the message and be sure the originator is indeed who he claims to be.

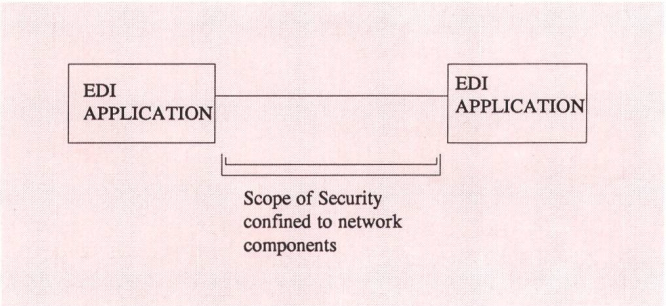

Fig. 3 Scope of security defined by OSI standards

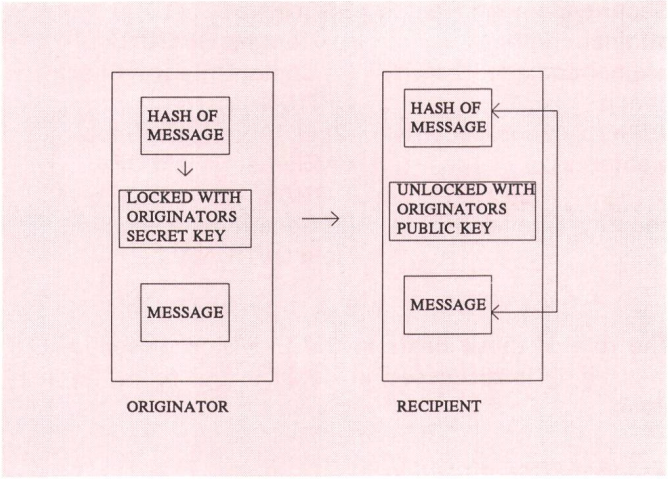

Fig. 4 Use of encryption for X.400 messages

The data integrity service

This service is used to guarantee the integrity of the data being transmitted between communicating entities. It ensures that the data are transmitted unalterd to the receiving entity. This feature is similar to the concept of a sealed envelope, which guarantees that the content has not been tampered with since being sent. It can be achieved by either symmetric or asymmetric encryption methods. Using the method described above, if the decrypted hash, which was sent with the message is identical to the hashed content, then this provides proof that the message has not been changed in any way, since no one but the originator could have created the encrypted result of the hash function.

Nonrepudiation service

This service is defined from two points of view:

- nonrepudiation with proof of origin of the data
- nonrepudiation with proof of delivery

The former protects against the threat that the sender could deny sending the data or any of its contents. The latter provides the sender of the data with proof of delivery. This will protect against any future attempts by the recipient to falsely deny receiving the data or its contents.

Confidentiality

This service can be provided by encrypting the message with the public key of the intended recipient. The message can then only be decrypted by the holder of the secret key.

732 EDI Security as defined by X.435

The CCITT X.435 and F.435 recommendations define a means of transmitting EDI messages in the MHS environment. The boundary between the EDI application and the EDI user agent (EDI-UA) is assumed by the standard documents to be trusted. That is, the security of the data being accessed by the EDI application is considered beyond the scope of the OSI recommendations.

The Pedi protocol provides security services as specified in the X.400 (88) standards such as authentication, message integrity, message confidentiality and confirmation of end-to-end delivery. Authentication can be incorporated in EDI messaging to prove that the message comes from the claimed originator whose name ('OR-Name') appears in the originator field of the message header. This facility is similar to the concept of a manual signature and is provided by using the original authentication features of the message transfer service [17].

Message integrity is an important feature of secure EDI service, as it proves that the message submitted by the originator has not been changed before it was received by the recipient. It can also be used by employing the asymmetric public key encryption techniques as previously described.

Message confidentiality is used to ensure that only the recipient of the message can read the contents of the message. Encryption techniques can also be used to achieve this.

The X.435 recommendations include definitions of requirements that are specific for EDI messaging, which are not adequately covered in existing message-handling system security services. An imporant aspect of the EDI environment, which is not recognized within the X.402 security mode, is the concept of EDI message responsibility. EDI message responsibility indicates whether the EDI message has been made available to its user by its EDI-UA. The security features available for EDI messaging are outlined in the following sections. Familiarization with the X.435 and F.435 recommendations is assumed.

The EDI message (EDIM)

The EDI message is contained in the P1 envelope transmitted to the message transfer service by the EDI user agent; therefore, it can make use of the security service elements defined for all X.400 messages *(fig. 5)*. In addition, security service elements are defined by X.435 as

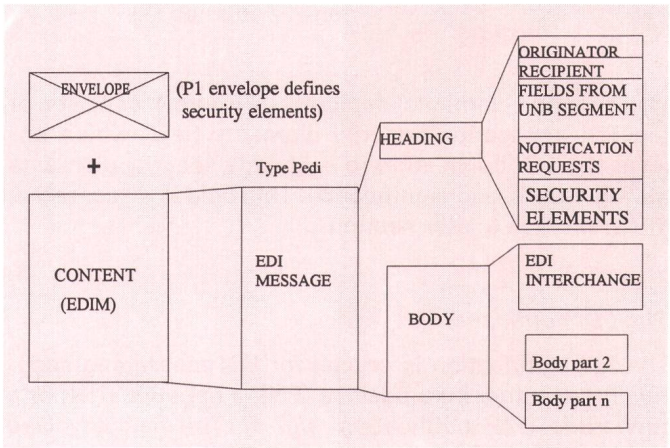

Fig. 5 The structure of X.400 messages containing EDI messages

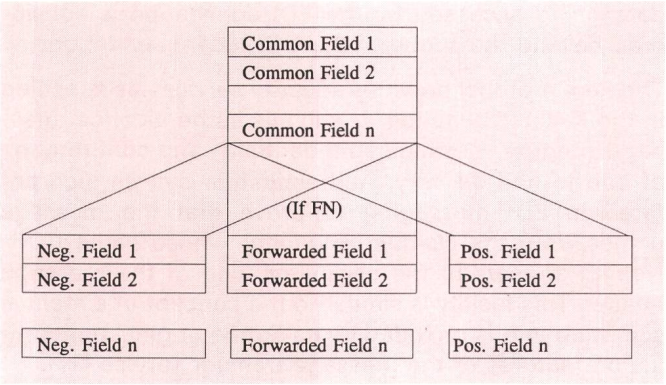

Fig. 6 The structure of the EDI notification

heading fields of the EDI message. These fields play a role in the provision of security features specific for a secure EDI service.

The EDI notification (EDIN) plays a significant role in the provision of security features. The EDI message heading field 'EDI Notification Request' can be used by the originator of a message to communicate his requirements for the generation of a notification to the recipient. This field consists of a sequence of three-bit strings, of which the first selects the type of notification requested, the second the type of security function applied to the notification, and the third may be used to make security requests for proof or nonrepudiation of reception of the EDI message.

The EDI notification requests field is defined in ASN.1 as follows:

```
EDINotificationRequestsField:: = SEQUENCE{
edi-notification-requests    [0] EDINotificationRe-
                                 quest,
edi-notification-security    [1] EDINotificationSecur-
                                 ity,
edi-reception-security       [2] EDIRecptionSecurity}
EDINotificationRequests::=BIT STRING{
                                 pn (0),
                                 nn (1),
                                 fn (2)}
EDINotificationSecurity::=BIT STRING{
                                 proof (0),
                                 non-repudiation (1)}
```

The security elements depicted in figure 4 consists of the EDI application security elements field, which enables the EDI application to exchange security elements having end-to-end significance. This field is discussed in more detail in a later section.

The EDI notification

The EDI notification is crucial for EDI messaging security. It can either be a positive (PN), a negative (NN) or a forwarded (FN) notification *(fig. 6)*. The field involved with security, the security elements field, is common to all three types of notifications. This field is defined in ASN.1 as follows:

```
SecurityElementsField::= SEQUENCE{
original-content          [0] Content OPTIONAL,
orginal-content-integrity- [1] ContentIntegrityCheck
check                     OPTIONAL,
edi-application-security- [2] EDIApplicationSecu-
elements                  rityElementsField OP-
                          TIONAL,
security-extensions       [3] SecurityExtensions-
                          Field OPTIONAL}
```

The role of these fields in the provision of secure EDI messaging is discussed in detail in the following sections.

Proof of EDI notification

This enables the recipient of an EDI message to create an EDI notification (EDIN) which can be used by the recipient of the EDIN as a means of authenticating the originator of the EDIN. This provides the means of confirming of end-to-end delivery of an EDI message between EDI user agents and can be used to counteract and detect the loss of the EDI service. The originator of a message requests an EDIN with authentication. The recipient of the message recognizes that it is required to generate an authenticated EDIN using the asymmetric public key encryption techniques. The originator can then verify the authenticity of the EDIN on receipt and therefore be sure that the recipient has received the EDI message.

Nonrepudiation of the EDIN

This provides the recipient of an EDIN with proof of its origin, which will protect against any attempt by the originator of the EDIN from falsely denying having sent it.

Proof of content received

This enables the originator of the EDI message (EDIM) to authenticate that the message content received by the recipient was the same as the message content originated by the originator. This facility is similar to the commercial practice of the recipient sending a photocopy of the trading document received [11]. The fields of the EDIN provide the mechanisms to request this facility.

The following steps are used to provide proof of content received:

Originator of EDIM:

a) Request an EDIN with authentication. This is achieved by setting the notification security field of the EDIN request field to the value 'proof'. In addition, apply a hash function to the content of the message, encrypt the result of the hash function and transmit it together with the message.

Recipient of the EDIM, originator of the EDIN:

b) If the received EDIM requests an EDIN with 'proof', use the authentication procedure to generate the EDIN. In addition, place the encrypted result of the hash function generated in a) above in the original content integrity check field of the EDIN.

Originator of the EDIM, recipient of the EDIN:

c) When the EDIN is received, use the verification procedures in order to prove the originator of the EDIN is indeed the originator indicated by the originator field in the EDIN.

In addition, verify that the encrypted result of the hash function generated in a) matches the value in the original content integrity check field of the EDIN.

Nonrepudiation of content originated

This provides the recipient of the EDIM with proof of the originated message content, which protects against any attempt by the originator to falsely deny originating the message content.

Nonrepudiation of content received

This provides the originator of the EDIM with proof that the message content received was the same as the message content originated. This proof will protect against any attempt by the recipient to falsely deny the content of the EDIM received.

Table I shows the provision and use of secure messaging elements of service by message-handling system components.

Table I. Elements of Service

Elements of Service	EDIM Originator	MTS	EDIM Recipient
Proof of EDI Notification	U	—	P
Non-repudiation of EDI Notification	U	—	P
Proof of Content Received	U	—	P
Non-repudiation of Content Originated	P	—	U
Non-repudiation of Content Received	U	—	P

Legend
P = a provider of the service
U = a user of the service

EDI application security elements

The EDI application security elements field of the EDIM heading and of the EDIN allow the EDI application to exchange security elements having end-to-end significance. The X.435 standard does not specify how these fields should be used.

One possible usage of the security elements field would be to provide authentication of the EDI application that created the EDI interchange. In this case a hash function would be applied to the EDI interchange and encrypted using the EDI application's secret key and placed in the security elements field of the EDIM. The recipient EDI application would apply the hash function to the received EDI interchange and decrypt and compare the contents of the security elements field using the public key of the originating EDI application. Clearly this field could also be used to guarantee end-to-end integrity of the EDI interchange.

8 *The Role of Value-Added Data Services (VADS) in Security*

The EDI service providers, generally referred to as VADS companies, are in an ideal position to extend their existing EDI services to incorporate security features, thus satisfying the legal and commercial requirements previously outlined. Due to their practical experience and established position in the EDI market, they could become the focal point for the definition of security policies and standard communications agreements between EDI trading partners. This would also satisfy a legal requirement to involve an independent third party in EDI business transactions.

These companies could assume the role of security administrators within an EDI system. A security administrator is an authority responsible for implementing a given security policy and the management of security information [18]. They would therefore assume responsibility for the EDI interchange within the scope of the network service they were providing. Security administration involves, on the one hand, the gathering of information about the EDI system. This information could provide the basis for an audit of EDI transactions. On the other hand, the security administrator is responsible for the entering and maintaining security information on the entities and users of the EDI system such as identities, credentials, access rights, cryptographic keys, etc.

The VADS security administrator of one specific closed EDI system could cooperate with security administrators of other EDI systems to ensure that a specific level of security is maintained when interworking is required.

VADS could also provide security-supportive applications necessary to enhance the EDI service with security. A security-supportive application is a specific type of application that provides security service at application level rather than being embedded in the communications architecture [18]. VADS could provide directory services to its EDI customers, which maintain information on location of other EDI users and their associated attributes and security information.

Scope for extension of the services of VADS companies exist in the provision of the following services, which would indeed be recognized by their customers as true added value:

- naming and registration of users
- digital signatures
- notary services
- encryption and key issue management
- service levels
- gateway conversion between networks
- confirmation of sending and delivering
- logging and tracing of messages
- use of external audit

– security segments in messages
– responsibility and liability

9 The Role of X.500 in EDI Security

This section briefly reviews the CCITT X.500 standard from the point of view of providing the infrastructure for a secure EDI service. The X.500 series of standards specify methods of providing a global distributed directory service. It manages information objects which contain information about objects in the real world [16]. These objects are modelled as entries in an information base termed the Directory Information Base (DIB). A directory entry consists of one or more attributes. An attribute consists of a type and at least one value. The directory is extensible in that it defines several common types of objects and attributes and allows the definition of new objects and attributes. This extendibility will become an important factor as new OSI applications are developed that make use of the directory.

Use of directory services by EDI will become a necessity, as 'open' EDI relations are established. The X.500 directory could provide a means of storing security information necessary to enable the secure exchange of data between arbitrary partners within the EDI system. The use of cryptographic techniques in providing security features for an EDI service implies a need for key management. Key management encompasses the generation, distribution and control of cryptographic keys. This service would be incorporated into the X.500 directory service.

Public keys are learned by obtaining verifying certificates, data structures that bind names to public keys. Certification authorities issue public key certificates which provide a trusted binding of the entities name to a public key. This service could also be provided by the X.500 directory.

10 Conclusions

Security issues encompass a broad field of topics which will all play an important role in achieving a secure Open-EDI service. A standardized approach to security and EDI is essential and must consider this complex situation at the abstract as well as at the detailed levels. The relationship between business partners wishing to trade by using EDI requires a standard definition in order that the transactions can be controlled by an independent third party service using recognized methods. In this way the EDI service could provide the necessary level of confidence in its integrity, thus satisfying legal requirements imposed on it by the commercial world.

The need for defining levels of security depending on the type of data involved in the transaction has also been recognized. This requirement should not involve compromising the standardization of a secure EDI service. On the contrary, the incorporation of security levels is regarded as an integral part of the definition of a standardized but flexible secure EDI service.

In the interim and possibly in the long term also, VADS could extend their services to incorporate security features. In this manner they could assume the responsibility of satisfying the legal requirements of EDI and thus provide true added value to their customers.

Glossary of Terms

ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
CCITT	Comité Consultatif International Télégraphique et Téléphonique
DIB	Directory Information Base
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Finance, Administration, Commerce and Trade
EDIM	EDI Message as defined by CCITT X.435
EDIN	EDI Notification as defined by CCITT X.435
EDI-UA	EDI User Agent
FN	Forwarded EDI Notification (CCITT X.435)
ICC	International Chamber of Commerce
ISO	International Standards Organization
JTCI/SWG	Joint Technical Committee 1 / Software Working Group
MHS	Message Handling System
MTS	Message Transfer System
NN	Negative EDI Notification
ORName	Originator Recipient Name
OSI	Open Systems Interconnection
Pedi	Protocol for EDI as defined in CCITT X.435
PN	Positive EDI Notification
TEDIS	Trade Electronic Data Interchange Systems
UNB	EDIFACT Interchange Header Segment
UNICD	Uniform Rules for Conduct for the Interchange of Trade Data by Teletransmission

Bibliography

[1] The TEDIS-EDI security workshop. Brussels, June 20/21, 1989.

[2] *Goerdler M.* Secure EDI — a management overview. Office for official Publications of the European Communities, 1992.

[3] CCITT Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications. Recommandation X.800, Geneva, 1991.

[4] *Boland T.* Government Open Systems Interconnection Profile Users' Guide, Version 2. Computer Systems Laboratory, NIST, October 1991.

[5] *Gifkins M.* and *Hitchcock D.* The EDI Handbook. Blenheim Online, 1988.
Wheble B. Creating Legal Relationships with trading Partners.

[6] TEDIS Legal Aspects Factsheet. Commission of the European Communities. EN/89/1.

[7] TEDIS EDI Security Factsheet. Commission of the European Communities. EN/89/1 EUR 12293.

[8] *Pope N.* Targeting protection for EDI on Open Networks (Security and Standards associates).

[9] CCITT Message Handling Systems. EDI Messaging System. Recommendation X.435.

[10] CCITT Message Handling Service. Recommendation F.435.

[11] *Hill R.* EDI and X.400 using Pedi. The Guide for Implementors and Users. Technology Appraisals 1990.

[12] Report on the Open-EDI Conceptual Model. ISO/IEC JTCI/SWG-EDI N222-1.

[13] *Casey T.A., Vinther S.T., Weber D.G., Varadarajan R.* and *Rosenthal D.* A Secure Distributed Operating System. 1988 IEEE Symposium on Security and Privacy.

[14] *Tardo J.J.* and *Alagappan K.* SPX: Global Authentication Using Public Key Certificates. 1991 IEEE Symposium on Security and Privacy.

[15] *Fritzner C., Nilsen L.* and *Skomedal A.* 1991 IEEE Symposium on Security and Privacy.

[16] *Rose M.T.* The Little Black Book. Mail Bonding with OSI Directory Services. 1992, Prentice-Hall, Inc.

[17] CCITT Recommendations X.400—X.420. IXth Plenary Assembly. Melbourne, 1988, Geneva, 1989.

[18] Security on Open Systems. A Security Framework. ECMA TR/46. July 1988.

[19] Edifact. ISO 9735. International Standard for Electronic Data Interchange for administration, commerce and transport (EDIFACT), 1988.

[20] *Nechvatal J.* Public-Key Cryptography. NIST Special Publication 800-2. US Department of Commerce, National Institute of Standards and Technology.

Zusammenfassung

Sicherheit und EDI

Die vermehrte Nutzung des elektronischen Datenaustausches EDI am Markt hat gezeigt, dass verschiedene Aspekte der heutigen kommerziellen und rechtlichen Praxis noch Anpassungen erfordern. Die Geschäftswelt erwartet, dass der elektronische Datenaustausch denselben Stand bezüglich Sicherheit und Vertraulichkeit erreicht wie das bisher übliche Verfahren mit Papier. Die Tendenz zu «offenen» EDI-Systemen auf internationaler Ebene unterstreicht die Notwendigkeit einer genormten, umfassenden Behandlung der Sicherheitsaspekte. Die Sicherheitsanforderungen haben die Bemühungen der internationalen Normenorganisationen wie CCITT und ISO zur Definition von Sicherheitsdiensten in offenen Systemen beeinflusst und beschleunigt. Mit anerkannten Sicherheitsregeln auf internationaler Ebene beabsichtigt man, den rechtlichen Anforderungen des internationalen Handels zu genügen. Da heutige EDI-Systeme bereits gut eingeführt sind, werden sie von den auf OSI-Normen beruhenden Systemen nicht sofort abgelöst werden. In der Übergangsphase können EDI-Dienstanbieter ihre Dienste mit Sicherheitsfunktionen aufwerten und mit ihren Erfahrungen zum Erstellen international anerkannter Sicherheitsregeln beitragen.

Résumé

Sécurité et EDI

Le recours toujours plus fréquent à l'échange de documents informatisés (EDI) montre que divers aspects de la pratique commerciale et juridique actuelle doivent encore être adaptés. Les utilisateurs du monde des affaires s'attendent à ce que la sécurité et la confidentialité de l'EDI soient comparables à celles des documents sur papier. La tendance à créer des systèmes EDI «ouverts» à l'échelle internationale montre la nécessité de normaliser et de traiter de manière globale tous les critères de sécurité. Cette nécessité de sécurisation a contribué à accélérer les efforts des organismes internationaux de normalisations, tels que le CCITT et l'ISO, au sens d'une définition de services de sécurité dans des systèmes ouverts. En mettant en place des règles de sécurité reconnues sur le plan mondial, on souhaite satisfaire les exigences juridiques du commerce international. Les systèmes EDI actuels étant déjà bien introduits, ils ne seront guère remplacés sous peu par des procédés reposant sur les normes OSI. Durant une phase transitoire, les fournisseurs de services EDI pourront valoriser leurs prestations en les liant à des fonctions de sécurité et contribuer par les expériences faites à établir des règles de sécurité internationalement reconnues.

Riassunto

Sicurezza e EDI

Data la crescente commercializzazione dello scambio elettronico dei dati EDI è necessario adattare ancora diversi aspetti di natura economica e giuridica nella prassi. Il mondo degli affari si attende che lo scambio elettronico dei dati raggiunga in fatto di sicurezza e affidabilità lo stesso livello raggiunto finora dallo scambio di dati su supporto cartaceo. La tendenza verso sistemi EDI «aperti» a livello internazionale sottolinea la necessità di trattare in modo completo e standardizzato gli aspetti concernenti la sicurezza. Le esigenze di sicurezza hanno influenzato e accelerato gli sforzi delle organizzazioni di normazione internazionali come il CCITT e l'ISO volti a definire i «servizi di sicurezza» in sistemi aperti. L'introduzione di regole di sicurezza riconosciute a livello internazionale deve consentire di soddisfare le esigenze del commercio internazionale in materia giuridica. Dato che sono già ben introdotti, gli attuali sistemi EDI non verranno subito sostituiti con i sistemi basati sulle norme OSI. Nella fase transitoria, i fornitori di servizi EDI possono rivalutare i loro servizi dotandoli delle funzioni di sicurezza e contribuire con le loro esperienze all'allestimento di regole di sicurezza riconosciute a livello internazionale.

Summary

Security and EDI

The increasing use of Electronic Data Interchange (EDI) in the marketplace has highlighted many aspects of existing commercial and legal practice which require adaptation. Likewise, the business world enforces its requirements on EDI, expecting it to offer the same level of confidence to its users as the paper system it is replacing. The trend towards «open» EDI systems emphasizes the need for a standardized, coherent approach to security. The security requirements have influenced and accelerated the efforts of the international standards organizations such as CCITT and ISO in defining security services for Open Systems. Recognised international level security policies are intended to satisfy legal requirements of international commercial trading. As existing EDI systems are currently well established, the transition to EDI Systems based on OSI standards will not be immediate. During the transitory phase, existing EDI Service providers could enhance their existing EDI services with security functionality. Based on their experience, they could also play an important role in defining internationally acceptable security policies for EDI.