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)*

# Contents







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 - 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)*

*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.

## 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) —

# 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.