

INTERNATIONAL STANDARD

ISO
9735-6

First edition
1999-04-01

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

Part 6:

Secure authentication and acknowledgement
message (message type - AUTACK)

*Échange de données informatisées pour l'administration, le commerce et le
transport (EDIFACT) — Règles de syntaxe au niveau de l'application
(Numéro de version de syntaxe: 4) —*

*Partie 6: Message de sécurité pour l'authentification et la connaissance
(type de message AUTACK)*



Reference number
ISO 9735-6:1999(E)

Contents

	Page
1 Scope	1
2 Conformance	1
3 Normative references	1
4 Definitions	2
5 Rules for the use of the secure authentication and acknowledgement message	2
Annex A: Syntax service directories (segments, composite data elements and simple data elements)	7
Annex B: Service code directory	12
Annex C: AUTACK message examples	13
Annex D: Security services and algorithms	23
Annex E: Bibliography	30

STANDARDSISO.COM : Click to view the full PDF of ISO 9735-6:1999

© ISO 1999

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch
Printed in Switzerland

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.

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.

This part of ISO 9735 was prepared by the UN/ECE Trade Division (as UN/EDIFACT) and was adopted, under a special "fast-track procedure", by Technical Committee ISO/TC 154, *Documents and data elements in administration, commerce and industry*.

Whereas this part supersedes the earlier publications, and shall use a version number of "4" in the mandatory data element 0002 (Syntax version number) 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 (amended and reprinted in 1990) plus Amendment 1:1992 — *Syntax version number: 3*

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)*:

- *Part 1: Syntax rules common to all parts, together with the syntax service directories for each of the 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 - CTRL)*
- *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)*

Further parts may be added in the future.

Annex A forms an integral part of this part of ISO 9735. Annexes B to E are for information only.

STANDARDSISO.COM : Click to view the full PDF of ISO 9735-6:1999

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.

STANDARDSISO.COM : Click to view the PDF or ISO 9735-6:1999

STANDARDSISO.COM : Click to view the full PDF of ISO 9735-6:1999

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

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

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 Part 1, Part 2 and Part 5 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 standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 9735. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 9735 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 9735-1:1998, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules — Part 1: Syntax rules common to all parts, together with syntax directories for each of the parts*.

ISO 9735-2:1998, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) — Part 2: Syntax rules specific to batch EDI*.

ISO 9735-5:1998, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) — Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*.

4 Definitions

For the purposes of this part of ISO 9735, the definitions in ISO 9735-1:1988, annex A and in ISO 9735-5:1998, annex A 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

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.

5.3.1 Use of AUTACK for the authentication function

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 Part 5 of ISO 9735, 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.

5.3.1.1 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.

5.3.1.2 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.

5.3.2 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 Part 5 of ISO 9735) 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.

Note: 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 Part 5 of ISO 9735).

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 Part 5 of ISO 9735).

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 Part 5 of ISO 9735.

In an AUTACK message, there are four possible scopes of security application:

- the first two scopes are as defined in Part 5 of ISO 9735 section 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 Part 5 of ISO 9735).

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 Part 5 of ISO 9735).

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 Part 5 of ISO 9735).

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 Part 5 of ISO 9735).

0080 USR, Security result

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

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 Part 5 of ISO 9735).

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 Part 5 of ISO 9735).

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 Part 5 of ISO 9735). 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

5.4.2.1 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.

STANDARDSISO.COM : Click to view the full PDF of ISO 9735-6:1999

Annex A (normative)

Addendum — to be added to Part 1 annex C when approved

Syntax service directories (segments, composite data elements and simple data elements)

A.1 Segment directory

A.1.1 Segment specification legend:

Function	The function of the segment
POS	The sequential position number of the stand-alone data element or composite data element in the segment table
TAG	The tags for all service segments contained in the segment directory start with the letter "U". The tags of all service composite data elements start with the letter "S", and the tags of all service simple data elements start with the figure "0"
Name	Name of a COMPOSITE DATA ELEMENT in capital letters Name of a STAND-ALONE DATA ELEMENT in capital letters Name of a component data element in small letters
S	The status of the stand-alone data element or composite data element in the segment, or of the components in the composite (where M = Mandatory and C = Conditional)
R	The maximum number of occurrences of a stand-alone data element or composite data element in the segment
Repr.	Data value representation of the stand-alone data element or component data elements in the composite. a alphabetic characters n numeric characters an alphanumeric characters a3 3 alphabetic characters, fixed length n3 3 numeric characters, fixed length an3 3 alphanumeric characters, fixed length a..3 up to 3 alphabetic characters n..3 up to 3 numeric characters an..3 up to 3 alphanumeric characters

A.1.2 Dependency note identifiers

Code	Name
D1	One and only one
D2	All or none
D3	One or more
D4	One or none
D5	If first, then all
D6	If first, then at least one more
D7	If first, then none of the others

See clause 11.5 in ISO 9735-1:1998 for the definition of the dependency note identifiers.

A.1.3 Index of segments by tag

TAG	Name
UNH	Message header
UNT	Message trailer
USA	Security algorithm
USB	Secured data identification
USC	Certificate
USH	Security header
USR	Security result
UST	Security trailer
USX	Security references
USY	Security on references

A.1.4 Index of segments by name

TAG	Name
USC	Certificate
UNH	Message header
UNT	Message trailer
USB	Secured data identification
USA	Security algorithm
USH	Security header
USY	Security on references
USX	Security references
USR	Security result
UST	Security trailer

A.1.5 Segment specifications

Note:

Only segments not defined in other parts of ISO 9735 are included here.

USB SECURED DATA IDENTIFICATION

Function: To contain details related to the AUTACK.

POS	TAG	Name	S	R	Repr.	Notes
010	0503	RESPONSE TYPE, CODED		M	1	an..3
020	S501	SECURITY DATE AND TIME		C	1	
	0517	Date and time qualifier		M		an..3
	0338	Event date		C		n..8
	0314	Event time		C		an..15
	0336	Time offset		C		n4
030	S002	INTERCHANGE SENDER		M	1	
	0004	Interchange sender identification		M		an..35
	0007	Identification code qualifier		C		an..4
	0008	Interchange sender internal identification		C		an..35
	0042	Interchange sender internal sub-identification		C		an..35

040	S003	INTERCHANGE RECIPIENT	M 1	
0010		Interchange recipient identification	M	an..35
0007		Identification code qualifier	C	an..4
0014		Interchange recipient internal identification	C	an..35
0046		Interchange recipient internal sub-identification	C	an..35

USX SECURITY REFERENCES

Function: To refer to the secured EDIFACT structure and its associated date and time.

POS	TAG	Name	S R	Repr.	Notes
010	0020	INTERCHANGE CONTROL REFERENCE	M 1		an..14
020	S002	INTERCHANGE SENDER	C 1		
	0004	Interchange sender identification	M	an..35	
	0007	Identification code qualifier	C	an..4	
	0008	Interchange sender internal identification	C	an..35	
	0042	Interchange sender internal sub-identification	C	an..35	
030	S003	INTERCHANGE RECIPIENT	C 1		
	0010	Interchange recipient identification	M	an..35	
	0007	Identification code qualifier	C	an..4	
	0014	Interchange recipient internal identification	C	an..35	
	0046	Interchange recipient internal sub-identification	C	an..35	
040	0048	GROUP REFERENCE NUMBER	C 1	an..14	1,3
050	S006	APPLICATION SENDER IDENTIFICATION	C 1		1
	0040	Application sender identification	M	an..35	
	0007	Identification code qualifier	C	an..4	
060	S007	APPLICATION RECIPIENT IDENTIFICATION	C 1		3
	0044	Application recipient identification	M	an..35	
	0007	Identification code qualifier	C	an..4	
070	0062	MESSAGE REFERENCE NUMBER	C 1	an..14	2,4
080	S009	MESSAGE IDENTIFIER	C 1		4
	0065	Message type	M	an..6	
	0052	Message version number	M	an..3	
	0054	Message release number	M	an..3	
	0051	Controlling agency, coded	M	an..3	
	0057	Association assigned code	C	an..6	
	0110	Code list directory version number	C	an..6	
	0113	Message type sub-function identification	C	an..6	
090	0800	PACKAGE REFERENCE NUMBER	C 1	an..14	2
100	S501	SECURITY DATE AND TIME	C 1		
	0517	Date and time qualifier	M	an..3	
	0338	Event date	C	n..8	
	0314	Event time	C	an..15	
	0336	Time offset	C	n4	

DEPENDENCY NOTES:

1. D5 (050, 040) If first, then all
2. D1 (070, 090) One and only one
3. D5 (060, 040) If first, then all
4. D5 (080, 070) If first, then all

USY SECURITY ON REFERENCES

Function: To identify the applicable header, and to contain the security result and/or to indicate the possible cause of security rejection for the referred value.

POS	TAG	Name	S	R	Repr.	Notes
010	0534	SECURITY REFERENCE NUMBER	M	1	an..14	
020	S508	VALIDATION RESULT	C	2		1
	0563	Validation value qualifier	M		an..3	
	0560	Validation value	C		an..512	
030	0571	SECURITY ERROR, CODED	C	1	an..3	1

NOTES:

1. D3 (020, 030) One or more

A.2 Composite data element directory

No composite data elements are defined.

A.3 Simple data element directory**A.3.1 Simple data element specification legend:**

The tags of all service simple data elements contained in the simple data element directory start with the figure "0".

Name	Name of a simple data element
Desc.	Description of the simple data element
Repr.	Data value representation of the simple data element:
	a alphabetic characters
	n numeric characters
	an alphanumeric characters
	a3 3 alphabetic characters, fixed length
	n3 3 numeric characters, fixed length
	an3 3 alphanumeric characters, fixed length
	a..3 up to 3 alphabetic characters
	n..3 up to 3 numeric characters
	an..3 up to 3 alphanumeric characters
Notes	Simple data element note number(s)

A.3.2 Index of simple data elements by tag

TAG	Name
0020	Interchange control reference
0048	Group reference number
0062	Message reference number
0503	Response type, coded
0534	Security reference number
0571	Security error, coded
0800	Package reference number

A.3.3 Index of simple data elements by name

TAG	Name
0048	Group reference number
0020	Interchange control reference
0062	Message reference number
0800	Package reference number
0503	Response type, coded
0571	Security error, coded
0534	Security reference number

A.3.4 Simple data element specifications

Note:

Only simple data elements not defined in other parts of ISO 9735 are included here.

0571 SECURITY ERROR, CODED

Desc: Identifies the security error causing the rejection of the EDIFACT structure.

Repr: an..3

Note 1: This element shall specify the security error encountered. These may be the reason for non-acknowledgement by a request for secure acknowledgement, or may be sent on the initiative of the receiver of an AUTACK or secured EDIFACT structure which contains error.

Annex B (informative)

Service code directory

The service code directory is maintained by the UN/ECE and is part of the UN Trade Data Interchange Directory (UNTDID) and as such is not reproduced in this International Standard. The most recent version of the service code directory should be used to reference the code values for the coded data elements in the simple data element directory (see annex C within this part). The UNTDID is updated and published at regular intervals.

STANDARDSISO.COM : Click to view the full PDF of ISO 9735-6:1999

Annex C (informative)

AUTACK message examples

Three examples are provided herein 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 an other 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.

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

C.1.1 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-USR, the certificate of Mr. Smith.
- USB
- USX-USY with the security references and results (for PAYORD message).
- UST, without USR, referencing the USH.

C.1.2 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 Certificate owner	Mr. SMITH of Company A

SECURITY IDENTIFICATION DETAILS	
Certificate issuer	Mr. SMITH's certificate was generated by a certification Authority called: AUTHORITY.
Key name	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 used when signature was computed
Service character for signature qualifier	Service character is segment terminator.
Service character for signature	Value "" (apostrophe).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is data element separator.
Service character for signature	Value "+" (plus sign).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is component data element separator.
Service character for signature	Value ":" (colon).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is repetition separator.
Service character for signature	Value "*" (asterisk).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is release character.
Service character for signature	Value "?" (question mark).
SECURITY DATE AND TIME	Certificate generation time
Date and time	Mr. SMITH's certificate was generated on 931215 at 14:12:00
SECURITY DATE AND TIME	Certificate start of validity period
Date and time	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 Cryptographic mode of operation Algorithm	An issuer hashing algorithm is used. 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 MD5 message-digest algorithm is used
SECURITY ALGORITHM	Asymmetric algorithm used by AUTHORITY to sign
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	An issuer 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. AUTHORITY's public key.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	Identifies this algorithm parameter as a Modulus for signature verification. AUTHORITY's modulus.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	Identifies this algorithm parameter as the length of AUTHORITY's modulus (in bits). AUTHORITY's modulus is 512 bits long.
SECURITY RESULT	Digital signature of the certificate
VALIDATION RESULT Validation value qualifier Validation value	Digital signature 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	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	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	Digital Signature (of the PAYORD message). 512 bit filtered hexadecimal Digital signature
SECURITY TRAILER	
SECURITY REFERENCE NUMBER	The reference of this security trailer is 1
NUMBER OF SECURITY SEGMENTS	The number of security segments is 7

C.2 Example 2: Securing several messages with AUTACK.

C.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. 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-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.

C.2.2 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	The message was coded in ASCII 8 bits when its
ENCODING	signature was generated.
SECURITY IDENTIFICATION DETAILS	
Message sender	Mr. Smith from Company A
SECURITY IDENTIFICATION DETAILS	
Message receiver	Bank A
CERTIFICATE	certificate of Mr. SMITH
CERTIFICATE REFERENCE	This certificate is referenced, by AUTHORITY: 00000001.
SECURITY IDENTIFICATION DETAILS	
Certificate owner	Mr. SMITH of Company A

SECURITY IDENTIFICATION DETAILS	
Certificate issuer	Mr. SMITH's certificate was generated by a certification Authority called: AUTHORITY.
Key name	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 used when signature was computed
Service character for signature qualifier	Service character is segment terminator.
Service character for signature	Value "" (apostrophe).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is data element separator.
Service character for signature	Value "+" (plus sign).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is component data element separator.
Service character for signature	Value ":" (colon).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is repetition separator.
Service character for signature	Value "*" (asterisk).
SERVICE CHARACTER FOR SIGNATURE	Service character used when signature was computed
Service character for signature qualifier	Service character is release character.
Service character for signature	Value "?" (question mark).
SECURITY DATE AND TIME	Certificate generation time
Date and time	Mr. SMITH's certificate was generated on 931215 at 14:12:00
SECURITY DATE AND TIME	Certificate start of validity period
Date and time	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 Cryptographic mode of operation Algorithm	An issuer hashing algorithm is used. 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 MD5 message-digest algorithm is used
SECURITY ALGORITHM	Asymmetric algorithm used by AUTHORITY to sign
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	An issuer 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. AUTHORITY's public key.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	Identifies this algorithm parameter as a Modulus for signature verification. AUTHORITY's modulus.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	Identifies this algorithm parameter as the length of AUTHORITY's modulus (in bits). AUTHORITY's modulus is 512 bits long.
SECURITY RESULT	Digital signature of the certificate
VALIDATION RESULT Validation value qualifier Validation value	Digital signature 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 Message sender	Mr. Smith from Company A
SECURITY IDENTIFICATION DETAILS 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.
SECURED DATA IDENTIFICATION	
RESPONSE TYPE, CODED	No acknowledgement from the Bank A is required
SECURITY DATE AND 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	Identifies the sender of the interchange of the message PAYORD: Mr. Smith from Company A.
INTERCHANGE RECIPIENT	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	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).
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	Identifies the sender of the interchange of the message PAYORD: Mr. Smith from Company A.
INTERCHANGE RECIPIENT	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	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	Digital Signature (of the first PAYORD message). 512 bit filtered hexadecimal Digital signature
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

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

C.3.1 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.

C.3.2 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 Message sender (party which generates the Digital Signature).	Bank A
SECURITY IDENTIFICATION DETAILS 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	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 Certificate owner	Bank A
SECURITY IDENTIFICATION DETAILS Certificate issuer	Bank A's certificate was generated by a certification Authority called: AUTHORITY.
Key name	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 Algorithm parameter value	Identifies this algorithm parameter as a Modulus for signature verification. Bank A's modulus.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	Identifies this algorithm parameter as the length of Bank A's modulus (in bits). 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 Cryptographic mode of operation Algorithm	An issuer hashing algorithm is used. 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 MD5 message-digest algorithm is used
SECURITY ALGORITHM	Asymmetric algorithm used by AUTHORITY to sign
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	An issuer 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. AUTHORITY's public key.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	Identifies this algorithm parameter as a Modulus for signature verification. AUTHORITY's modulus.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	Identifies this algorithm parameter as the length of AUTHORITY's modulus (in bits). AUTHORITY's modulus is 512 bits long.
SECURITY RESULT	Digital signature of the certificate
VALIDATION RESULT Validation value qualifier Validation value	Digital signature 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	Digital Signature of the PAYORD acknowledged. 512 bit filtered hexadecimal digital signature
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	Digital Signature of the AUTACK. 512 bit filtered hexadecimal Digital signature

Annex D (informative) Security services and algorithms

D.1 Purpose and scope

Annex D 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 two 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	0505	Filter function, coded
1	Non-repudiation of origin	6	UN/EDIFACT EDC filter
2	Message origin authentication		
9	Referenced EDIFACT structure integrity		
0523	Use of algorithm, coded	0525	Cryptographic mode of operation, coded
1	Owner hashing	6	MAC (Message Authentication Code)
2	Owner symmetric	9	MDC2 (Modification Detection Code)
3	Issuer signing (CA)	11	HDS2 (Hash functions)
4	Issuer hashing (CA)		
6	Owner signing		
0527	Algorithm, coded	0531	Algorithm parameter qualifier
1	DES (Data Encryption Standard)	12	Modulus
10	RSA (Rivest, Shamir, Adleman)	13	Exponent
		14	Modulus length
0563	Validation value qualifier	0577	Security party qualifier
1	Unique validation value	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

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

The following matrix 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 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.