AUTACK

Secure authentication and acknowledgement message

Edition 2016

1. Introduction ................................................................................................................................. 2
2. Message Structure Chart ........................................................................................................... 3
3. Branching Diagram .................................................................................................................... 4
4. Segments Description ................................................................................................................ 5
5. Segments Layout ....................................................................................................................... 6
6. Example(s) .................................................................................................................................. 24
1. Introduction

Status

MESSAGE TYPE : AUTACK
REFERENCE DIRECTORY : D.01B
EANCOM® SUBSET VERSION : 001

Definition

The service message AUTACK (Secure Authentication and Acknowledgement Message) enables the transmission of integrity and authenticity data for referenced data. The message is used to transport the digital signature and the related information needed by the recipient to verify the digital signature.

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.

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). 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 to the cryptographic methods used, the reference numbers for the EDIFACT structures and the date and time of the original structures.

The AUTACK message can apply to one or more messages, packages or groups from one or more interchanges.

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 provided by electronic signatures, i.e., authenticity, integrity, and non-repudiation of origin of its associated EDIFACT structures.
## 2. Message Structure Chart

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNH</td>
<td>1 M 1</td>
<td>Message header</td>
<td></td>
</tr>
<tr>
<td>SG1</td>
<td>M 99</td>
<td>USH-USA-SG2</td>
<td></td>
</tr>
<tr>
<td>USH</td>
<td>2 M 1</td>
<td>Security header</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>3 C 3</td>
<td>Security algorithm</td>
<td></td>
</tr>
<tr>
<td>SG2</td>
<td>C 2</td>
<td>USC-USA</td>
<td></td>
</tr>
<tr>
<td>USC</td>
<td>4 M 1</td>
<td>Certificate</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>5 C 3</td>
<td>Security algorithm</td>
<td></td>
</tr>
<tr>
<td>USB</td>
<td>6 M 1</td>
<td>Secured data identification</td>
<td></td>
</tr>
<tr>
<td>SG3</td>
<td>M 9999</td>
<td>USX-USY</td>
<td></td>
</tr>
<tr>
<td>USX</td>
<td>7 M 1</td>
<td>Security references</td>
<td></td>
</tr>
<tr>
<td>USY</td>
<td>8 M 9</td>
<td>Security on references</td>
<td></td>
</tr>
<tr>
<td>SG4</td>
<td>M 99</td>
<td>UST</td>
<td></td>
</tr>
<tr>
<td>UST</td>
<td>9 M 1</td>
<td>Security trailer</td>
<td></td>
</tr>
<tr>
<td>UNT</td>
<td>10 M 1</td>
<td>Message trailer</td>
<td></td>
</tr>
</tbody>
</table>
3. Branching Diagram
4. Segments Description

UNH - M 1 - Message header
This segment is used to head, identify and specify a message.

SG1 - M 99 - USH-USA-SG2
A group of segments identifying the security service and security mechanisms applied and containing the data necessary to carry out the validation calculations. This segment group shall specify the security service and algorithm(s) applied to the referenced EDIFACT structure. Each security header group shall be linked to a security trailer group, and additionally linked to the USY segment(s).

USH - M 1 - Security header
A segment specifying a security service applied to the referenced EDIFACT structure.

USA - C 3 - Security algorithm
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the hash value.

SG2 - C 2 - USC-USA
A group of segments containing the data necessary to validate the security methods applied.

USC - M 1 - Certificate
This segment either contains information regarding the certificate, and identifies the certification authority which has generated the certificate, or is used to identify bilaterally interchanged signature keys.

USA - C 3 - Security algorithm
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the digital signature.

USB - M 1 - Secured data identification
This segment shall contain identification of the interchange sender and interchange recipient.

SG3 - M 9999 - USX-USY
This segment group shall be used to identify a party in the security process and to give security information for the referenced EDIFACT structure.

USX - M 1 - Security references
This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.

USY - M 9 - Security on references
This segment contains a link to the security header group and the result of the security services applied to the referenced EDIFACT structure (i.e., the digital signature) as specified in this linked security header group.

SG4 - M 99 - UST
A group of segments containing a link with security header segment group and the result of the security services applied to the message/package.

UST - M 1 - Security trailer
A segment establishing a link between security header and security trailer segment group, and stating the number of security segments in these groups.

UNT - M 1 - Message trailer
A service segment ending a message, giving the total number of segments and the control reference number of the message.
5. Segments Layout

This section describes each segment used in the EANCOM® AUTACK message. The original EDIFACT segment layout is listed. The appropriate comments relevant to the EANCOM® subset are indicated.

Notes:

1. The segments are presented in the sequence in which they appear in the message. The segment or segment group tag is followed by the (M)andatory / (C)onditional indicator, the maximum number of occurrences and the segment description.

2. Reading from left to right, in column one, the data element tags and descriptions are shown, followed by in the second column the EDIFACT status (M or C), the field format, and the picture of the data elements. These first pieces of information constitute the original EDIFACT segment layout.

Following the EDIFACT information, EANCOM® specific information is provided in the third, fourth, and fifth columns. In the third column a status indicator for the use of (C)onditional EDIFACT data elements (see 2.1 through 2.3 below), in the fourth column the restricted indicator (see point 3 on the following page), and in the fifth column notes and code values used for specific data elements in the message.

2.1 (M)andatory data elements in EDIFACT segments retain their status in EANCOM®.

2.2 Additionally, there are five types of status for data elements with a (C)onditional EDIFACT status, whether for simple, component or composite data elements. These are listed below and can be identified when relevant by the following abbreviations:

- REQUIRED R Indicates that the entity is required and must be sent.
- ADVISED A Indicates that the entity is advised or recommended.
- DEPENDENT D Indicates that the entity must be sent in certain conditions, as defined by the relevant explanatory note.
- OPTIONAL O Indicates that the entity is optional and may be sent at the discretion of the user.
- NOT USED N Indicates that the entity is not used and should be omitted.

2.3 If a composite is flagged as N, NOT USED, all data elements within that composite will have blank status indicators assigned to them.

3. Status indicators detailed in the fourth column which directly relate to the code values detailed in the fifth column may have two values:

- RESTRICTED * A data element marked with an asterisk (*) in the fourth column indicates that the listed codes in column five are the only codes available for use with this data element, in this segment, in this message.
- OPEN All data elements where coded representation of data is possible and a restricted set of code values is not indicated are open (no asterisk in fourth column). The available codes are listed in the EANCOM® Data Elements and Code Sets Directory. Code values may be given as examples or there may be a note on the format or type of code to be used.

4. Different colours are used for the code values in the segment details: restricted codes are in red and open codes in blue.
## 5. Segments Layout

### Segment number: 1

<table>
<thead>
<tr>
<th>UNH</th>
<th>-M</th>
<th>1 - Message header</th>
</tr>
</thead>
</table>

**Function:**

To head, identify and specify a message.

**Notes:**

1. Data element S009/S057 is retained for upward compatibility. The use of S016 and/or S017 is encouraged in preference.
2. The combination of the values carried in data elements 0062 and S009 shall be used to identify uniquely the message within its group (if used) or if not used, within its interchange, for the purpose of acknowledgement.

### Table: Message Header

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0062 Message reference number</td>
<td>M an..14</td>
<td>M</td>
</tr>
<tr>
<td>S009 MESSAGE IDENTIFIER</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>0065 Message type</td>
<td>M an..6</td>
<td>M *</td>
</tr>
<tr>
<td>0052 Message version number</td>
<td>M an..3</td>
<td>M *</td>
</tr>
<tr>
<td>0054 Message release number</td>
<td>M an..3</td>
<td>M *</td>
</tr>
<tr>
<td>0051 Controlling agency, coded</td>
<td>M an..3</td>
<td>M *</td>
</tr>
<tr>
<td>0057 Association assigned code</td>
<td>C an..6</td>
<td>R *</td>
</tr>
<tr>
<td>0110 Code list directory version number</td>
<td>C an..6</td>
<td>O</td>
</tr>
<tr>
<td>0113 Message type sub-function identification</td>
<td>C an..6</td>
<td>N</td>
</tr>
<tr>
<td>0068 Common access reference</td>
<td>C an..35</td>
<td>N</td>
</tr>
<tr>
<td>S010 STATUS OF THE TRANSFER</td>
<td>C</td>
<td>N</td>
</tr>
<tr>
<td>0070 Sequence of transfers</td>
<td>M n..2</td>
<td></td>
</tr>
<tr>
<td>0073 First and last transfer</td>
<td>C a1</td>
<td></td>
</tr>
<tr>
<td>S016 MESSAGE SUBSET IDENTIFICATION</td>
<td>C</td>
<td>N</td>
</tr>
<tr>
<td>0115 Message subset identification</td>
<td>M an..14</td>
<td></td>
</tr>
<tr>
<td>0116 Message subset version number</td>
<td>C an..3</td>
<td></td>
</tr>
<tr>
<td>0118 Message subset release number</td>
<td>C an..3</td>
<td></td>
</tr>
<tr>
<td>0051 Controlling agency, coded</td>
<td>C an..3</td>
<td></td>
</tr>
<tr>
<td>S017 MESSAGE IMPLEMENTATION GUIDELINE IDENTIFICATION</td>
<td>C</td>
<td>N</td>
</tr>
<tr>
<td>0121 Message implementation guideline identification</td>
<td>M an..14</td>
<td></td>
</tr>
<tr>
<td>0122 Message implementation guideline version number</td>
<td>C an..3</td>
<td></td>
</tr>
<tr>
<td>0124 Message implementation</td>
<td>C an..3</td>
<td></td>
</tr>
</tbody>
</table>

*EDIFACT = Secure authentication and acknowledgement message*

*GS1 = Service message, version 4*

*UN = UN/CEFACT*

*EAN001 = GS1 version control number (GS1 Permanent Code)*

This data element can be used to identify the codelist agreed by the interchange partners, e.g. EAN001 = EANCOM 2002 S4 codelist released on 01.12.2001 by GS1.
## 5. Segments Layout

<table>
<thead>
<tr>
<th>Segment number:</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EDIFACT</td>
</tr>
<tr>
<td>guideline release number</td>
<td></td>
</tr>
<tr>
<td>0051</td>
<td>Controlling agency, coded</td>
</tr>
<tr>
<td>S018</td>
<td>SCENARIO IDENTIFICATION</td>
</tr>
<tr>
<td>0127</td>
<td>Scenario identification</td>
</tr>
<tr>
<td>0128</td>
<td>Scenario version number</td>
</tr>
<tr>
<td>0130</td>
<td>Scenario release number</td>
</tr>
<tr>
<td>0051</td>
<td>Controlling agency, coded</td>
</tr>
</tbody>
</table>

**Segment Notes:**

This segment is used to head, identify and specify a message.

DE's 0065, 0052, 0054, and 0051: Indicate that the message is an UNSM AUTACK under the control of the United Nations.

Example:

UNH+AUT00001+AUTACK:4:1:UN:EAN001'
5. Segments Layout

Segment number: 2

| SG1   | - M | 99 - USH-USA-SG2 |
| USH   | - M | 1 - Security header |

Function:
To specify a security mechanism applied to a EDIFACT structure (i.e.: either message/package, group or interchange).

Notes:
1. 0541, if not present the default scope is the current security header segment group and the message body or object itself.
2. 0507, the original character set encoding of the EDIFACT structure when it was secured. If no value is specified, the character set encoding corresponds to that identified by the syntax identifier character repertoire in the UNB segment.
3. S500, two occurrences are possible: one for the security originator, one for the security recipient.
4. S500/0538, may be used to establish the key relationship between the sending and receiving parties.
5. S501, may be used as a security timestamp. It is security related and may differ from any dates and times that may appear elsewhere in the EDIFACT structure. It may be used to provide sequence integrity.

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>*</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0501</td>
<td>Security service, coded</td>
<td>M an..3</td>
<td>M *</td>
</tr>
<tr>
<td>0534</td>
<td>Security reference number</td>
<td>M an..14</td>
<td>M</td>
</tr>
<tr>
<td>0541</td>
<td>Scope of security application, coded</td>
<td>C an..3</td>
<td>R *</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specification of the scope of application of the security service defined in the security header.</td>
</tr>
<tr>
<td>0503</td>
<td>Response type, coded</td>
<td>C an..3</td>
<td>N</td>
</tr>
<tr>
<td>0505</td>
<td>Filter function, coded</td>
<td>C an..3</td>
<td>R *</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification of the filtering function used to reversibly map any bit pattern to a restricted character set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The filter function describes how binary information (e.g., a digital signature) can be shown in a readable format. This is for example the case if the value &quot;01111111 00111011&quot; has no readable presentation and can be shown with the hexadecimal filter as &quot;7F 3B&quot;.</td>
</tr>
<tr>
<td>0507</td>
<td>Original character set encoding, coded</td>
<td>C an..3</td>
<td>R *</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 = ASCII 8 bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 = Code page 850 (IBM PC Multinational)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 = Code page 500 (EBCDIC Multinational No. 5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification of the character set in which the secured EDIFACT structure was encoded when security mechanisms were applied (i.e., when the digital signature was generated).</td>
</tr>
<tr>
<td>0509</td>
<td>Role of security provider, coded</td>
<td>C an..3</td>
<td>N</td>
</tr>
<tr>
<td>S500</td>
<td>SECURITY IDENTIFICATION DETAILS</td>
<td>C</td>
<td>N</td>
</tr>
</tbody>
</table>
5. Segments Layout

| 0577 | Security party qualifier | Man..3 |   |   |
### 5. Segments Layout

<table>
<thead>
<tr>
<th>Segment number:</th>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0538</td>
<td>Key name</td>
<td>C an..35</td>
<td></td>
</tr>
<tr>
<td>0511</td>
<td>Security party identification</td>
<td>C an..512</td>
<td></td>
</tr>
<tr>
<td>0513</td>
<td>Security party code list qualifier</td>
<td>C an..3</td>
<td></td>
</tr>
<tr>
<td>0515</td>
<td>Security party code list responsible agency, coded</td>
<td>C an..3</td>
<td></td>
</tr>
<tr>
<td>0586</td>
<td>Security party name</td>
<td>C an..35</td>
<td></td>
</tr>
<tr>
<td>0586</td>
<td>Security party name</td>
<td>C an..35</td>
<td></td>
</tr>
<tr>
<td>0586</td>
<td>Security party name</td>
<td>C an..35</td>
<td></td>
</tr>
<tr>
<td>0520</td>
<td>Security sequence number</td>
<td>C an..35</td>
<td>N</td>
</tr>
<tr>
<td>S501</td>
<td>SECURITY DATE AND TIME</td>
<td>C R</td>
<td></td>
</tr>
<tr>
<td>0517</td>
<td>Date and time qualifier</td>
<td>M an..3</td>
<td>M * = 1 = Security Timestamp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Date and time when the signature was generated.</td>
</tr>
<tr>
<td>0338</td>
<td>Event date</td>
<td>C n..8</td>
<td>R Date of event, format is CCYYMMDD.</td>
</tr>
<tr>
<td>0314</td>
<td>Event time</td>
<td>C an..15</td>
<td>R Time of event, format is HHMMSS</td>
</tr>
<tr>
<td>0336</td>
<td>Time offset</td>
<td>C n4</td>
<td>O UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be prefixed with '-' for negative offsets.</td>
</tr>
</tbody>
</table>

**Segment Notes:**

A segment specifying a security service applied to the referenced EDIFACT structure. The security service data element (DE 0501) shall specify the security service applied to the referenced EDIFACT structure.

Example:

USH+7+1+3+1+2+1++++1:20011010:110522:0100'}
5. Segments Layout

Segment number: 3

<table>
<thead>
<tr>
<th>SG1</th>
<th>- M</th>
<th>99 - USH-USA-SG2</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>- C</td>
<td>3 - Security algorithm</td>
</tr>
</tbody>
</table>

Function:
To identify a security algorithm, the technical usage made of it, and to contain the technical parameters required.

Notes:
1. S503, provides space for one parameter. The number of repetitions of S503 actually used will depend on the algorithm used. The order of the parameters is arbitrary but, in each case, the actual value is preceded by a coded algorithm parameter qualifier.

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S502</td>
<td></td>
<td>SECURITY ALGORITHM</td>
</tr>
<tr>
<td>0523</td>
<td>M</td>
<td>Use of algorithm, coded</td>
</tr>
<tr>
<td>0525</td>
<td>C</td>
<td>Cryptographic mode of operation, coded</td>
</tr>
<tr>
<td>0533</td>
<td>C</td>
<td>Mode of operation code list identifier</td>
</tr>
<tr>
<td>0527</td>
<td>C</td>
<td>Algorithm, coded</td>
</tr>
<tr>
<td>0529</td>
<td>C</td>
<td>Algorithm code list identifier</td>
</tr>
<tr>
<td>0591</td>
<td>C</td>
<td>Padding mechanism, coded</td>
</tr>
<tr>
<td>0601</td>
<td>C</td>
<td>Padding mechanism code list identifier</td>
</tr>
<tr>
<td>S503</td>
<td>C</td>
<td>ALGORITHM PARAMETER</td>
</tr>
<tr>
<td>0531</td>
<td>M</td>
<td>Algorithm parameter qualifier</td>
</tr>
<tr>
<td>0554</td>
<td>M</td>
<td>Algorithm parameter value</td>
</tr>
</tbody>
</table>

Segment Notes:
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the hash value.
At least one occurrence of this segment is mandatory.

Example:
USA+1:16:1:6:1:7:1'
5. Segments Layout

Segment number: 4

<table>
<thead>
<tr>
<th>Segment</th>
<th>Function</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG1</td>
<td>- M 99 - USH-USA-SG2</td>
<td></td>
</tr>
<tr>
<td>SG2</td>
<td>- C 2 - USC-USA</td>
<td></td>
</tr>
<tr>
<td>USC</td>
<td>- M 1 - Certificate</td>
<td></td>
</tr>
</tbody>
</table>

Function:
To convey the public key and the credentials of its owner.

Dependency Notes:
1. D5(110,100) If first, then all

Notes:
2. 0536, if a full certificate (including the USR segment) is not used, the only data elements of the certificate shall be a unique certificate reference made of: the certificate reference (0536), the S500 identifying the issuer certification authority or the S500 identifying the certificate owner, including its public key name. In the case of a non-EDIFACT certificate data element 0545 shall also be present.
3. S500/0538, identifies a public key: either of the owner of this certificate, or the public key related to the private key used by the certificate issuer (certification authority or CA) to sign this certificate.
4. 0507, the original character set encoding of the certificate when it was signed. If no value is specified, the character set encoding corresponds to that identified by the character set repertoire standard.
5. 0543, the original character set repertoire of the certificate when it was signed. If no value is specified, the default is defined in the interchange header.
6. S505, when this certificate is transferred, it will use the default service characters defined in part 1 of ISO 9735, or those defined in the service string advice, if used. This data element may specify the service characters used when the certificate was signed. If this data element is not used then they are the default service characters.
7. S501, dates and times involved in the certification process. Four occurrences of this composite data element are possible: one for the certificate generation date and time, one for the certificate start of validity period, one for the certificate end of validity period, one for revocation date and time.

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0536</td>
<td>C an..35 O</td>
<td>Certificate reference</td>
</tr>
<tr>
<td>S500</td>
<td>SECURITY IDENTIFICATION DETAILS</td>
<td>C R</td>
</tr>
<tr>
<td>0577</td>
<td>Security party qualifier</td>
<td>M an..3 M * 3 = Certificate owner 4 = Authenticating party</td>
</tr>
<tr>
<td>0538</td>
<td>Key name</td>
<td>C an..35 O</td>
</tr>
<tr>
<td>0511</td>
<td>Security party identification</td>
<td>C an..512 O</td>
</tr>
<tr>
<td>0513</td>
<td>Security party code list qualifier</td>
<td>C an..3 D * 2 = GS1 ZZZ = Mutually agreed</td>
</tr>
<tr>
<td>0515</td>
<td>Security party code list responsible agency, coded</td>
<td>C an..3 N</td>
</tr>
<tr>
<td>0586</td>
<td>Security party name</td>
<td>C an..35 N</td>
</tr>
<tr>
<td>0545</td>
<td>Certificate syntax and version, coded</td>
<td>C an..3 D 3 = X.509 Where it is decided to refer to a non-EDIFACT</td>
</tr>
</tbody>
</table>
5. Segments Layout

<table>
<thead>
<tr>
<th>Segment number: 4</th>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0505</td>
<td>C an..3</td>
<td>N</td>
<td>Filter function, coded</td>
</tr>
<tr>
<td>0507</td>
<td>C an..3</td>
<td>N</td>
<td>Original character set encoding, coded</td>
</tr>
<tr>
<td>0543</td>
<td>C an..3</td>
<td>N</td>
<td>Certificate original character set repertoire, coded</td>
</tr>
<tr>
<td>0546</td>
<td>C an..35</td>
<td>N</td>
<td>User authorisation level</td>
</tr>
<tr>
<td>S505</td>
<td>C</td>
<td>N</td>
<td>SERVICE CHARACTER FOR SIGNATURE</td>
</tr>
<tr>
<td>0551</td>
<td>M an..3</td>
<td></td>
<td>Service character for signature qualifier</td>
</tr>
<tr>
<td>0548</td>
<td>M an..4</td>
<td></td>
<td>Service character for signature</td>
</tr>
<tr>
<td>S501</td>
<td>C</td>
<td>N</td>
<td>SECURITY DATE AND TIME</td>
</tr>
<tr>
<td>0517</td>
<td>M an..3</td>
<td></td>
<td>Date and time qualifier</td>
</tr>
<tr>
<td>0338</td>
<td>C n..8</td>
<td></td>
<td>Event date</td>
</tr>
<tr>
<td>0314</td>
<td>C an..15</td>
<td></td>
<td>Event time</td>
</tr>
<tr>
<td>0336</td>
<td>C n4</td>
<td></td>
<td>Time offset</td>
</tr>
<tr>
<td>0567</td>
<td>C an..3</td>
<td>N</td>
<td>Security status, coded</td>
</tr>
<tr>
<td>0569</td>
<td>C an..3</td>
<td>N</td>
<td>Revocation reason, coded</td>
</tr>
</tbody>
</table>

Segment Notes:

This segment either contains information regarding the certificate, and identifies the certification authority which has generated the certificate, or is used to identify bilaterally interchanged signature keys.

1. Use of USC for certificate reference:
   A certificate reference (DE 0536) and trusted third party (DEG S500, DE 0577 = 4 and DEG S500, DE 511) can be identified.
   Example 1:
   USC+AXZ4711+4::5412345000006:2+3'

2. Use of USC for reference to signature keys:
   Identification of the name of the signature key in DEG S500, DE 0538 (DEG S500, DE 0577 = 3).
   The interchange of signature keys and the references have to be bilaterally agreed between the partners.
   Example 2:
   USC++3:PUBLIC KEY 01'
5. Segments Layout

Segment number:  5

<table>
<thead>
<tr>
<th>SG1</th>
<th>- M</th>
<th>99 - USH-USA-SG2</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG2</td>
<td>- C</td>
<td>2 - USC-USA</td>
</tr>
<tr>
<td>USA</td>
<td>- C</td>
<td>3 - Security algorithm</td>
</tr>
</tbody>
</table>

Function:
To identify a security algorithm, the technical usage made of it, and to contain the technical parameters required.

Notes:
1. S503 provides space for one parameter. The number of repetitions of S503 actually used will depend on the algorithm used. The order of the parameters is arbitrary but, in each case, the actual value is preceded by a coded algorithm parameter qualifier.

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S502</td>
<td>M</td>
<td>SECURITY ALGORITHM</td>
</tr>
<tr>
<td>0523</td>
<td>M</td>
<td>Use of algorithm, coded</td>
</tr>
<tr>
<td>0525</td>
<td>R</td>
<td>Cryptographic mode of operation, coded</td>
</tr>
<tr>
<td>0533</td>
<td></td>
<td>Mode of operation code list identifier</td>
</tr>
<tr>
<td>0527</td>
<td>R</td>
<td>Algorithm, coded</td>
</tr>
<tr>
<td>0529</td>
<td>R</td>
<td>Algorithm code list identifier</td>
</tr>
<tr>
<td>0591</td>
<td>R</td>
<td>Padding mechanism, coded</td>
</tr>
<tr>
<td>0601</td>
<td>R</td>
<td>Padding mechanism code list identifier</td>
</tr>
<tr>
<td>S503</td>
<td></td>
<td>ALGORITHM PARAMETER</td>
</tr>
<tr>
<td>0531</td>
<td></td>
<td>Algorithm parameter qualifier</td>
</tr>
<tr>
<td>0554</td>
<td></td>
<td>Algorithm parameter value</td>
</tr>
</tbody>
</table>

Segment Notes:
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the digital signature.
At least one occurrence of this segment is mandatory.

Example:
USA+6:16:1:10:1:7:1'
## 5. Segments Layout

<table>
<thead>
<tr>
<th>Segment number:</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>USB</strong></td>
<td>- M</td>
</tr>
<tr>
<td>1 - Secured data identification</td>
<td></td>
</tr>
</tbody>
</table>

**Function:**
To contain details related to the AUTACK.

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0503</td>
<td>M an..3</td>
<td>M *</td>
</tr>
<tr>
<td>S501</td>
<td>SECURITY DATE AND TIME</td>
<td>C N</td>
</tr>
<tr>
<td>0517</td>
<td>Date and time qualifier</td>
<td>M an..3</td>
</tr>
<tr>
<td>0338</td>
<td>Event date</td>
<td>C n..8</td>
</tr>
<tr>
<td>0314</td>
<td>Event time</td>
<td>C an..15</td>
</tr>
<tr>
<td>0336</td>
<td>Time offset</td>
<td>C n4</td>
</tr>
<tr>
<td>S002</td>
<td>INTERCHANGE SENDER</td>
<td>M M</td>
</tr>
<tr>
<td>0004</td>
<td>Interchange sender identification</td>
<td>M an..35 M</td>
</tr>
<tr>
<td>0007</td>
<td>Identification code qualifier</td>
<td>C an..4 R *</td>
</tr>
<tr>
<td>0008</td>
<td>Interchange sender internal identification</td>
<td>C an..35 N</td>
</tr>
<tr>
<td>0042</td>
<td>Interchange sender internal sub-identification</td>
<td>C an..35 N</td>
</tr>
<tr>
<td>S003</td>
<td>INTERCHANGE RECIPIENT</td>
<td>M M</td>
</tr>
<tr>
<td>0010</td>
<td>Interchange recipient identification</td>
<td>M an..35 M</td>
</tr>
<tr>
<td>0007</td>
<td>Identification code qualifier</td>
<td>C an..4 R *</td>
</tr>
<tr>
<td>0014</td>
<td>Interchange recipient internal identification</td>
<td>C an..35 N</td>
</tr>
<tr>
<td>0046</td>
<td>Interchange recipient internal sub-identification</td>
<td>C an..35 N</td>
</tr>
</tbody>
</table>

**Segment Notes:**
This segment shall contain identification of the interchange sender and interchange 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.

Example:
USB+1++5412345123450:14+5411234512300:14'
## 5. Segments Layout

**Segment number:** 7

<table>
<thead>
<tr>
<th>Segment</th>
<th>Definition</th>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG3</td>
<td>- M 9999 - USX-USY</td>
<td></td>
<td></td>
<td>Unique reference number of interchange containing the data to which the</td>
</tr>
<tr>
<td>USX</td>
<td>- M 1 - Security references</td>
<td></td>
<td></td>
<td>security service was applied (UNB, DE 0020).</td>
</tr>
<tr>
<td>0020</td>
<td>Interchange control reference</td>
<td>M an..14</td>
<td>M</td>
<td>Unique reference number of interchange containing the data to which the</td>
</tr>
<tr>
<td>S002</td>
<td>INTERCHANGE SENDER</td>
<td>C</td>
<td>R</td>
<td>security service was applied (UNB, DE 0020).</td>
</tr>
<tr>
<td>0004</td>
<td>Interchange sender identification</td>
<td>M an..35</td>
<td>M</td>
<td>Identification of the party sending the interchange which contains the data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>to which security services were applied. It is recommended to use GLN -</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Format n13.</td>
</tr>
<tr>
<td>0007</td>
<td>Identification code qualifier</td>
<td>C an..4</td>
<td>R</td>
<td>* 14 = GS1</td>
</tr>
<tr>
<td>0008</td>
<td>Interchange sender internal identification</td>
<td>C an..35</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0042</td>
<td>Interchange sender internal sub-identification</td>
<td>C an..35</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>S003</td>
<td>INTERCHANGE RECIPIENT</td>
<td>C</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>0010</td>
<td>Interchange recipient identification</td>
<td>M an..35</td>
<td>M</td>
<td>Identification of the party receiving the interchange which contains the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>data to which security services were applied. It is recommended to use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>GLN - Format n13.</td>
</tr>
<tr>
<td>0007</td>
<td>Identification code qualifier</td>
<td>C an..4</td>
<td>R</td>
<td>* 14 = GS1</td>
</tr>
<tr>
<td>0014</td>
<td>Interchange recipient internal identification</td>
<td>C an..35</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0046</td>
<td>Interchange recipient internal sub-identification</td>
<td>C an..35</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0048</td>
<td>Group reference number</td>
<td>C an..14</td>
<td>D</td>
<td>Reference to a message group (UNG to UNE) containing data to which the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>security service was applied (UNG, DE 0048).</td>
</tr>
<tr>
<td>S006</td>
<td>APPLICATION SENDER IDENTIFICATION</td>
<td>C</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0040</td>
<td>Application sender identification</td>
<td>M an..35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0007</td>
<td>Identification code qualifier</td>
<td>C an..4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S007</td>
<td>APPLICATION RECIPIENT IDENTIFICATION</td>
<td>C</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0044</td>
<td>Application recipient identification</td>
<td>M an..35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0007</td>
<td>Identification code qualifier</td>
<td>C an..4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0062</td>
<td>Message reference number</td>
<td>C an..14</td>
<td>D</td>
<td>Reference number of a message (UNH to UNT) to which the security service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>was applied (UNH, DE</td>
</tr>
</tbody>
</table>
## 5. Segments Layout

<table>
<thead>
<tr>
<th>Segment number:</th>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>0062 of this message).</td>
</tr>
<tr>
<td>S009 MESSAGE IDENTIFIER</td>
<td>C</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0065 Message type</td>
<td>M.an..6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0052 Message version number</td>
<td>M.an..3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0054 Message release number</td>
<td>M.an..3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0051 Controlling agency, coded</td>
<td>M.an..3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0057 Association assigned code</td>
<td>C.an..6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0110 Code list directory version number</td>
<td>C.an..6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0113 Message type sub-function identification</td>
<td>C.an..6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0800 Package reference number</td>
<td>C.an..35</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>S501 SECURITY DATE AND TIME</td>
<td>C</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>0517 Date and time qualifier</td>
<td>M.an..3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0338 Event date</td>
<td>C.n..8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0314 Event time</td>
<td>C.an..15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0336 Time offset</td>
<td>C.n4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Segments Layout

Segment Notes:
This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.

The USX segment of the AUTACK message refers to a whole interchange, a message group within this interchange or a message in the interchange. Any reference made has to be non-ambiguous; if necessary the reference on a higher hierarchical level has to be indicated.

The USX segment enables the use following references:
- DE 0020 Interchange reference number
- DE 0048 Group reference number
- DE 0062 Message reference number

Application of the interchange reference number of the UNB segment:
Definition: Unique reference number generated by the sender in order to identify the interchange to which security services were applied or which contains messages or groups to which security services were applied.

The message recipient can combine the interchange reference number (DE 0020) and the sender identification (DE 0004) in order to ensure unambiguousness of the reference.

The interchange reference number as the only reference number is used if the security function (i.e., the digital signature) applies to the whole interchange. If the reference data and the AUTACK message are sent in different interchanges, then the interchange reference number is also mandatory, if the security function applies to groups or messages. If the reference data (messages or groups) and the AUTACK message are sent in the same interchange, the interchange reference number is not necessary.

Application of the group reference number of the UNG segment:
Definition: Unique reference number of a group of messages within an interchange to which security services were applied.

In this case to the USX segment refers to the unambiguous group reference number of the sender within an interchange. The group reference number is used if the security function (i.e., the digital signature) was applied to a group of messages.
5. Segments Layout

Segment number: 7

Application of the message reference number of the UNH segment:

Definition: Unique reference number of a message within an interchange to which the security service was applied, generated by the sender.
In this case to the USX segment refers to the unambiguous message reference number of the sender within an interchange.
If the security service applies to every single message,
1) a separate AUTACK message needs to be sent for every message or
2) the segment group 3 (USX/USY) has to be repeated for every message

A separate AUTACK message for every message is necessary, if the messages on their way to the recipient are forwarded within another interchange (e.g., distribution by a clearing centre).

Example:
USX+DAT001+5412345123450:14+5411234512300:14+GRP002+++MES003’
5. Segments Layout

Segment number: 8

<table>
<thead>
<tr>
<th>SG3</th>
<th>- M</th>
<th>9999 - USX-USY</th>
</tr>
</thead>
<tbody>
<tr>
<td>USY</td>
<td>- M</td>
<td>9 - Security on references</td>
</tr>
</tbody>
</table>

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.

Dependency Notes:
1. D3(020,030) One or more

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0534</td>
<td></td>
<td>Security reference number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M an..14 M</td>
</tr>
<tr>
<td>S508</td>
<td></td>
<td>VALIDATION RESULT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C R</td>
</tr>
<tr>
<td>0563</td>
<td></td>
<td>Validation value, qualifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M an..3 M * 1 = Unique validation value</td>
</tr>
<tr>
<td>0560</td>
<td></td>
<td>Validation value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C an..512 R</td>
</tr>
<tr>
<td>0571</td>
<td></td>
<td>Security error, coded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C an..3 N</td>
</tr>
</tbody>
</table>

Segment Notes:
This segment contains a link to the security header group and the result of the security services applied to the referenced EDIFACT structure (i.e., the digital signature) as specified in this linked security header group.

Example:
USY+1+1:139B7CB7...C72B03CE5F
## 5. Segments Layout

Segment number: 9

<table>
<thead>
<tr>
<th>Segment</th>
<th>Segment Grouping</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG4</td>
<td>- M 99 - UST</td>
<td></td>
</tr>
<tr>
<td>UST</td>
<td>- M 1 - Security trailer</td>
<td></td>
</tr>
</tbody>
</table>

**Function:**
To establish a link between security header and security trailer segment groups.

**Notes:**
1. 0534, the value shall be identical to the value in 0534 in the corresponding USH segment.

<table>
<thead>
<tr>
<th>EDIFACT</th>
<th>GS1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0534</td>
<td>M</td>
<td>Security reference number</td>
</tr>
<tr>
<td>M an..14</td>
<td>M</td>
<td>Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).</td>
</tr>
<tr>
<td>0588</td>
<td>M</td>
<td>Number of security segments</td>
</tr>
<tr>
<td>M n..10</td>
<td>M</td>
<td>The number of security segments in a security header/trailer group pair. Only the segment groups 1, 2 and 4 are counted. Each security header/trailer group pair shall contain its own count of the number of security segments within that group pair.</td>
</tr>
</tbody>
</table>

**Segment Notes:**
A segment establishing a link between security header and security trailer segment group, and stating the number of security segments in these groups.

**Example:**
UST+1+5'
5. Segments Layout

Segment number: 10

**UNT** - M 1 - Message trailer

**Function:**
To end and check the completeness of a message.

**Notes:**
1. 0062, the value shall be identical to the value in 0062 in the corresponding UNH segment.

<table>
<thead>
<tr>
<th>Segment</th>
<th>Description</th>
<th>EDIFACT</th>
<th>GS1</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0074</td>
<td>Number of segments in a message</td>
<td>M n..10</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>0062</td>
<td>Message reference number</td>
<td>M an..14</td>
<td>M</td>
<td></td>
</tr>
</tbody>
</table>

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

**Example:**
UNT+10+AUT00001'
6. Examples

The following examples will show how the message type AUTACK can be used in order to transport the digital signature and the information necessary for signature verification by the recipient. There are various scenarios and possibilities how to use the AUTACK in relation to the data to which security services were applied. The appropriate scenario depends on the technical and legal requirements.

Example 1

Two interchanges are transmitted. The first interchange contains the data secured, the second interchange contains the AUTACK message.

This example is recommended if

- the data secured and the AUTACK do not use the same EDIFACT syntax version;
- for technical or organisational reasons the data secured and the AUTACK are generated separately;
- for legal reasons the data secured and the AUTACK must be generated and sent separately.

Structure:

Interchange containing the data secured

```
UNB
   UNH
      message data
   UNT
   UNZ
```

Interchange containing the AUTACK message

```
UNB
   UNH
      AUTACK
   UNT
   UNZ
```
6. Examples

EANCOM® realisation:

message data:

UNA:+.?’ Service string advice, syntax 3
UNB+UNOA:3+5412345678908:14+87987654321 06:14+20020102:1000+INT12345’ Interchange header of the syntax 3 interchange INT12345.
UNH+ME0001+INVOIC:D:96A:UN:EAN008’ Message header of an INVOIC message, the message number is ME0001
....
UNT+7+ME0001’ Message trailer
UNZ+1+12345’ Interchange trailer

security data:

UNA:+.?'' Service string advice, syntax 4
UNH+AUT0001+AUTACK:4:1:UN:EAN001’ Message header of the service message AUTACK
USH+7+1+3+1+2+1++++1:20020102:100522:0100’ Security header,
  • security service “non-repudiation of origin to a referenced EDIFACT structure” is applied,
  • the security function applies to the whole referenced message or interchange,
  • for filtering the signature a hexadecimal filter is used,
  • the original character set encoding of the EDIFACT structure was ASCII 7 bit
  • security time stamp is 2nd January 2002, 10:05:22
USA+1:16:1:6:1:7:1’ The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.
USC+AXZ4711+4::5412345000006:2+3’ The reference of the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1’ The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.
6. Examples

USB+1++5412345678908:14+8798765432106:14 The sender and recipient of the interchange in which the
AUTACK is present are identified with the GLNs
5412345678908 and 8798765432106.

USX+INT12345+5412345678908:14+8798765432
106:14++++ ME0001' The referenced message ME 0001 to which security
functions were applied is within interchange INT12345. The
sender and recipient of the interchange in which the
referenced message is present are identified with the GLNs
5412345678908 and 8798765432106.

USY+1+1:139B7CB.......7C72B03CE5F' The digital signature is 139B7CB.......7C72B03CE5F.

UST+1+5' The number of security segments in the segment groups 1, 2
and 4 equals 5.

UNT+10+ AUT0001' Message trailer, the total number of segments equals 10.

UNZ+1+INT12346' Interchange trailer
6. Examples

Example 2

Two interchanges are transmitted. The first interchange contains three messages to be secured, the second interchange contains the AUTACK message.

This example is recommended if

- the data secured and the AUTACK do not use the same EDIFACT syntax version;
- for technical or organisational reasons the data secured and the AUTACK are generated separately;
- for legal reasons the data secured and the AUTACK must be generated and sent separately;
- several messages in one interchange should be signed at once.

Structure:

```
UNB
  UNH
    message data
    UNH
    message data
    UNH
    message data
  UNT
  UNZ
```

Interchange containing the data secured

```
UNB
  UNH
    AUTACK
  UNT
  UNZ
```

Interchange containing the AUTACK message
6. Examples

**EANCOM® realisation:**

**message data:**

```
UNA:+.?'  Service string advice, syntax 3
UNB+:UNOA:3+:5412345678908:14+87987654321
06:14+20020102:1000+12345'
UNH+:ME0001+:INVOIC:D:96A:UN:EAN008'
  Message header of the first INVOIC message, the message number is ME0001.
  ...
UNT+7+ME0001'  Message trailer of the first message
UNH+:ME0002+:INVOIC:D:96A:UN:EAN008'
  Message header of the second INVOIC message, the message number is ME0002.
  ...
UNT+7+ME0002'  Message trailer of the second message
UNH+:ME0003+:INVOIC:D:96A:UN:EAN008'
  Message header of the third INVOIC message, the message number is ME0003.
  ...
UNT+7+ME0003'  Message trailer of the third message
UNZ+3+12345'
  Interchange trailer
```

**security data:**

```
UNA:+.?"  Service string advice, syntax 4
UNB+:UNOA:4+:5412345678908:14+87987654321
06:14+20020102:1000+12346'
UNH+:AUT0001+:AUTACK:4:1:UN:EAN001'
  Message header of the service message AUTACK
USH+7+1+3+1+2+1++++1:20020102:100522:0100'
  Security header,
  * security service "non-repudiation of origin to a referenced EDIFACT structure" is applied,
  * the security function applies to the whole referenced message or interchange,
  * for filtering the signature a hexadecimal filter is used,
  * the original character set encoding of the EDIFACT structure was ASCII 7 bit
  * security time stamp is 2\textsuperscript{nd} January 2002, 10:05:22
```
6. Examples

**USA+1:16:1:6:1:7:1’**

The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.

**USC+AXZ4711+4::541234500006:2+3’**

The reference to the certificate issued by the trust centre identified with the GLN 541234500006 is AXZ4711. The syntax of the certificate is X.509.

**USA+6:16:1:10:1:7:1’**

The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.

**USB+1++5412345678908:14+8798765432106:14’**

The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.

**USX+INT12435+5412345678908:14+8798765432106:14’**

The referenced messages to which security functions were applied are within interchange INT12345. The sender and recipient of the referenced interchange are identified with the GLNs 5412345678908 and 8798765432106.

**USY+1+1:139B7CB..........7C72B03CE5F’**

The digital signature is 139B7CB........7C72B03CE5F.

**UST+1+5’**

The number of security segments in the segment groups 1, 2 and 4 equals 5.

**UNT+10+AUT0001’**

Message trailer, the total number of segments equals 10.

**UNZ+1+12346’**

Interchange trailer
6. Examples

Example 3

Two interchanges are transmitted. The first interchange contains three messages to be secured, the second interchange contains the AUTACK message. In order to transmit the digital signature for every single message, segment group 3 of the AUTACK message is repeated three times.

This example is recommended if

- the data secured and the AUTACK do not use the same EDIFACT syntax version;
- for technical or organisational reasons the data secured and the AUTACK are generated separately;
- for legal reasons the data secured and the AUTACK must be generated and sent separately;
- every single message in one interchange should be signed separately (e.g., for legal reasons).

Structure:
6. Examples

EANCOM® realisation:

message data:

UNA:+.? ’ Service string advice, syntax 3

UNB+UNOA:3+5412345678908:14+87987654321 06:14+20020102:1000+12345’ Interchange header of the syntax 3 interchange INT12345.

UNH+ME0001+INVOIC:D:96A:UN:EAN008’ Message header of the first INVOIC message, the message number is ME0001.

....

UNT+7+ME0001’ Message trailer of the first message

UNH+ME0002+INVOIC:D:96A:UN EAN008’ Message header of the second INVOIC message, the message number is ME0002.

....

UNT+7+ME0002’ Message trailer of the second message

UNH+ME0003+INVOIC:D:96A:UN EAN008’ Message header of the third INVOIC message, the message number is ME0003.

....

UNT+7+ME0003’ Message trailer of the third message

UNZ+3+12345’ Interchange trailer

security data:

UNA:+.?’ Service string advice, syntax 4


UNH+AUT0001+AUTACK:4:1:UN:EAN001’ Message header of the service message AUTACK

USH+7+1+3+1+2+1+++++1:20020102:100522:0100’ Security header,
- security service "non-repudiation of origin to a referenced EDIFACT structure" is applied,
- the security function applies to the whole referenced message or interchange,
- for filtering the signature a hexadecimal filter is used,
- the original character set encoding of the EDIFACT structure was ASCII 7 bit
- security time stamp is 2nd January 2002, 10:05:22
6. Examples

USA+1:16:1:6:1:7:1' The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 #2.

USC+AXZ4711+4::541234500006:2+3' The reference to the certificate issued by the trust centre identified with the GLN 541234500006 is AXZ4711. The syntax of the certificate is X.509.

USA+6:16:1:10:1:7:1' The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 #2.

USB+1++5412345678908:14+8798765432106:14' The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.

USX+INT12435+5412345678908:14+8798765432 106:14++++ME0001' The first referenced message ME0001 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.

USY+1+1:139B7CB7.......C72B03CE5F' The digital signature of the first message is 139B7CB.......C72B03CE5F.

USX+INT12435+5412345678908:14+8798765432 106:14++++ME0002' The second referenced message ME0002 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.

USY+1+1:145D8BB........2B69B38DC6A' The digital signature of the second message is 145D8BB........2B69B38DC6A.

USX+INT12435+5412345678908:14+8798765432 106:14++++ME0003' The third referenced message ME0003 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.

USY+1+1:186A3DC........4C54B59CE4E' The digital signature of the third message is 186A3DC........4C54B59CE4E.

UST+1+5' The number of security segments in the segment groups 1, 2 and 4 equals 5.

UNT+1+4+AUT0001' Message trailer, the total number of segments equals 14.

UNZ+1+123456' Interchange trailer
6. Examples

Example 4

Message data and AUTACK are transmitted in one interchange. The interchange contains one AUTACK message and one message to be secured.

This example is recommended if

- the data secured and the AUTACK both use EDIFACT syntax version 4;
- for technical or organisational reasons the data secured and the AUTACK must be sent together;
- for legal reasons the data secured and the AUTACK must be generated and sent in one interchange.

The advantage of this scenario is that the signature can be verified directly, because the message and the signature information do not need to be matched by the recipient.

Structure:

```
UNB
  UNH
    message data
  UNT
    UNH
      AUTACK
      UNT
    UNZ
```

EANCOM® realisation:

```
UNA:+.?*
Service string advice, syntax 4
UNB+UNOC:4+5412345678908:14+8798765432106:14+20020102:1015+12346
Interchange header of the syntax 4 interchange INT12346.
UNH+ME0001+INVOIC:D:01B:UN:EAN010
Message header of the an INVOIC message, the message number is ME0001.
...
UNT+7+ME0001
Message trailer of the INVOIC message
UNH+AUT0001+AUTACK:4:1:UN:EAN001
Message header of the service message AUTACK
```
6. Examples

**USH+7+1+3+1+2+1++++1:20020102:100522:0100’**  Security header,
- security service "non-repudiation of origin to a referenced EDIFACT structure" is applied,
- the security function applies to the whole referenced message or interchange,
- for filtering the signature a hexadecimal filter is used,
- the original character set encoding of the EDIFACT structure was ASCII 7 bit
- security time stamp is 2nd January 2002, 10:05:22

**USA+1:16:1:6:1:7:1’**  The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.

**USC+AXZ4711+4::541234500006:2+3’**  The reference to the certificate issued by the trust centre identified with the GLN 541234500006 is AXZ4711. The syntax of the certificate is X.509.

**USA+6:16:1:10:1:7:1’**  The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.

**USB+1++5412345678908:14+8798765432106:14’**  The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.

**USX+INT12345+5412345678908:14+8798765432106:14+++++ME0001’**  The referenced message ME0001 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.

**USY+1+1:139B7CB.....7C72B03CE5F’**  The digital signature is 139B7CB.......7C72B03CE5F.

**UST+1+5’**  The number of security segments in the segment groups 1, 2 and 4 equals 5.

**UNT+10+AUT0001’**  Message trailer, the total number of segments equals 10.

**UNZ+2+12346’**  Interchange trailer
6. Examples

Example 5

Message data and AUTACK are transmitted in one interchange. The interchange contains two groups of messages. The first group contains the data to be secured, the second group contains the AUTACK message. The security function applies to the group of messages.

This example is recommended if

- the data secured and the AUTACK both use EDIFACT syntax version 4;
- for technical or organisational reasons the data secured and the AUTACK must be sent together;
- for legal reasons the data secured and the AUTACK must be generated and sent in one interchange;
- several messages in one interchange should be signed at once.

The advantage of this scenario is, that the signature can be verified directly, because the message and the signature information do not need to be matched by the recipient.

Structure:

```
UNB
  UNG
    UNH
    message data
    UNT
    UNH
    message data
    UNT
    UNH
    message data
  UNT
  UNE
    UNG
    UNH
    AUTACK
    UNT
    UNE
  UNZ
```
6. Examples

EANCOM\textsuperscript{\textregistered} realisation:

UNA:+.?*' Service string advice, syntax 4


UNG+INVOIC+5412345678908:14+8798765432106:14+20020102:1015+GRP0001+UN+D:01B:EAN010' Message group header of the message group GRP0001, containing INVOIC messages

UNH+ME0001+INVOIC:D:01B:UN:EAN010' Message header of the first INVOIC message, the message number is ME0001.

....

UNT+7+ME0001' Message trailer of the first message

UNH+ME0002+INVOIC:D:01B:UN:EAN010' Message header of the second INVOIC message, the message number is ME0002.

....

UNT+7+ME0002' Message trailer of the second message

UNH+ME0003+INVOIC:D:01B:UN:EAN010' Message header of the third INVOIC message, the message number is ME0003.

....

UNT+7+ME0003' Message trailer of the third message

UNE+3+GRP0001' Message group trailer of the first group

UNG+AUTACK+5412345678908:14+8798765432106:14+20020102:1015+GRP0002+UN+D:01B:EAN001' Message group header of the message group GRP0002, containing the AUTACK message

UNH+AUT0001+AUTACK:4:1:UN:EAN001' Message header of the service message AUTACK

USH+7+1+3+1+2+1++++1:20020102:100522:0100' Security header,

- security service "non-repudiation of origin to a referenced EDIFACT structure" is applied,
- the security function applies to the whole referenced message or interchange,
- for filtering the signature a hexadecimal filter is used,
- the original character set encoding of the EDIFACT structure was ASCII 7 bit
- security time stamp is 2\textsuperscript{nd} January 2002, 10:05:22

USA+1:16:1:6:1:7:1' The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.
6. Examples

USC+AXZ4711+4::541234500006:2+3' The reference to the certificate issued by the trust centre identified with the GLN 541234500006 is AXZ4711. The syntax of the certificate is X.509.

USA+6:16:1:10:1:7:1' The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.

USB+1++5412345678908:14+8798765432106:14' The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.

USX+INT12436+5412345678908:14+879876543210 6:14+GRP0001' The referenced group of messages GRP0001 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced group is present are identified with the GLNs 5412345678908 and 8798765432106.

USY+1+1:139B7CB7.......C72B03CE5F' The digital signature of the group of messages is 139B7CB.......7C72B03CE5F.

UST+1+5' The number of security segments in the segment groups 1, 2 and 4 equals 5.

UNT+10+AUT0001' Message trailer, the total number of segments equals 10.

UNE+1+GRP0002' Message group trailer of the second group

UNZ+4+12346' Interchange trailer
6. Examples

Example 6

Message data and AUTACK are transmitted in one interchange. The interchange contains one AUTACK message and three messages to be secured. Within the AUTACK (repetition of SG 3) the signature information on every single message is transmitted.

This example is recommended if

- the data secured and the AUTACK both use EDIFACT syntax version 4;
- for technical or organisational reasons the data secured and the AUTACK must be sent together;
- for legal reasons the data secured and the AUTACK must be generated and sent in one interchange;
- every single message in one interchange should be signed separately (e.g. for legal reasons).

The advantage of this scenario is that the signature can be verified directly and the message and the signature information do not need to be matched by the recipient.

Structure:

```
UNB
  UNH
  message data
  UNT
  UNH
  message data
  UNT
  UNH
  message data
  UNT
  UNH
  AUTACK SG 3
  AUTACK SG 3
  AUTACK SG 3
  UNT
  UNZ
```
6. Examples

**EANCOM® realisation:**

**UNA:+.?”**

Service string advice, syntax 4

**UNB+UNOC:4+5412345678908:14+8798765432106:14+20020102:1015+12346’**

Interchange header of the syntax 4 interchange INT12346.

**UNH+ME0001+INVOIC:D:01B:UN:EAN010’**

Message header of the first INVOIC message, the message number is ME0001.

**...**

**UNT+7+ME0001’**

Message trailer of the first message

**UNH+ME0002+INVOIC:D:01B:UN:EAN010’**

Message header of the second INVOIC message, the message number is ME0002.

**...**

**UNT+7+ME0002’**

Message trailer of the second message

**UNH+ME0003+INVOIC:D:01B:UN:EAN010’**

Message header of the third INVOIC message, the message number is ME0003.

**...**

**UNT+7+ME0003’**

Message trailer of the third message

**UNH+AUT0001+AUTACK:4:1:UN:EAN001’**

Message header of the service message AUTACK

**USH+7+1+3+1+2+1++++1:20020102:100522:0100’**

Security header,

- security service "non-repudiation of origin to a referenced EDIFACT structure" is applied,
- the security function applies to the whole referenced message or interchange,
- for filtering the signature a hexadecimal filter is used,
- the original character set encoding of the EDIFACT structure was ASCII 7 bit
- security time stamp is 2nd January 2002, 10:05:22

**USA+1:16:1:6:1:7:1’**

The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.

**USC+AXZ4711+4::541234500006:2+3’**

The reference to the certificate issued by the trust centre identified with the GLN 541234500006 is AXZ4711. The syntax of the certificate is X.509.

**USA+6:16:1:10:1:7:1’**

The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.

**USB+1++5412345678908:14+8798765432106:14’**

The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.
6. Examples

USX+INT12436+5412345678908:14+8798765432106:14++++ME0001'
The first referenced message ME0001 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.

USY+1+1:139B7CB7........C72B03CE5F'
The digital signature of the first message is 139B7CB........C72B03CE5F.

USX+INT12436+5412345678908:14+8798765432106:14++++ME0002'
The second referenced message ME0002 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.

USY+1+1:145D8BB........2B69B38DC6A'
The digital signature of the second message is 145D8BB........2B69B38DC6A.

USX+INT12436+5412345678908:14+8798765432106:14++++ME0003'
The third referenced message ME0003 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.

USY+1+1:186A3DC........4C54B59CE4E'
The digital signature of the third message is 186A3DC........4C54B59CE4E.

UST+1+5'
The number of security segments in the segment groups 1, 2 and 4 equals 5.

UNT+14+AUT0001'
Message trailer, the total number of segments equals 14.

UNZ+4+12346'
Interchange trailer