INTERNATIONAL STANDARD

ISO 9735-6

Second edition
2002-07-01

Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 6: Secure authentication and acknowledgement message (message type — AUTACK)

Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (numéro de version de syntaxe: 4, numéro d'édition de syntaxe: 1) —

Partie 6: Message sécurisé pour l'authentification et accusé de réception (type de message AUTACK)

Reference number
ISO 9735-6:2002(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO 9735 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 9735-6 was prepared by Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration* in collaboration with UN/CEFACT through the Joint Syntax Working Group (JSWG).

This second edition cancels and replaces the first edition (ISO 9735-6:1999). However ISO 9735:1988 and its Amendment 1:1992 are provisionally retained for the reasons given in clause 2.

Furthermore, for maintenance reasons the Syntax service directories have been removed from this and all other parts of the ISO 9735 series. They are now consolidated in a new part, ISO 9735-10.

At the time of publication of ISO 9735-1:1998, ISO 9735-10 had been allocated as a part for “Security rules for interactive EDI”. This was subsequently withdrawn because of lack of user support, and as a result, all relevant references to the title “Security rules for interactive EDI” were removed in this second edition of ISO 9735-6.

Definitions from all parts of the ISO 9735 series have been consolidated and included in ISO 9735-1.

ISO 9735 consists of the following parts, under the general title *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1)*:

— *Part 1: Syntax rules common to all parts*

— *Part 2: Syntax rules specific to batch EDI*

— *Part 3: Syntax rules specific to interactive EDI*

— *Part 4: Syntax and service report message for batch EDI (message type — CONTRL)*

— *Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*

— *Part 6: Secure authentication and acknowledgement message (message type — AUTACK)*

— *Part 7: Security rules for batch EDI (confidentiality)*

— *Part 8: Associated data in EDI*

— *Part 9: Security key and certificate management message (message type — KEYMAN)*

— *Part 10: Syntax service directories*

Further parts may be added in the future.

Annexes A to C of this part of ISO 9735 are for information only.

Introduction

This part of ISO 9735 includes the rules at the application level for the structuring of data in the interchange of electronic messages in an open environment, based on the requirements of either batch or interactive processing. These rules have been agreed by the United Nations Economic Commission for Europe (UN/ECE) as syntax rules for Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) and are part of the United Nations Trade Data Interchange Directory (UNTDID) which also includes both batch and interactive Message Design Guidelines.

Communications specifications and protocols are outside the scope of this part of ISO 9735.

This is a new part, which has been added to ISO 9735. It provides an optional capability of securing batch EDIFACT structures, i.e. messages, packages, groups or interchanges, by means of a secure authentication and acknowledgement message.

Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 6: Secure authentication and acknowledgement message (message type — AUTACK)

1 Scope

This part of ISO 9735 for EDIFACT security defines the secure authentication and acknowledgement message AUTACK.

2 Conformance

Whereas this part shall use a version number of “4” in the mandatory data element 0002 (Syntax version number), and shall use a release number of “01” in the conditional data element 0076 (Syntax release number), each of which appear in the segment UNB (Interchange header), interchanges continuing to use the syntax defined in the earlier published versions shall use the following Syntax version numbers, in order to differentiate them from each other and from this part:

— ISO 9735:1988 — *Syntax version number: 1*

— ISO 9735:1988 (amended and reprinted in 1990) — *Syntax version number: 2*

— ISO 9735:1988 and its Amendment 1:1992 — *Syntax version number: 3*

— ISO 9735:1998 — *Syntax version number: 4*

Conformance to a standard means that all of its requirements, including all options, are supported. If all options are not supported, any claim of conformance shall include a statement which identifies those options to which conformance is claimed.

Data that is interchanged is in conformance if the structure and representation of the data conform to the syntax rules specified in this part of ISO 9735.

Devices supporting this part of ISO 9735 are in conformance when they are capable of creating and/or interpreting the data structured and represented in conformance with this part of ISO 9735.

Conformance to this part of ISO 9735 shall include conformance to parts 1, 2, 5 and 10 of ISO 9735.

When identified in this part of ISO 9735, provisions defined in related standards shall form part of the conformance criteria.

3 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 9735. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 9735 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 9735-1:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 1: Syntax rules common to all parts*

ISO 9735-2:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 2: Syntax rules specific to batch EDI*

ISO 9735-5:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*

ISO 9735-10:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 10: Syntax service directories*

4 Terms and definitions

For the purposes of this part of ISO 9735, the terms and definitions given in ISO 9735-1 apply.

5 Rules for the use of the secure authentication and acknowledgement message

5.1 Functional definition

AUTACK is a message authenticating sent, or providing secure acknowledgement of received interchanges, groups, messages or packages.

A secure authentication and acknowledgement message can be used to:

a) give secure authentication, integrity or non-repudiation of origin to messages, packages, groups or interchanges;

b) give secure acknowledgement or non-repudiation of receipt to secured messages, packages, groups or interchanges.

5.2 Field of application

The secure authentication and acknowledgement message (AUTACK) may be used for both national and international trade. It is based on universal practice related to administration, commerce and transport, and is not dependent on the type of business or industry.

5.3 Principles

5.3.1 General

The applied security procedures shall be agreed to by trading partners and specified in an interchange agreement.

The secure authentication and acknowledgement message (AUTACK) applies security services to other EDIFACT structures (messages, packages, groups or interchanges) and provides secure acknowledgement to secured EDIFACT structures. It can be applied to combinations of EDIFACT structures that need to be secured between two parties.

The security services are provided by cryptographic mechanisms applied to the content of the original EDIFACT structures. The results of these mechanisms form the body of the AUTACK message, supplemented by relevant data such as references of the cryptographic methods used, the reference numbers for the EDIFACT structures and the date and time of the original structures.

The AUTACK message shall use the standard security header and trailer groups.

The AUTACK message can apply to one or more messages, packages or groups from one or more interchanges, or to one or more interchanges. As one example, Figure 1 describes an interchange when using the AUTACK message together with one or more messages.

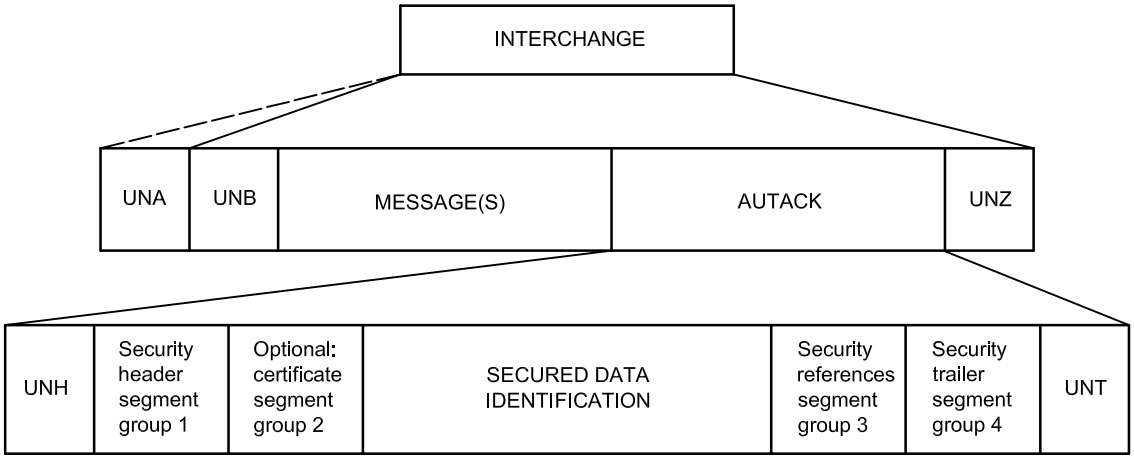

Figure 1 — Interchange showing security by using the AUTACK message at message level (schematic)

5.3.2 Use of AUTACK for the authentication function

5.3.2.1 General

An AUTACK message used as an authentication message shall be sent by the originator of one or more other EDIFACT structures, or by a party having authority to act on behalf of the originator. Its purpose is to facilitate the security services defined in ISO 9735-5, i.e. authenticity, integrity, and non-repudiation of origin of its associated EDIFACT structures.

An AUTACK authentication message can be implemented in two ways. The first method conveys the hashed values of the referenced EDIFACT structures secured by the AUTACK itself; the second uses the AUTACK only to convey digital signatures of the referenced EDIFACT structures.

5.3.2.2 Authentication using hash values of the referenced EDIFACT structures

The secured EDIFACT structure shall be referenced in an occurrence of the USX (security references) segment. For each USX there shall be at least one corresponding USY (security on references) segment which contains the security result, for example the hash value, of the security function performed on the referenced EDIFACT structure.

Details about the security function performed shall be contained in the AUTACK security header group. The USY and USH segments for the referenced EDIFACT structure shall be linked using security reference number data elements in both segments.

As a final step, all the information conveyed in the AUTACK shall be secured using at least one pair of security header and security trailer groups.

NOTE AUTACK uses the USX segment to reference one or more messages, packages or groups in one or more interchanges, or to reference an entire interchange. For each USX segment a corresponding USY segment contains the result of the hashing, authentication or non-repudiation method applied to the referenced EDIFACT structure.

5.3.2.3 Authentication using digital signatures of the referenced EDIFACT structures

The secured EDIFACT structure shall be referenced in an occurrence of the USX (security references) segment. For each USX at least one corresponding USY (security on references) segment, which contains the digital signature of the referenced EDIFACT structure, shall be present. Details about the security function performed shall be contained in the AUTACK security header group. Because a single referenced EDIFACT structure may be secured more than once, the related USY and security header group shall be linked using security reference number data elements in both segments.

If the digital signature of the referenced EDIFACT structure is contained in AUTACK (rather than just a hash value), the AUTACK does not itself require to be secured.

5.3.3 The use of AUTACK for the acknowledgement function

An AUTACK message used as an acknowledgement message shall be sent by the recipient of one or more previously received secured EDIFACT structures, or by a party having authority to act on behalf of the recipient. Its purpose is to facilitate confirmation of receipt, validation of integrity of content, validation of completeness and/or non-repudiation of receipt of its associated EDIFACT structures.

The acknowledgement function shall be applied only to secured EDIFACT structures. The secured EDIFACT structure shall be referenced in an occurrence of the USX (security references) segment. For each USX there shall be at least one corresponding USY (security on references) segment which contains either the hash value or the digital signature of the referenced EDIFACT structure. The USY shall be linked to a security header group of the referenced EDIFACT structure, or of an AUTACK message securing it, by using security reference number data element. The corresponding security header related to the referenced EDIFACT structure contains the details of the security function performed on the referenced EDIFACT structure by the sender of the original message.

As a final step in generation of the acknowledgement message, all the information conveyed in the AUTACK shall be secured using at least one pair of security header and security trailer groups.

AUTACK may also be used for non-acknowledgement in case of problems with the verification of the security results.

NOTE Secure acknowledgement is only meaningful for secured EDIFACT structures. Securing EDIFACT structures is accomplished by the use of either integrated security segments (see ISO 9735-5) or AUTACK authentication.

To prevent endless loops, an AUTACK used for the acknowledgement function shall not require its recipient to send back an AUTACK acknowledgement message.

5.4 Message definition

5.4.1 Data segment clarification

0010 **UNH, Message header**

A service segment starting and uniquely identifying a message.

The message type code for the secure authentication and acknowledgement message is AUTACK.

The data element message type sub-function identification shall be used to indicate the usage of the AUTACK function as either authentication, acknowledgement or refusal of acknowledgement.

Secure authentication and acknowledgement messages conforming to this document must contain the following data in segment UNH, composite S009:

Data element	0065	AUTACK
	0052	4
	0054	1
	0051	UN

0020 **Segment Group 1: USH-USA-SG2 (security header group)**

A group of segments identifying the security service and security mechanisms applied and containing the data necessary to carry out the validation calculations (as defined in ISO 9735-5).

This segment group shall specify the security service and algorithm(s) applied to the AUTACK message or applied to the referenced EDIFACT structure.

Each security header group shall be linked to a security trailer group, and some may be linked additionally to USY segments.

0030 **USH, Security header**

A segment specifying a security service applied to the message/package in which the segment is included, or to the referenced EDIFACT structure (as defined in ISO 9735-5).

The security service data element shall specify the security function applied to the AUTACK message or the referenced EDIFACT structure:

— the security services: message origin authentication and non-repudiation of origin shall only be used for the AUTACK message itself;

— the security services: referenced EDIFACT structure integrity, referenced EDIFACT structure origin authentication and referenced EDIFACT structure non-repudiation of origin shall only be used by the sender to secure the AUTACK referenced EDIFACT structures;

— the security services: receipt authentication and non-repudiation of receipt shall only be used by the receiver of secured EDIFACT structures to secure the acknowledgement.

The scope of security application of the security service shall be specified, as defined in ISO 9735-5. In an AUTACK message, there are four possible scopes of security application:

— the first two scopes are as defined in ISO 9735-5:2002, clause 5;

— the third scope includes the whole EDIFACT structure, in which the scope of the security application is from the first character of the referenced message, package, group or interchange (namely a “U”) to the last character of the message, package, group or interchange, inclusive;

— the fourth scope is user defined, in which scope the security application is defined in an agreement between sender and receiver.

0040 **USA, Security algorithm**

A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required (as defined in ISO 9735-5).

0050 **Segment Group 2: USC-USA-USR (certificate group)**

A group of segments containing the data necessary to validate the security methods applied to the message/package, when asymmetric algorithms are used (as defined in ISO 9735-5).

0060 **USC, Certificate**

A segment containing the credentials of the certificate owner and identifying the certification authority which has generated the certificate (as defined in ISO 9735-5).

0070 **USA, Security algorithm**

A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required (as defined in ISO 9735-5).

0080 **USR, Security result**

A segment containing the result of the security functions applied to the certificate by the certification authority (as defined in ISO 9735-5).

0090 **USB, Secured data identification**

This segment shall contain identification of the interchange sender and interchange recipient, a security related timestamp of the AUTACK and it shall specify whether a secure acknowledgement from the AUTACK message recipient is required or not. If one is required, the message sender will expect an AUTACK acknowledgement message to be sent back by the message recipient.

The interchange sender and interchange recipient in USB shall refer to the sender and the recipient of the interchange in which the AUTACK is present, in order to secure this information.

0100 **Segment group 3: USX-USY**

This segment group shall be used to identify a party in the security process and to give security information on the referenced EDIFACT structure.

0110 **USX, Security references**

This segment shall contain references to the party involved in the security process.

The composite data element security date and time may contain the original generation date and time of the referenced EDIFACT structure.

If data element 0020 is present and none of: 0048, 0062 and 0800 are present, the whole interchange is referenced.

If data elements 0020 and 0048 are present and none of: 0062 and 0800 are present, the group is referenced.

0120 **USY, Security on references**

A segment containing a link to a security header group and the result of the security services applied to the referenced EDIFACT structure as specified in this linked security header group.

When the referenced EDIFACT structures are secured by the same security service, with the same related security parameters many USY segments may be linked to the same security header group. In this case the link value between the security header group and the related USYs shall be the same.

When AUTACK is used for the acknowledgement function, the corresponding security header group shall be either one of the referenced EDIFACT structure or of an AUTACK message that is used to provide the referenced EDIFACT structure with the authentication function.

In a USY segment the value of data element 0534 shall be identical to the value in 0534 in the corresponding USH segment of either:

— the current AUTACK, if the authentication function is used (security services: referenced EDIFACT structure origin authenticity, referenced EDIFACT structure integrity or referenced EDIFACT structure non-repudiation of origin);

— the referenced EDIFACT structure itself, or an AUTACK message providing the referenced EDIFACT structure with the authentication function, if the acknowledgement function is used (security services: non-repudiation of receipt or receipt authentication).

0130 **Segment Group 4: UST-USR (security trailer group)**

A group of segments containing a link with security header segment group and the result of the security functions applied to the message/package (as defined in ISO 9735-5).

USR segment may be omitted if the security trailer group is linked to a security header group related to a referenced EDIFACT structure. In this case the corresponding results of the security function shall be found in the USY segments which are linked to the relevant security header group.

0140 **UST, Security trailer**

A segment establishing a link between security header and security trailer segment group and stating the number of security segments contained in these groups (as defined in ISO 9735-5).

0150 **USR, Security result**

A segment containing the result of the security functions applied to the message/package as specified in the linked security header group (as defined in ISO 9735-5). The security result in this segment shall be applied to the AUTACK message itself.

0160 **UNT, Message trailer**

A service segment ending a message, giving the total number of segments and the control reference number of the message.

5.4.2 Message structure

Table 1 — Segment table

POS	TAG	Name	S	R	Notes
0010	UNH	Message header	M	1	
0020	----	Segment group 1 ----------	M	99	-------+
0030	USH	Security header	M	1	|
0040	USA	Security algorithm	C	3	|
					|
0050	-----	Segment group 2 ----------	C	2	----+ |
0060	USC	Certificate	M	1	| |
0070	USA	Security algorithm	C	3	| |
0080	USR	Security result	C	1	----+--+
0090	USB	Secured data identification	M	1	
0100	-----	Segment group 3 ----------	M	9999	----+
0110	USX	Security references	M	1	|
0120	USY	Security on references	M	9	----+
0130	-----	Segment group 4 ----------	M	99	----+
0140	UST	Security trailer	M	1	|
0150	USR	Security result	C	1	----+
0160	UNT	Message trailer	M	1	

NOTE The message body of the AUTACK message comprises the USB segment and segment group 3.

Annex A
(informative)

AUTACK message examples

A.1 Introduction

Three examples are provided in this annex to illustrate different applications of the AUTACK message.

The first one shows how to use an AUTACK message to secure a previously sent message, in order to provide the security service of non-repudiation of origin. An AUTACK acknowledgement message is required.

The second example shows how an AUTACK message may secure two messages with different security services: non-repudiation of origin for one message, message origin authentication for another message.

The third example illustrates the usage of AUTACK message for secure acknowledgement. It shows the AUTACK acknowledgement message required by the AUTACK in the first example.

A.2 Example 1: Non-repudiation of origin service provided by an AUTACK message

A.2.1 Narrative

Bank A wants the security service of non-repudiation of origin on the payment orders from Company A, performed by Mr. Smith when they exceed a certain amount.

The interchange agreement between the parties establishes that the security service of non-repudiation of origin, required by Bank A, shall be achieved for these payment orders, by Mr. Smith of Company A, with the use of one digital signature.

Both parties agree that this digital signature is computed by 512 bit RSA (asymmetric algorithm) upon a hashing value computed using the MD5 algorithm.

The certificate identifying the public key of Mr. Smith is issued by an authority trusted by both parties, the certificate issuer.

In these conditions, because the digital signature of the PAYORD is included in the AUTACK message, the AUTACK itself does not need to be signed.

The PAYORD message secured by AUTACK was the third message of the first interchange sent by Mr. Smith to the Bank A. It was generated in 1996.01.15 at 10:00:00.

The AUTACK itself was the fifth message of the interchange and it was generated in 1996.01.15 at 10:05:32.

The appearing security segments are the following ones:

— USH to indicate the security service applied to the PAYORD message;

— USC-USA-USA-USA-USR, the certificate of Mr. Smith;

— USB;

— USX-USY with the security references and results (for PAYORD message);

— UST, without USR, referencing the USH.

A.2.2 Security details

SECURITY HEADER	
SECURITY SERVICE, CODED	Non-repudiation of origin
SECURITY REFERENCE NUMBER	The reference of this header is 1.
RESPONSE TYPE	Acknowledgement required: 1.
FILTER FUNCTION	All binary values (signatures) are filtered with hexadecimal filter.
ORIGINAL CHARACTER SET ENCODING	The message was coded in ASCII 8 bits when its signature was generated.
CERTIFICATE	Certificate of Mr. SMITH
CERTIFICATE REFERENCE	This certificate is referenced, by AUTHORITY: 00000001.
SECURITY IDENTIFICATION DETAILS Security party qualifier	 Certificate owner (Mr. SMITH of Company A)
SECURITY IDENTIFICATION DETAILS Security party qualifier Key name	 Certificate issuer (Mr. SMITH's certificate was generated by a certification Authority called: AUTHORITY.) The Public Key of AUTHORITY used to generate Mr. SMITH's certificate is PK1.
CERTIFICATE SYNTAX VERSION	Version of certificate of UN/EDIFACT service segment directory.
FILTER FUNCTION	All binary values (keys and digital signatures) are filtered with hexadecimal filter.
ORIGINAL CHARACTER SET ENCODING	The credentials of the certificate were coded in ASCII 8 bits when the certificate was generated.
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is segment terminator. Value “'” (apostrophe)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is data element separator. Value “+” (plus sign)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is component data element separator. Value “:” (colon)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is repetition separator. Value “*” (asterisk)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is release character. Value “?” (question mark)
SECURITY DATE AND TIME Date and time	Certificate generation time Mr. SMITH certificate was generated on 931215 at 14:12:00.
SECURITY DATE AND TIME Date and time	Certificate start of validity period Validity period of Mr. SMITH's certificate starts: 1996 01 01 000000.
SECURITY DATE AND TIME Date and time	Certificate end of validity period Validity of Mr. SMITH's certificate ends: 1996 12 31 235959.

SECURITY ALGORITHM	Asymmetric algorithm used by Mr. SMITH to sign.
SECURITY ALGORITHM	
Use of algorithm	An owner signing algorithm is used.
Cryptographic mode of operation	No mode of operation is relevant here.
Algorithm	RSA is the asymmetric algorithm.
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Public exponent for signature verification.
Algorithm parameter value	Mr. SMITH's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Modulus for signature verification.
Algorithm parameter value	Mr. SMITH's modulus
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as the length of Mr. SMITH's modulus (in bits).
Algorithm parameter value	Mr. SMITH's modulus is 512 bits long.
SECURITY ALGORITHM	Hash function used by AUTHORITY to generate Mr. SMITH's certificate.
SECURITY ALGORITHM	
Use of algorithm	An issuer hashing algorithm is used.
Cryptographic mode of operation	Hash function CD 10118-2 Hash functions using a n-bit block cipher algorithm applied to provide a double length hash code (128 bits); initializing values: A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210
Algorithm	MD5 message-digest algorithm is used.
SECURITY ALGORITHM	Asymmetric algorithm used by AUTHORITY to sign.
SECURITY ALGORITHM	
Use of algorithm	An issuer signing algorithm is used.
Cryptographic mode of operation	No mode of operation is relevant here.
Algorithm	RSA is the asymmetric algorithm.
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a public exponent for signature verification.
Algorithm parameter value	AUTHORITY's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Modulus for signature verification.
Algorithm parameter value	AUTHORITY's modulus
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as the length of AUTHORITY's modulus (in bits).
Algorithm parameter value	AUTHORITY's modulus is 512 bits long.
SECURITY RESULT	Digital signature of the certificate

VALIDATION RESULT Validation value qualifier Validation value	 Unique validation value is 1. 512 Bit filtered hexadecimal digital signature.
SECURED DATA IDENTIFICATION	
RESPONSE TYPE, CODED	A secure acknowledgement from the Bank A is required.
SECURITY DATE AND TIME Date and time Event date Event time	 A security related time-stamp of the AUTACK. The security time stamp is: date: 1996 01 15. Time: 10:05:32
INTERCHANGE SENDER Interchange sender identification	Identification of the interchange sender Identification of Mr. Smith, Company A
INTERCHANGE RECIPIENT Interchange sender identification	Identification of the interchange recipient Identification of Bank A
SECURITY REFERENCES	Refers to the security entity (PAYORD related with the service of non-repudiation of origin) and its associated date and time.
INTERCHANGE CONTROL REFERENCE	Identifies the reference number assigned by the sender to the interchange of the message PAYORD: 1.
INTERCHANGE SENDER Interchange sender identification	 Identifies the sender of the interchange of the message PAYORD: Mr. Smith from Company A.
INTERCHANGE RECIPIENT Interchange recipient identification	 Identifies the recipient of the interchange of the message PAYORD: Bank A.
MESSAGE REFERENCE NUMBER	Identifies the reference number assigned by the sender to the PAYORD message: 3.
SECURITY DATE AND TIME Date and time Event date Event time	 A security related time-stamp referring the PAYORD. The security time stamp is date: 1996 01 15. Time: 10:00:00
SECURITY ON REFERENCES	Identifies the applicable header (associated with the functions of security applied to the PAYORD message), and the result of applying these functions to the PAYORD message.
SECURITY REFERENCE NUMBER	Number which links the validation result to the corresponding USH segment. In this case his value is 1.
VALIDATION RESULT Validation value qualifier Validation value	 Unique validation value is 1. 512 bit filtered hexadecimal digital signature (of the PAYORD message).
SECURITY TRAILER	
SECURITY REFERENCE NUMBER	The reference of this security trailer is 1.
NUMBER OF SECURITY SEGMENTS	The number of security segments is 7.

A.3 Example 2: Securing several messages with AUTACK

A.3.1 Narrative

Bank A wants the security service of non-repudiation of origin on the payment orders from Company A, performed by Mr. Smith when they exceed a certain amount. For those payment orders not exceeding such amount, message origin authentication service is requested.

The interchange agreement between the parties establishes that the security service of non-repudiation of origin, required by Bank A, shall be achieved for these payment orders, by Mr. Smith of Company A, with the use of one digital signature. Both parties agree that this digital signature is computed by 512 bit RSA (asymmetric algorithm) upon a hashing value computed using the MD5 algorithm.

In addition, message origin authentication will be achieved by generating a “Message Authentication Code” (MAC) with the symmetric DES according to ISO 8731-1 at the sender's site.

The certificate identifying the public key of Mr. Smith is issued by an authority trusted by both parties, the certificate issuer.

The first PAYORD message sent has to be secured with a digital signature by AUTACK. It is the fifth message of the first interchange sent by Mr. Smith to Bank A. It was sent in 1996.01.15 at 08:00:00.

The second PAYORD message sent has to be secured with a MAC by AUTACK. It is the seventh message of the first interchange. It was sent in 1996.01.15 at 09:00:00.

The AUTACK itself is the tenth message of the first interchange. It was sent in 1996.01.15 at 10:05:32.

As the first PAYORD message is secured with a digital signature, the AUTACK itself does not need to be signed.

In consequence, the appearing security segments are the following ones:

— USH to indicate the non-repudiation of origin service applied to the first PAYORD message;

— USC-USA-USA-USA-USR, the certificate of Mr. Smith;

— USH to indicate the message origin authentication service applied to the second PAYORD message;

— USB;

— USX-USY with the security references and result (digital signature) for the first PAYORD message;

— USX-USY with the security references and result (MAC) for the second PAYORD message;

— UST, without USR, referencing the first USH;

— UST, without USR, referencing the second USH.

A.3.2 Security details

SECURITY HEADER	Header containing information of the security function performed on the referenced entity (first PAYORD message).
SECURITY SERVICE, CODED	Non-repudiation of origin for the first PAYORD
SECURITY REFERENCE NUMBER	The reference of this header is 1.
FILTER FUNCTION	All binary values are filtered with hexadecimal filter.
ORIGINAL CHARACTER SET ENCODING	The message was coded in ASCII 8 bits when its signature was generated.
SECURITY IDENTIFICATION DETAILS Security party qualifier	 Message sender (Mr. Smith from Company A)
SECURITY IDENTIFICATION DETAILS Security party qualifier	 Message receiver (Bank A)
CERTIFICATE	Certificate of Mr. SMITH
CERTIFICATE REFERENCE	This certificate is referenced by AUTHORITY: 00000001.
SECURITY IDENTIFICATION DETAILS Security party qualifier	 Certificate owner (Mr. SMITH of Company A)
SECURITY IDENTIFICATION DETAILS Security party qualifier Key name	 Certificate issuer (Mr. SMITH's certificate was generated by a certification Authority called: AUTHORITY.) The Public Key of AUTHORITY used to generate Mr. SMITH's certificate is PK1.
CERTIFICATE SYNTAX VERSION	Version of certificate of UN/EDIFACT service segment directory
FILTER FUNCTION	All binary values (keys and digital signatures) are filtered with hexadecimal filter.
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is segment terminator. Value “'” (apostrophe)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is data element separator. Value “+” (plus sign)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is component data element separator. Value “:” (colon)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is repetition separator. Value “*” (asterisk)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is release character. Value “?” (question mark)
SECURITY DATE AND TIME Date and time	Certificate generation time Mr. SMITH certificate was generated on 931215 at 14:12:00.
SECURITY DATE AND TIME Date and time	Certificate start of validity period Validity period of Mr. SMITH's certificate starts: 1996 01 01 000000.

SECURITY DATE AND TIME	Certificate end of validity period
Date and time	Validity of Mr. SMITH's certificate ends: 1996 12 31 235959.
SECURITY ALGORITHM	Asymmetric algorithm used by Mr. SMITH to sign.
SECURITY ALGORITHM	
Use of algorithm	An owner signing algorithm is used.
Cryptographic mode of operation	No mode of operation is relevant here.
Algorithm	RSA is the asymmetric algorithm.
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Public exponent for signature verification.
Algorithm parameter value	Mr. SMITH's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Modulus for signature verification.
Algorithm parameter value	Mr. SMITH's modulus
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as the length of Mr. SMITH's modulus (in bits).
Algorithm parameter value	Mr. SMITH's modulus is 512 bits long.
SECURITY ALGORITHM	Hash function used by AUTHORITY to generate Mr. SMITH's certificate.
SECURITY ALGORITHM	
Use of algorithm	An issuer hashing algorithm is used.
Cryptographic mode of operation	Hash function CD 10118-2 Hash functions using a n-bit block cipher algorithm applied to provide a double length hash code (128 bits); initializing values: A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210
Algorithm	MD5 message-digest algorithm is used.
SECURITY ALGORITHM	Asymmetric algorithm used by AUTHORITY to sign.
SECURITY ALGORITHM	
Use of algorithm	An issuer signing algorithm is used.
Cryptographic mode of operation	No mode of operation is relevant here.
Algorithm	RSA is the asymmetric algorithm.
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a public exponent for signature verification.
Algorithm parameter value	AUTHORITY's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Modulus for signature verification.
Algorithm parameter value	AUTHORITY's modulus
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as the length of AUTHORITY's modulus (in bits).
Algorithm parameter value	AUTHORITY's modulus is 512 bits long.

SECURITY RESULT	Digital signature of the certificate
VALIDATION RESULT Validation value qualifier Validation value	 Unique validation value is 1. 512 Bit filtered hexadecimal digital signature
SECURITY HEADER	Header containing information of the security function performed on the referenced entity (second PAYORD message).
SECURITY SERVICE, CODED	Message origin authentication for the second PAYORD
SECURITY REFERENCE NUMBER	The reference of this header is 2.
FILTER FUNCTION	All binary values are filtered with hexadecimal filter.
SECURITY IDENTIFICATION DETAILS Security party qualifier	 Message sender (Mr. Smith from Company A)
SECURITY IDENTIFICATION DETAILS Security party qualifier	 Message receiver (Bank A)
SECURITY ALGORITHM	
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	 A symmetric algorithm is used to achieve message origin authentication. A MAC is computed, according to ISO 8731-1. The DES algorithm is used.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 Identifies this algorithm parameter values as the name of a previously exchanged symmetric key. 1234567890ABCDEF
SECURED DATA IDENTIFICATION	
RESPONSE TYPE, CODED	No acknowledgement from the Bank A is required.
SECURITY DATE AND TIME Date and time Event date Event time	 A security related timestamp of the AUTACK. The security time stamp is: date: 1996 01 15. Time: 10:05:32
INTERCHANGE SENDER Interchange sender identification	Identification of the interchange sender Identification of Mr. Smith, Company A
INTERCHANGE RECIPIENT Interchange sender identification	Identification of the interchange recipient Identification of Bank A
SECURITY REFERENCES	Refers to the security entity (second PAYORD).
INTERCHANGE CONTROL REFERENCE	Identifies the reference number assigned by the sender to the interchange of the second PAYORD: 1.
INTERCHANGE SENDER Interchange sender identification	 Identifies the sender of the interchange of the message PAYORD: Mr. Smith from Company A.
INTERCHANGE RECIPIENT Interchange recipient identification	 Identifies the recipient of the interchange of the message PAYORD: Bank A.
MESSAGE REFERENCE NUMBER	Identifies the reference number assigned by the sender to the second PAYORD message: 7.

SECURITY DATE AND TIME Event date Event time	 The security time stamp is: date: 1996 01 15. Time: 09:00:00
SECURITY ON REFERENCES	Identifies the applicable header (associated with the functions of security applied to the second PAYORD message), and the result of applying these functions to it.
SECURITY REFERENCE NUMBER	Number which links the validation result to the corresponding USH segment. In this case his value is 2.
VALIDATION RESULT Validation value qualifier Validation value	 MAC (Message Authentication Code) 12345678 - This is a 4 byte value.
SECURITY REFERENCES	Refers to the security entity (the first PAYORD) and its associated date and time.
INTERCHANGE CONTROL REFERENCE	Identifies the reference number assigned by the sender to the interchange of the message PAYORD: 1.
INTERCHANGE SENDER Interchange sender identification	 Identifies the sender of the interchange of the message PAYORD: Mr. Smith from Company A.
INTERCHANGE RECIPIENT Interchange recipient identification	 Identifies the recipient of the interchange of the message PAYORD: Bank A.
MESSAGE REFERENCE NUMBER	Identifies the reference number assigned by the sender to the first PAYORD message: 5.
SECURITY DATE AND TIME Event date Event time	 The security time stamp is: date: 1996 01 15. Time: 08:00:00
SECURITY ON REFERENCES	Identifies the applicable header (associated with the functions of security applied to the first PAYORD message) and the result of applying these functions to it.
SECURITY REFERENCE NUMBER	Number which links the validation result to the corresponding USH segment. In this case his value is 1.
VALIDATION RESULT Validation value qualifier Validation value	 Unique validation value is 1. 512 bit filtered hexadecimal digital signature (of the first PAYORD message).
SECURITY TRAILER	
SECURITY REFERENCE NUMBER	The reference of this security trailer is 2.
NUMBER OF SECURITY SEGMENTS	The number of security segments is 2.
SECURITY TRAILER	
SECURITY REFERENCE NUMBER	The reference of this security trailer is 1.
NUMBER OF SECURITY SEGMENTS	The number of security segments is 7.

A.4 Example 3: Secure acknowledgement of a received message by AUTACK

A.4.1 Narrative

In the example 1, AUTACK was used by the sender (Mr. Smith of Company A) of a previous message PAYORD. The AUTACK message requested an acknowledgement to Bank A.

In this example, it is shown how the AUTACK message is used as secure acknowledgement.

It has been established that AUTACK messages acting as secure acknowledgement will be protected with the non-repudiation of origin, by using a digital signature.

The AUTACK message is generated in 1996.01.16 at 11:00:00, being the 20th message from the interchange.

The appearing security segments are the following ones:

— USH, to identify the security service applied to the AUTACK message;

— USH, to identify the security service applied to the entity acknowledged;

— USC-USA(3)-USR, the certificate of Bank A;

— USB, to contain details of the AUTACK;

— USX-USY, to contain references to the acknowledged entity and the digital signature;

— UST, the Security Trailer without USR;

— UST-USR to secure the AUTACK itself.

A.4.2 Security details

SECURITY HEADER	
SECURITY SERVICE, CODED	Non-repudiation of origin
SECURITY REFERENCE NUMBER	The reference of this header is 1.
FILTER FUNCTION	All binary values are filtered with hexadecimal filter.
ORIGINAL CHARACTER SET ENCODING	The message was coded in ASCII 8 bits when the MAC was generated.
SECURITY IDENTIFICATION DETAILS Security party qualifier	Message sender (party which generates the digital Signature): Bank A
SECURITY IDENTIFICATION DETAILS Security party qualifier	Message receiver (party which verifies the digital Signature): Mr. SMITH of Company A
SECURITY SEQUENCE NUMBER	The security sequence number of this message is 20.
SECURITY DATE AND TIME Event date Event time	 The security time stamp is: date: 1996.01.16. Time: 11:00:00
CERTIFICATE	Certificate of Bank A
CERTIFICATE REFERENCE	This certificate is referenced, by AUTHORITY: 00000010.

SECURITY IDENTIFICATION DETAILS Security party qualifier	 Certificate owner (Bank A)
SECURITY IDENTIFICATION DETAILS Security party qualifier Key name	 Certificate issuer (Bank A's certificate was generated by a certification Authority called: AUTHORITY.) The Public Key of AUTHORITY used to generate Bank A's certificate is PK1.
CERTIFICATE SYNTAX VERSION	Version of certificate of UN/EDIFACT service segment directory
FILTER FUNCTION	All binary values (keys and digital signatures) are filtered with hexadecimal filter.
ORIGINAL CHARACTER SET ENCODING	The credentials of the certificate were coded in ASCII 8 bits when the certificate was generated.
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is segment terminator. Value “'” (apostrophe)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is data element separator. Value “+” (plus sign)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is component data element separator. Value “:” (colon)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is repetition separator. Value “*” (asterisk)
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	Service character used when signature was computed. Service character is release character. Value “?” (question mark)
SECURITY DATE AND TIME Date and time	Certificate generation time Bank A certificate was generated on 1995 12 31 at 14:00:00.
SECURITY DATE AND TIME Date and time	Certificate start of validity period Validity period of Bank A's certificate starts: 1996 01 01 000000.
SECURITY DATE AND TIME Date and time	Certificate end of validity period Validity of Bank A's certificate ends: 1996 12 31 235959.
SECURITY ALGORITHM	Asymmetric algorithm used by Bank A to sign.
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	 An owner signing algorithm is used. No mode of operation is relevant here. RSA is the asymmetric algorithm.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 Identifies this algorithm parameter as a Public exponent for signature verification. Bank A's public key

ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Modulus for signature verification.
Algorithm parameter value	Bank A's modulus
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as the length of Bank A's modulus (in bits).
Algorithm parameter value	Bank A's modulus is 512 bits long.
SECURITY ALGORITHM	Hash function used by AUTHORITY to generate Bank A's certificate.
SECURITY ALGORITHM	
Use of algorithm	An issuer hashing algorithm is used.
Cryptographic mode of operation	Hash function CD 10118-2 Hash functions using a n-bit block cipher algorithm applied to provide a double length hash code (128 bits); initializing values: A = 01234567 B = 89ABCDEF C = FEDCBA98 D = 76543210
Algorithm	MD5 message-digest algorithm is used.
SECURITY ALGORITHM	Asymmetric algorithm used by AUTHORITY to sign.
SECURITY ALGORITHM	
Use of algorithm	An issuer signing algorithm is used.
Cryptographic mode of operation	No mode of operation is relevant here.
Algorithm	RSA is the asymmetric algorithm.
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a public exponent for signature verification.
Algorithm parameter value	AUTHORITY's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as a Modulus for signature verification.
Algorithm parameter value	AUTHORITY's modulus
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter as the length of AUTHORITY's modulus (in bits).
Algorithm parameter value	AUTHORITY's modulus is 512 bits long.
SECURITY RESULT	Digital signature of the certificate
VALIDATION RESULT	
Validation value qualifier	Unique validation value is 1.
Validation value	512 Bit filtered hexadecimal digital signature
SECURITY HEADER	Header containing information of the security function performed on the referenced entity (PAYORD) acknowledged.
SECURITY SERVICE, CODED	Non-repudiation of origin
SECURITY REFERENCE NUMBER	The reference of this header is 2.
FILTER FUNCTION	All binary values (signatures) are filtered with hexadecimal filter.
ORIGINAL CHARACTER SET ENCODING	The message was coded in ASCII 8 bits when its signature was generated.

SECURED DATA IDENTIFICATION	
SECURITY DATE AND TIME	The security time stamp for this AUTACK message is: date: 1996.01.16 time: 11:00:00.
INTERCHANGE SENDER Interchange sender identification	Identification of the interchange sender Identification of the Bank A
INTERCHANGE RECIPIENT Interchange recipient identification	Identification of the interchange recipient Identification of the Mr. Smith, Company A
SECURITY REFERENCES	To refer to the security entity (message acknowledged) and its associated date and time.
INTERCHANGE CONTROL REFERENCE	To identify the reference number of the interchange of the acknowledged PAYORD message: 1.
INTERCHANGE SENDER Interchange sender identification	To identify the sender of the interchange to which belongs the message acknowledged: Mr. Smith of Company A.
INTERCHANGE RECIPIENT Interchange recipient identification	To identify the recipient of the interchange of the message acknowledged: Bank A.
MESSAGE REFERENCE NUMBER	To identify the reference number assigned by the sender to the message acknowledged: 3 (see example 1).
SECURITY DATE AND TIME	The security time stamp of the PAYORD is: date:1996.01.15, time: 10:00:00.
SECURITY ON REFERENCES	
SECURITY REFERENCE NUMBER	Identifies the applicable header 2.
VALIDATION RESULT Validation value qualifier Validation value	 Unique validation value is 1. 512 bit filtered hexadecimal digital signature of the PAYORD acknowledged.
SECURITY TRAILER	
SECURITY REFERENCE NUMBER	The reference of this security trailer is 2.
NUMBER OF SECURITY SEGMENTS	The number of security segments is 3.
SECURITY TRAILER	
SECURITY REFERENCE NUMBER	The reference of this security trailer is 1.
NUMBER OF SECURITY SEGMENTS	The number of security segments is 7.
SECURITY RESULT	
VALIDATION RESULT Validation value qualifier Validation value	 Unique validation value is 1. 512 bit filtered hexadecimal digital signature of the AUTACK.

Annex B
(informative)

Security services and algorithms

B.1 Purpose and scope

This annex gives examples of possible combinations of data elements and code values from the security segment groups. These examples have been chosen to illustrate some widely used security techniques, based on International Standards.

The full set of possible combinations is far too large to be presented in this annex. The choices made here must not be considered as an endorsement of the algorithms or modes of operation. The user is invited to choose the techniques appropriate to the security threats he wants to be protected against.

The purpose of this annex is to provide the user, once he has chosen the security techniques, with a comprehensive starting point to work out a suitable solution for his particular application.

For easier reading and understanding the subject has been divided into three paragraphs, each of which concentrates on different basic principles for applying security.

The three sets are:

1. combinations using symmetric algorithms and AUTACK for referenced entities;

2. combinations using asymmetric algorithms and AUTACK for referenced entities;

3. combinations using AUTACK for acknowledgement.

List of codes used in the matrixes (subset of the complete code list)

0501	***Security service, coded***
1	Non-repudiation of origin
2	Message origin authentication
9	Referenced EDIFACT structure integrity

0505	***Filter function, coded***
6	UN/EDIFACT EDC filter

0523	***Use of algorithm, coded***
1	Owner hashing
2	Owner symmetric
3	Issuer signing (CA)
4	Issuer hashing (CA)
6	Owner signing

0527	***Algorithm, coded***
1	DES (Data Encryption Standard)
10	RSA (Rivest, Shamir, Adleman)
37	MAC (Message Authentication Code)
40	MDC2 (Modification Detection Code)
42	HDS2 (Hash functions)

0531	***Algorithm parameter qualifier***
12	Modulus
13	Exponent
14	Modulus length

0563	***Validation value qualifier***
1	Unique validation value

0577	***Security party qualifier***
1	Message sender
2	Message receiver
3	Certificate owner
4	Authenticating party

Abbreviations used

a, b, c, d	=	Representations of a Security Reference Number
CA	=	Certification Authority
Enc-Key	=	Encrypted Key
Hash	=	Hash value
Key-N	=	Key Name
MAC	=	Message authenticating code
Mod	=	Modulus
Mod-L	=	Length of Modulus
PK/CA	=	Public Key of Certification Authority
Pub-K	=	Public Key
Sig	=	Signature

B.2 Combinations using symmetric algorithms and AUTACK for referenced entities

The matrix given in Table B.1 establishes the relationships for the specific cases of

— referenced entity security provided by AUTACK message (ISO 9735-6);

— use of symmetric algorithm only;

— the security services provided are referenced EDIFACT structure origin authentication for the referenced message and message origin authentication for the AUTACK message. Referenced EDIFACT structure origin authentication is provided by the combination of referenced EDIFACT structure integrity and message origin authentication of the AUTACK;

— referenced EDIFACT structure integrity is provided by a hash function based on DES algorithm used in MDC mode, according to ISO/IEC 10118-2. There is no secret key to be shared between the sender and the receiver. The hash value is conveyed in the AUTACK and is protected by the security on the AUTACK message;

— message origin authentication for the AUTACK is provided by computing a MAC (Message Authentication Code) on the AUTACK message. In this example, the algorithm used is DES in CBC mode with a secret key which is known by the message receiver and is only referred to by a key name. This example complies to ISO 8731-1;

— although sender and receiver share keys, the cryptographic mechanisms have not been completely agreed beforehand. Therefore all the algorithms and mode of operation used are explicitly named;

— only the security fields related to security techniques, algorithms and modes of operation actually used are shown.

Table B.1 — Matrix of relationships when only symmetric algorithms are used

TAG	Name	S	R	Referenced EDIFACT structure integrity ISO/IEC 10118-2	AUTACK message origin authentication ISO 8731-1	Notes
SG 1		M	99	one per security service		
USH	SECURITY HEADER	M	1			
0501	SECURITY SERVICE, CODED	M	1	9	2	
0534	SECURITY REFERENCE NUMBER	M	1	a	b	1
0505	FILTER FUNCTION, CODED	C	1	6	6	
S500	SECURITY IDENTIFICATION DETAILS	C	2			
0577	Security party qualifier	M		1	1	2
0538	Key name	C			Key-N	3
S500	SECURITY IDENTIFICATION DETAILS	C	2			
0577	Security party qualifier	M		2	2	4
USA	SECURITY ALGORITHM	C	3			
S502	SECURITY ALGORITHM	M	1			
0523	Use of algorithm, coded	M		1	2	
0525	Cryptographic mode of operation, coded	C		—	—	
0527	Algorithm, coded	C		40	37	
USB	SECURED DATA IDENTIFICATION	M	1	reference to the secured data structures		
SG 3		M	9999			
USX	SECURITY REFERENCES	M	1			
USY	SECURITY ON REFERENCES	M	9			
0534	SECURITY REFERENCE NUMBER	M	1	a	—	5
S508	VALIDATION RESULT	C	2			
0563	Validation value qualifier	M		1		
0560	Validation value	C		Hash		6
SG 4		M	99			
UST	SECURITY TRAILER	M	1			
0534	SECURITY REFERENCE NUMBER	M	1	a	b	7
0588	NUMBER OF SECURITY SEGMENTS	M	1			
USR	SECURITY RESULT	C	1			
S508	VALIDATION RESULT	M	2			
0563	Validation value qualifier	M			1	
0560	Validation value	C			MAC	8

Notes:

1. One security header refers to the AUTACK security trailer and the other to the security on references segment.
2. Message sender
3. Name of the secret key shared by sender and receiver of the AUTACK.
4. Message receiver
5. Refers to one of the security headers.
6. Hash value computed on the referenced EDIFACT structure. It is protected by the MAC computed on the AUTACK message.
7. Refers to one of the security headers.
8. MAC computed on the AUTACK message.

B.3 Combinations using asymmetric keys and AUTACK for referenced entities

The matrix given in Table B.2 establishes the relationships for the specific cases of

— referenced entity security provided by AUTACK message (ISO 9735-6);

— the security services provided are referenced EDIFACT structure non-repudiation of origin and message non-repudiation of origin for the AUTACK message. Referenced EDIFACT structure non-repudiation of origin is provided by the combination of referenced EDIFACT structure integrity and non-repudiation of origin of the AUTACK;

— the asymmetric algorithm is RSA;

— the hash-function is DES algorithm in MDC mode. The same hash function is used to compute the hash value on the referenced EDIFACT structure and on the AUTACK message;

— certificates are assumed to not have been exchanged previously;

— the USC segment contains explicitly the identification of the hash function and the signature function used by the Certification Authority to sign the certificate. The public key of Certification Authority, needed to check the certificate signature is already known by the receiver. It is referred to by name in the USC segment;

— only one certificate is included, a second one would be necessary, only if a public key of the recipient were used.

Table B.2 — Matrix of relationships when asymmetric algorithms are used

TAG	Name	S	R	Referenced EDIFACT structure integrity ISO/IEC 10118-2	AUTACK message Non-repudiation of origin (RSA)	Notes
SG 1		M	99	one per security service		
USH	SECURITY HEADER	M	1			
0501	SECURITY SERVICE, CODED	M	1	9	1	1
0534	SECURITY REFERENCE NUMBER	M	1	c	d	
0505	FILTER FUNCTION, CODED	C	1	6	6	
S500	SECURITY IDENTIFICATION DETAILS	C	2			
0577	Security party qualifier	M		1	1	2
S500	SECURITY IDENTIFICATION DETAILS	C	2			
0577	Security party qualifier	M		2	2	3
USA	SECURITY ALGORITHM	C	3			
S502	SECURITY ALGORITHM	M	1			
0523	Use of algorithm, coded	M		1	1	4
0525	Cryptographic mode of operation, coded	C		—	—	
0527	Algorithm, coded	C		40	40	
SG 2		C	2		only one: sender certificate	
USC	CERTIFICATE	M	1			
0536	CERTIFICATE REFERENCE	C	1		reference of this certificate	

TAG	Name	S	R	Referenced EDIFACT structure integrity ISO/IEC 10118-2	AUTACK message Non-repudiation of origin (RSA)	Notes
S500	SECURITY IDENTIFICATION DETAILS	C	2		(certificate owner)	
0577	Security party qualifier	M			3	5
S500	SECURITY IDENTIFICATION DETAILS	C	2		(authenticating party)	
0577	Security party qualifier	M			4	6
0538	Key name	C			(PK/CA name)	
USA	SECURITY ALGORITHM	C	3		(sender's signature function)	
S502	SECURITY ALGORITHM	M	1			
0523	Use of algorithm, coded	M			6	7
0527	Algorithm, coded	C			10	
S503	ALGORITHM PARAMETER	C	9		(length of modulus)	
0531	Algorithm parameter qualifier	M			14	
0554	Algorithm parameter value	M			Mod-L	
S503	ALGORITHM PARAMETER	C	9		(modulus)	
0531	Algorithm parameter qualifier	M			12	
0554	Algorithm parameter value	M			Mod	
S503	ALGORITHM PARAMETER	C	9		(public exponent)	
0531	Algorithm parameter qualifier	M			13	
0554	Algorithm parameter value	M			Pub-K	
USA	SECURITY ALGORITHM	C	3		(CA's hash function for certificate's signature)	
S502	SECURITY ALGORITHM	M	1			
0523	Use of algorithm, coded	M			4	8
0525	Cryptographic mode of operation, coded	C			—	
0527	Algorithm, coded	C			42	
USA	SECURITY ALGORITHM	C	3		(CA's signature function for certificate's signature)	
S502	SECURITY ALGORITHM	M	1			
0523	Use of algorithm, coded	M			3	9
0527	Algorithm, coded	C			10	
USR	SECURITY RESULT	C	1			
S508	VALIDATION RESULT	M	2			11
0563	Validation value qualifier	M			1	
0560	Validation value	C			Sig	
USB	SECURED DATA IDENTIFICATION	M	1	reference to the secured data structures		
SG 3		M	9999			

TAG	Name	S	R	Referenced EDIFACT structure integrity ISO/IEC 10118-2	AUTACK message Non-repudiation of origin (RSA)	Notes
USX	SECURITY REFERENCES	M	1			
USY	SECURITY ON REFERENCES	M	9			
0534	SECURITY REFERENCE NUMBER	M	1	c	—	
S508	VALIDATION RESULT	C	2			11
0563	Validation value qualifier	M		1	—	
0560	Validation value	C		Hash	—	
SG 4		M	99			
UST	SECURITY TRAILER	M	1			
0534	SECURITY REFERENCE NUMBER	M	1	c	d	
0588	NUMBER OF SECURITY SEGMENTS	M	1			
USR	SECURITY RESULT	C	1			
S508	VALIDATION RESULT	M	2			11
0563	Validation value qualifier	M			1	
0560	Validation value	C		—	Sig	

Notes:

1. Message origin authentication and Integrity for AUTACK are assumed to be included in the Non-repudiation of origin. Referenced EDIFACT structure non-repudiation of origin is provided by the combination of referenced EDIFACT structure integrity and AUTACK non-repudiation of origin.
2. Message sender
3. Message receiver
4. Hash function applied by the sender on the secured structure.
6. Certificate owner: identification details should be the same as in USH S500 for the message sender.
7. Authenticating party: Certification Authority (CA)
8. Sender's signature function
9. CA's hash function
10. CA's signature function
11. Some signature algorithms (for instance DSA) require two result parameters.

B.4 Combinations using AUTACK for acknowledgements

The combinations possible for acknowledgement AUTACKs follow the above described cases.

In particular:

— for USH 0501 code 6 (receipt authentication), the combinations of matrix 1 apply;

— for USH 0501 code 5 (non-repudiation of receipt), the combinations of matrix 2 apply.

Further code combinations are possible and required.

Bibliography

[1] ISO 8731-1:1987, *Banking — Approved algorithms for message authentication — Part 1: DEA*

[2] ISO/IEC 10118-2:2000, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using a n-bit block cipher*

ICS 35.240.60

Price based on 28 pages