

Australian Standard™

**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**



Standards Australia



Documents

Document Sharing Hub

This Australian Standard was prepared by Committee IT-001, Information systems—Interconnection. It was approved on behalf of the Council of Standards Australia on 30 March 2003 and published on 14 May 2003.

The following are represented on Committee IT-001:

- Australian Bureau of Statistics
- Australian Communications Industry Forum
- Australian Information Industry Association
- Australian Telecommunications Users Group
- Australian Vice-Chancellors' Committee
- Electrical Compliance Testing Association
- Information Technology Association of New Zealand

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 03044.

Australian Standard™

**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**

First published as AS ISO 9735.6—2003.

COPYRIGHT

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5205 5

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-001, Information systems—Interconnection. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian, rather than an Australian/New Zealand Standard.

This Standard is identical with, and has been reproduced from, ISO 9735-6:2002, *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*.

The objective of this Standard is to specify syntax rules for EDIFACT security and to provide a method to address message/package level, group level and interchange level security for authenticity, integrity and non-repudiation of origin, in accordance with established security mechanisms.

This Standard is Part 6 of AS ISO 9735—2003, *Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number: 4, Syntax release number: 1)*, which is published in parts as follows:

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 (this Standard)

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

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

As this Standard is reproduced from an international standard, the following applies:

- (a) Its number appears on the cover and title page while the international standard number appears only on the cover.
- (b) In the source text ‘this International Standard’ should read ‘this Australian Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>		<i>Australian Standard</i>	
ISO		AS ISO	
9735	Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number: 4, Syntax release number: 1)	9735	Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number: 4, Syntax release number: 1)
9735-1	Part 1: Syntax rules common to all parts	9735.1	Part 1: Syntax rules common to all parts

ISO		AS ISO	
9735-2	Part 2: Syntax rules specific to batch EDI	9735.2	Part 2: Syntax rules specific to batch EDI
9735-5	Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)	9735.5	Part 5: Security rules for batch EDI—authenticity, integrity and non-repudiation of origin
9735-10	Part 10: Syntax service directories	9735.10	Part 10: Syntax service directories

CONTENTS

	<i>Page</i>
1 Scope	1
2 Conformance.....	1
3 Normative references	2
4 Terms and definitions	2
5 Rules for the use of the secure authentication and acknowledgement message.....	2
Annex A (informative) AUTACK message examples	9
Annex B (informative) Security services and algorithms	22
Bibliography	28

AUSTRALIAN STANDARD

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.

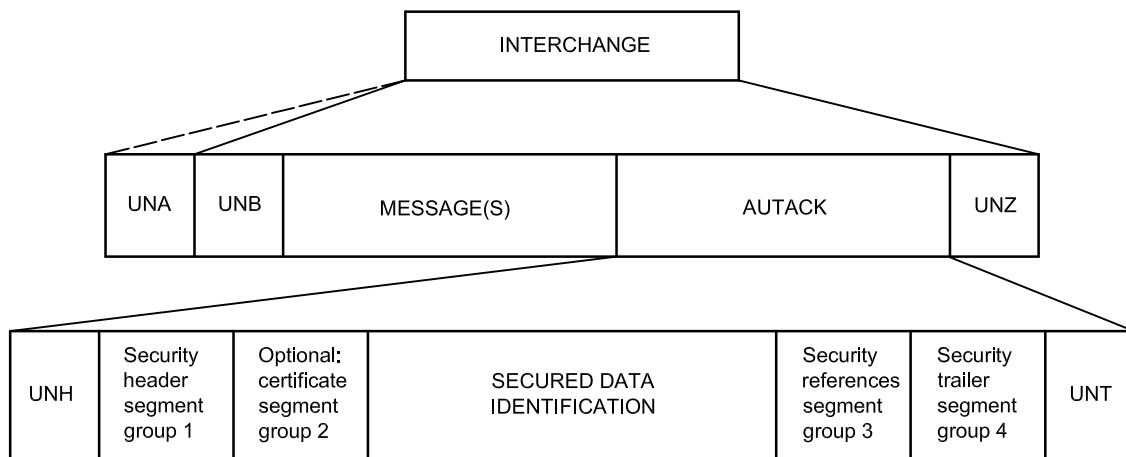


Figure 1 — Interchange showing security by using the AUTACK message at message level (schematic)

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.