NPL Report CISE 5/95

December 1995

Security target and test purposes for EDIFACT

Richard Lampard
Centre for Information Systems Engineering
National Physical Laboratory
Teddington
Middlesex
United Kingdom
TW11 0LW

ABSTRACT

This document provides a partial security target for an implementation of a secure EDIFACT translator. It is based in part on a vulnerability analysis of the EDIFACT standard.

ISSN 1361-407X

National Physical Laboratory
Teddington, Middlesex, UK, TW11 0LW

Approved on behalf of the Managing Director of NPL,
by Mr A J Marks, Director, Centre for Information Systems Engineering

CONTENTS

1 INTRODUCTION

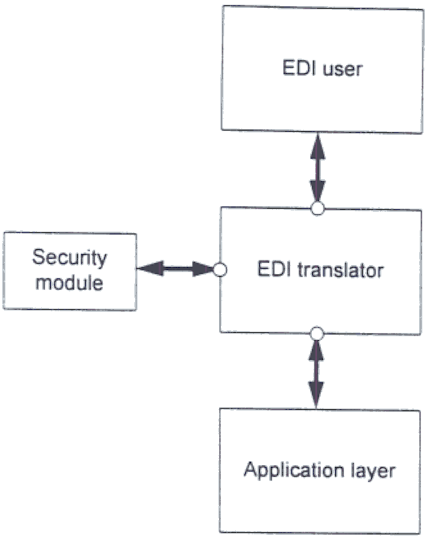
This document provides a partial security target for an implementation of an EDIFACT translator. It is based in part on a vulnerability analysis of the EDIFACT standard as given in Appendix 1.

In addition, the test suite structure and test purposes developed for EDIFACT are given in Appendix 2.

2 FUNCTIONAL AND ENVIRONMENTAL ASSUMPTIONS

This security target assumes that the EDIFACT translator will be operating over insecure communications links (e.g. provided by PTTs), using X.400 as the transmission protocol. The EDIFACT translator can be implemented on an insecure platform (e.g. a PC) in a public area. It is assumed that procedures are in place for the secure generation, storage, distribution, revocation and destruction of keys where appropriate.

The architecture of the system containing the EDIFACT implementation will therefore be as follows:



The EDI User sits atop the EDIFACT translator, which submits EDI interchanges to an X.435 User Agent for transmission. The User Agent submits X.435 messages to the Message Transfer System. The security module is a unit secured against physical interference (e.g. tamper resistant), which provides security mechanisms as requested by the translator. It is the EDIFACT translator that decides which mechanisms and modes of operation are to be used, the security module merely applies the chosen mechanisms and returns the result. It is also assumed that the security module is responsible for the secure generation and storage of cryptographic material such as keys and initialisation vectors. All security functions are transparent to the EDI User, and are applied by the EDIFACT translator in accordance with the prevailing security policy.

It is further assumed that the EDIFACT translator and X.435 User Agent are not necessarily co-located, so that security must be provided at the EDIFACT interchange level. This is by means of extensions to existing EDIFACT messages [1], and through the provision of a special secure authentication and acknowledgement message, AUTACK [2].

Security is also available in X.435, but this is not necessary if EDIFACT security has been applied. Indeed, the implementation assumes that X.435 security is not being applied.

3 SECURITY OBJECTIVES AND THREATS

The following threats to EDIFACT interchanges are assumed to be present in the environment:

Loss, deletion, addition, duplication, replay or re-ordering of messages;
Modification of message contents;
Masquerade by interchange sender;
Repudiation of message origination;
Repudiation of message receipt;
Sender wrongly claims authorship of a message;
Two or more individuals claim to be legitimate (temporary) owners of a message;
One party refuses to complete a transaction;
Disclosure of the identity of the sender;
Disclosure of message contents.

The first nine threats are countered by the following security services respectively:

Message sequence integrity;
Message content integrity;
Message origin authentication;
Non-repudiation of origin;
Non-repudiation of receipt;
Claim of origin;
Claim of ownership;
Fair exchange of values;
Anonymity.

The latter four are taken from [3].

Claim of origin requires the use of a notary to indicate authorship of a document, it is not clear from [3] how claim of ownership could be achieved, and fair exchange of values requires the use of an oblivious transfer protocol. Therefore, provision of these three services is not an EDI matter per se, and so is outside the scope of this security target. Neither does this implementation protect against disclosure of message contents.[1]

Note also that the provision of anonymity is only secure if the underlying transmission protocol provides a similar service for network addresses, otherwise it will be possible to infer the identity of the sender and recipient.

Thus, the security objectives of the EDIFACT translator are:

Provision of interchange and message integrity;
Authentication of message origin;
Prevention of repudiation of message origination or receipt;
Confidentiality of the identity of sender.

---

[1] Note that an EDIFACT message, CIPHER, is being defined to provide confidentiality, but details of this message are currently unavailable. The security target will be updated accordingly when the definition of CIPHER has been obtained.

ACKNOWLEDGEMENTS

This work was carried out by the Data Security Group at the National Physical Laboratory, and was sponsored by the Telecommunications Division of the Department of Trade and Industry, and by the Defence Research Agency on behalf of the Ministry of Defence.

REFERENCES

[1] EDIFACT Security Implementation Guidelines, Paris, 3rd December 1993.

[2] WESTERN EUROPEAN EDIFACT BOARD SPECIAL INTEREST GROUP ON SECURITY. Message Implementation Guidelines Handbook - UN/EDIFACT Message AUTACK. 10th December 1993.

[3] CRYPTOMATHIC & MBLE. Security in Open Environments. Deliverable 7 of TEDIS II.

APPENDIX 1 Vulnerability analysis

Threat	Security service	Security mechanisms	Vulnerabilities
Loss, deletion, addition, duplication, replay, re-ordering of messages.	Message sequence integrity.	Security reference number in USH segment. Security timestamp in USH segment.	When security reference number cycles around, implementation may misinterpret ordering. Loss or deletion of last message may not be detected since no more reference numbers. Security reference number and security timestamp can be modified undetectably if message content integrity not applied to security header containing reference number or timestamp. If multiple USHs are used, each one may have a different reference number or timestamp so that it is not clear which one should be used. If AUTACK response expected, but this is blocked by an attacker originator may re-send initial message believing that recipient never received it.
Modification of contents.	Message content integrity.	Hash function. Sealing (e.g. MAC). Digital signature	Security result in USH segment may refer to wrong USR segment. Vulnerability in mechanism or in mode of operation used. Key compromise

message sender.	authentication	Digital signature.	wrong USR segment. Vulnerability in mechanism or in mode of operation used. Key compromise.
Repudiation of message origination.	Non-repudiation of origin.	Digital signature.	Vulnerability in mechanism or in mode of operation used. Key compromise
Repudiation of message receipt.	Non-repudiation of receipt.	AUTACK message using digital signature.	Security result in AUTACK USH segment may refer to wrong USR or USY segment. Response type given in security header could be modified if not protected by message content integrity. If multiple USHs are used, they may all have different response types set, so that recipient may not know whether to issue an AUTACK. Vulnerability in mechanism or in mode of operation used. Key compromise
Disclosure of message contents.	Confidentiality		Not available in EDIFACT.
Multiple copies of a document are all claimed to be the original.	Claim of origin.	Digital signature of a third party notary indicating authorship of document.	Notary may not be trustworthy. Notary key compromise.
Two or more users claim to be the legitimate (temporary) owners of a document.	Claim of ownership.	N/K	

owners of a document.

One party refuses to complete a transaction.	Fair exchange of values.	Oblivious transfer.	
Disclosure of the identity of the sender.	Anonymity (untraceability).	Blind signatures.	Notary may not be trustworthy. Notary key compromise. Traffic analysis and analysis of header and trailer information in transmission protocol may yield sender and recipient names.

APPENDIX 2 Test suite structure and test purposes for secure EDIFACT

Note that we have taken the practical expedient of reducing redundancy in the TSS by not repeating sub-trees of tests when these already occur earlier in the tree.

2.1 RECIPIENT TEST SUITE STRUCTURE

Security behaviour
|__ General
    |__ Interchange sender invalid
    |__ Security structure version number invalid
    |__ Security result link invalid
    |__ Recipient party identification invalid
    |__ Originator party identification invalid
|__ Message sequence integrity
    |__ Security reference number valid
        |__ Security reference number cycles around
    |__ Security reference number invalid
        |__ Security reference number cycles around
    |__ Security date and time invalid
    |__ Multiple USHs invalid
__ Message content integrity (use of algorithm = OHA)
    |__ Use of algorithm identifier invalid
    |__ Cryptographic mode of operation valid
    |__ Cryptographic mode of operation invalid
    |__ Mode of operation code list identifier invalid
    |__ Algorithm identifier valid
    |__ Algorithm identifier invalid
    |__ Algorithm code list identifier invalid
    |__ Algorithm parameter valid
        |__ Algorithm parameter qualifier invalid
    |__ Algorithm parameter invalid
        |__ Algorithm parameter qualifier valid
        |__ Algorithm parameter qualifier invalid
    |__ Security result invalid
__ Message origin authentication (use of algorithm = OSY)
    |__ Cryptographic mode of operation invalid
    |__ Mode of operation code list identifier invalid
    |__ Algorithm identifier valid
    |__ Algorithm identifier invalid
    |__ Algorithm code list identifier invalid
    |__ Algorithm parameter valid
        |__ Algorithm parameter qualifier invalid
    . Algorithm parameter invalid
        |__ Algorithm parameter qualifier valid
    . Use of algorithm in Gr. 2 = OCF, OSG or OCS
        |__ Cryptographic mode of operation valid
        |__ Cryptographic mode of operation invalid
        |__ Mode of operation code list identifier invalid
        |__ Algorithm identifier valid

```
                    |__ Algorithm identifier invalid
                    |__ Algorithm code list identifier invalid
                    |__ Algorithm parameter valid
                            |__ Algorithm parameter qualifier invalid
                    |__ Algorithm parameter invalid
                            |__ Algorithm parameter qualifier valid
        |__ Security result in Gr. 2 valid
        |__ Security result in Gr. 2 invalid
    Non-repudiation of origin
        |__ Certificate reference invalid
        |__ Security party qualifier = OW
                |__ Key name invalid
                |__ Party identification invalid
                |__ Code list qualifier invalid
                |__ Code list responsible agency invalid
        |__ Security party qualifier = AX
                |__ Key name invalid
                |__ Party identification invalid
                |__ Code list qualifier invalid
                |__ Code list responsible agency invalid
        |__ Certificate generation timestamp invalid
        |__ Certificate validity start timestamp invalid
        |__ Certificate validity end timestamp invalid
        |__ Use of algorithm in Gr. 2 = ISG or IHA
                |__ Cryptographic mode of operation valid
                |__ Cryptographic mode of operation invalid
                |__ Mode of operation code list identifier invalid
                |__ Algorithm identifier valid
                |__ Algorithm identifier invalid
                |__ Algorithm code list identifier invalid
                |__ Algorithm parameter valid
                        |__ Algorithm parameter qualifier valid
                        |__ Algorithm parameter qualifier invalid
                |__ Algorithm parameter invalid
                        |__ Algorithm parameter qualifier valid
                        |__ Algorithm parameter qualifier invalid
        |__ Security result in Gr. 2 valid
        |__ Security result in Gr. 2 invalid
    Non-repudiation of receipt
        |__ Response type invalid
        |__ Multiple USHs invalid
    Anonymity
        |__ Anonymous message valid
```

2.2 ORIGINATOR TEST SUITE STRUCTURE

```
Security behaviour
|__ General
        |__ Security structure version number valid
        |__ Security structure version number invalid
        |__ Originator party identification valid
        |__ Originator party identification invalid
|__ Message sequence integrity
        |__ No AUTACK response received
```

Non-repudiation of receipt
- |__ AUTACK security structure version number invalid
- |__ Response type invalid
- |__ AUTACK Gr. 3 interchange control reference invalid
- |__ AUTACK Gr. 3 security date and time invalid
- |__ AUTACK security result link invalid
- |__ AUTACK security function invalid
- |__ AUTACK security identification details invalid
- |__ AUTACK security date and time invalid
- |__ AUTACK signature invalid

Anonymity
- |__ Anonymous message

2.3 TEST PURPOSES

Each test purpose has a reference of the form:

AA/BB/CC/DD/(No)-VI

EDIS, for all tests relating to EDIFACT syntax.

REC or ORG, identifying either IUT recipient or IUT originator test.

CC = identifying which security service is being tested, and may take one of the following values:

GEN	general behaviour
MSI	message sequence integrity
MCI	message content integrity
MOA	message origin authentication
NRO	non-repudiation of origin
NRR	non-repudiation of receipt
ANON	anonymity

DD = this field is used to further provide subsections within CC.

(No) = if there are more than one test purpose for the same reference, they are then numbered sequentially, as they occur in this document.

is the validity indicator (either V or Iv) in that the described test purpose may present the IUT with either a valid or invalid message.

Recipient tests

EDIS/REC/GEN/IS/EDIS_REC_GEN_IS_1_Iv

/* A message is submitted to the IUT with a discrepancy between the sender name given in the interchange header and the name given in the security header of the message */;

EDIS/REC/GEN/SVN/EDIS_REC_GEN_SVN_2_Iv

/* A message is submitted to the IUT containing an invalid security structure version number.*/;

EDIS/REC/GEN/SVN/EDIS_REC_GEN_SVN_3_Iv

/* A message is submitted to the IUT containing several USH segments, each of which has a different security structure version number.*/;

EDIS/REC/GEN/SRL/EDIS_REC_GEN_SRL_2_Iv

/* A message is submitted to the IUT containing an invalid security result link in the USH segment.*/;

EDIS/REC/GEN/RPI/EDIS_REC_GEN_RPI_2_Iv

/* A message is submitted to the IUT containing an invalid security party qualifier.*/;

EDIS/REC/GEN/RPI/EDIS_REC_GEN_RPI_3_Iv

/* An interchange is submitted to the IUT containing an invalid recipient key name.*/;

EDIS/REC/GEN/RPI/EDIS_REC_GEN_RPI_4_Iv

/* A message is submitted to the IUT containing an invalid recipient party identification.*/;

EDIS/REC/GEN/RPI/EDIS_REC_GEN_RPI_5_Iv

/* A message is submitted to the IUT containing an invalid recipient party name.*/;

EDIS/REC/GEN/OPI/EDIS_REC_GEN_OPI_2_Iv

/* A message is submitted to the IUT containing an invalid originator key name.*/

EDIS/REC/GEN/OPI/EDIS_REC_GEN_OPI_3_Iv

/* A message is submitted to the IUT containing a non-existent originator party identification.*/;

EDIS/REC/GEN/OPI/EDIS_REC_GEN_OPI_4_Iv

/* A message is submitted to the IUT containing the originator party identification belonging to a different originator (masquerade attack).*/;

EDIS/REC/GEN/OPI/EDIS_REC_GEN_OPI_5_Iv

/* A message is submitted to the IUT containing an invalid originator party name.*/;

EDIS/REC/GEN/OPI/EDIS_REC_GEN_OPI_6_Iv

/* A message is submitted to the IUT containing an originator key name which denotes the key of another originator (masquerade attack).*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_1_V

/* A message is submitted to the IUT containing a valid security reference number.*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_2_V

/* A message is submitted to the IUT containing a valid security reference number which has just cycled around to the starting value.*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_3_Iv

/* A interchange is submitted to the IUT containing a security reference number which is greater than the successor of the previous reference number (deletion or reordering attack).*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_4_Iv

/* A interchange is submitted to the IUT containing a security reference number which is equal to the previous reference number (replay attack).*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_5_Iv

/* A interchange is submitted to the IUT containing a security reference number which is equal to a reference number which is less than the previous reference number (replay or reordering attack).*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_6_Iv

/* A message is submitted to the IUT containing a security reference number which is greater than the successor of the previous reference number, where that previous number was of the maximum size before the number cycles back to the starting value (deletion or reordering attack).*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_7_Iv

/* A message is submitted to the IUT containing a security reference number which is equal to the maximum size before the number cycles back to the starting value, where the previous reference number was equal to the starting value (replay or reordering attack).*/;

EDIS/REC/MSI/SRN/EDIS_REC_MSI_SRN_8_Iv

/* An interchange is submitted to the IUT where the last message has been deleted.*/;

EDIS/REC/MSI/SDT/EDIS_REC_MSI_SDT_2_Iv

/* A message is submitted to the IUT containing a date and time which is greater than the current date and time (preplay attack).*/;

EDIS/REC/MSI/SDT/EDIS_REC_MSI_SDT_3_Iv

/* A message is submitted to the IUT containing a date and time which is less than the current date and time, and outside the window when messages are considered to be fresh (replay attack).*/;

EDIS/REC/MSI/MUSH/EDIS_REC_MSI_MUSH_2_Iv

/* A message is submitted to the IUT containing multiple USHs, each of which has the same security timestamp but a different security reference number (reordering attack).*/;

EDIS/REC/MSI/MUSH/EDIS_REC_MSI_MUSH_3_Iv

/* A message is submitted to the IUT containing multiple USHs, each of which has a different security timestamp but the same security reference number (masquerade or replay attack).*/;

EDIS/REC/MCI/UAI/EDIS_REC_MCI_UAI_2_Iv

/* A message is submitted to the IUT containing an invalid use of algorithm identifier.*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Va

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (NUL).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vb

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (CBC).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vc

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (CFB1).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vd

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (CFB8).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Ve

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (OFB).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vf

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (DIM1).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vg

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (DIM2).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vh

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (MDC2).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vi

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (HDS1).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vj

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (HDS2).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vk

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (NVB7.1).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vl

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (NVBAK).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_1_Vm

/* A message is submitted to the IUT containing a valid cryptographic mode of operation (ZZZ).*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_2_Iv

/* A message is submitted to the IUT containing an invalid cryptographic mode of operation.*/;

EDIS/REC/MCI/CMO/EDIS_REC_MCI_CMO_3_Iv

/* A message is submitted to the IUT for which the cryptographic mode of operation is inconsistent with the use of algorithm identifier (content integrity attack).*/;

EDIS/REC/MCI/MOCI/EDIS_REC_MCI_MOCI_2_Iv

/* A message is submitted to the IUT containing a mode of operation code list identifier which is inconsistent with the cryptographic mode of operation (content integrity attack).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_1_Va

/* A message is submitted to the IUT containing a valid algorithm identifier (MD4).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_1_Vb

/* A message is submitted to the IUT containing a valid algorithm identifier (MD5).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_1_Vc

/* A message is submitted to the IUT containing a valid algorithm identifier (RIPEMD).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_1_Vd

/* A message is submitted to the IUT containing a valid algorithm identifier (SHA).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_1_Ve

/* A message is submitted to the IUT containing a valid algorithm identifier (AR/DFP).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_1_Vf

/* A message is submitted to the IUT containing a valid algorithm identifier (ZZZ).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_2_Iv

/* A message is submitted to the IUT containing an invalid algorithm identifier.*/

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_3_Iv

/* A message is submitted to the IUT containing an algorithm identifier which is inconsistent with the use of algorithm (content integrity attack).*/;

EDIS/REC/MCI/AI/EDIS_REC_MCI_AI_4_Iv

/* A message is submitted to the IUT containing an algorithm identifier which is inconsistent with the cryptographic mode of operation (content integrity attack).*/;

EDIS/REC/MCI/ACLI/EDIS_REC_MCI_ACLI_2_Iv

/* A message is submitted to the IUT containing an algorithm code list identifier which is inconsistent with the algorithm identifier (content integrity attack).*/;

EDIS/REC/MCI/AP/EDIS_REC_MCI_AP_2_Iv

/* A message is submitted to the IUT containing a valid algorithm parameter, and an algorithm parameter qualifier which is inconsistent with the algorithm (content integrity attack).*/;

EDIS/REC/MCI/AP/EDIS_REC_MCI_AP_3_Iv

/* A message is submitted to the IUT containing an algorithm parameter which is inconsistent with the algorithm, and a valid algorithm parameter qualifier (content integrity attack).*/;

EDIS/REC/MCI/AP/EDIS_REC_MCI_AP_4_Iv

/* A message is submitted to the IUT containing an algorithm parameter and algorithm parameter qualifier which are both inconsistent with the algorithm (content integrity attack).*/;

EDIS/REC/MCI/SR/EDIS_REC_MCI_SR_1_Iv

/* A message is submitted to the IUT containing an invalid security result in the trailer */;

EDIS/REC/MOA/CMO/EDIS_REC_MOA_CMO_2_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing an invalid cryptographic mode of operation.*/;

EDIS/REC/MOA/CMO/EDIS_REC_MOA_CMO_3_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) for which the cryptographic mode of operation is inconsistent with the use of algorithm identifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/MOCI/EDIS_REC_MOA_MOCI_2_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing a mode of operation code list identifier which is inconsistent with the cryptographic mode of operation (content integrity or masquerade attack).*/;

EDIS/REC/MOA/AI/EDIS_REC_MOA_AI_1_Va

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing a valid algorithm identifier (MAA).*/;

EDIS/REC/MOA/AI/EDIS_REC_MOA_AI_1_Vb

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing a valid algorithm identifier (FEAL).*/;

EDIS/REC/MOA/AI/EDIS_REC_MOA_AI_1_Vc

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing a valid algorithm identifier (IDEA).*/;

EDIS/REC/MOA/AI/EDIS_REC_MOA_AI_2_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing an invalid algorithm identifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/AI/EDIS_REC_MOA_AI_3_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing an algorithm identifier which is inconsistent with the use of algorithm (content integrity or masquerade attack).*/;

EDIS/REC/MOA/AI/EDIS_REC_MOA_AI_4_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing an algorithm identifier which is inconsistent with the cryptographic mode of operation (content integrity or masquerade attack).*/;

EDIS/REC/MOA/ACLI/EDIS_REC_MOA_ACLI_2_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing an algorithm code list identifier which is inconsistent with the algorithm identifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/AP/EDIS_REC_MOA_AP_2_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing a valid algorithm parameter, and an algorithm parameter qualifier which is inconsistent with the algorithm (content integrity or masquerade attack).*/;

EDIS/REC/MOA/AP/EDIS_REC_MOA_AP_3_Iv

/* A message is submitted to the IUT (with use of algorithm identifier set to OSY) containing an algorithm parameter which is inconsistent with the algorithm, and a valid algorithm parameter qualifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2CMO/EDIS_REC_MOA_Gr2CMO_1_Va

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing a valid cryptographic mode of operation (NUL).*/;

EDIS/REC/MOA/Gr2CMO/EDIS_REC_MOA_Gr2CMO_1_Vb

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing a valid cryptographic mode of operation (ZZZ).*/;

EDIS/REC/MOA/Gr2CMO/EDIS_REC_MOA_Gr2CMO_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing an invalid cryptographic mode of operation (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2CMO/EDIS_REC_MOA_Gr2CMO_3_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) for which the cryptographic mode of operation is inconsistent with the use of algorithm identifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2MOCI/EDIS_REC_MOA_Gr2MOCI_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing a mode of operation code list identifier which is inconsistent with the cryptographic mode of operation (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2AI/EDIS_REC_MOA_Gr2AI_1_V

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing a valid algorithm identifier.*/;

EDIS/REC/MOA/Gr2AI/EDIS_REC_MOA_Gr2AI_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing an invalid algorithm identifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2AI/EDIS_REC_MOA_Gr2AI_3_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing an algorithm identifier which is inconsistent with the use of algorithm (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2AI/EDIS_REC_MOA_Gr2AI_4_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing an algorithm identifier which is inconsistent with the cryptographic mode of operation (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2ACLI/EDIS_REC_MOA_Gr2ACLI_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing an algorithm code list identifier which is inconsistent with the algorithm identifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2AP/EDIS_REC_MOA_Gr2AP_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing a valid algorithm parameter, and an algorithm parameter qualifier which is inconsistent with the algorithm (content integrity or masquerade attack).*/;

EDIS/REC/MOA/Gr2AP/EDIS_REC_MOA_Gr2AP_3_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of OCF, OSG or OCS) containing an algorithm parameter which is inconsistent with the algorithm, and a valid algorithm parameter qualifier (content integrity or masquerade attack).*/;

EDIS/REC/MOA/SR/EDIS_REC_MOA_SR_1_V

/* A message is submitted to the IUT containing a valid Gr. 2 security result (content integrity or masquerade attack).*/;

EDIS/REC/MOA/SR/EDIS_REC_MOA_SR_2_Iv

/* A message is submitted to the IUT containing an invalid Gr. 2 security result (content integrity or masquerade attack).*/;

EDIS/REC/NRO/CR/EDIS_REC_NRO_CR_2_Iv

/* A message is submitted to the IUT containing an invalid certificate reference (sender repudiation attack).*/;

EDIS/REC/NRO/KNOW/EDIS_REC_NRO_KNOW_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to OW) containing an invalid key name (repudiation attack).*/;

EDIS/REC/NRO/PIOW/EDIS_REC_NRO_PIOW_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to OW) containing an invalid party identification (repudiation attack).*/;

EDIS/REC/NRO/CLQOW/EDIS_REC_NRO_CLQOW_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to OW) containing an invalid code list qualifier (repudiation attack).*/;

EDIS/REC/NRO/CLRAOW/EDIS_REC_NRO_CLRAOW_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to OW) containing an invalid code list responsible agency (repudiation attack).*/;

EDIS/REC/NRO/KNAX/EDIS_REC_NRO_KNAX_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to AX) containing an invalid key name (repudiation attack).*/;

EDIS/REC/NRO/PIAX/EDIS_REC_NRO_PIAX_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to AX) containing an invalid party identification (repudiation attack).*/;

EDIS/REC/NRO/CLQAX/EDIS_REC_NRO_CLQAX_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to AX) containing an invalid code list qualifier (repudiation attack).*/;

EDIS/REC/NRO/CLRAAX/EDIS_REC_NRO_CLRAAX_2_Iv

/* A message is submitted to the IUT (with security party qualifier set to AX) containing an invalid code list responsible agency (repudiation attack).*/;

EDIS/REC/NRO/CGT/EDIS_REC_NRO_CGT_2_Iv

/* A message is submitted to the IUT containing a certificate generation timestamp which is greater than the current date and time.*/;

EDIS/REC/NRO/CGT/EDIS_REC_NRO_CGT_3_Iv

/* A message is submitted to the IUT containing a certificate generation timestamp which is less than the current date and time.*/;

EDIS/REC/NRO/CVST/EDIS_REC_NRO_CVST_2_Iv

/* A message is submitted to the IUT containing a certificate validity start timestamp which is greater than the current date and time.*/;

EDIS/REC/NRO/CVST/EDIS_REC_NRO_CVST_3_Iv

/* A message is submitted to the IUT containing a certificate validity start timestamp which is less than the current date and time.*/;

EDIS/REC/NRO/CVET/EDIS_REC_NRO_CVET_2_Iv

/* A message is submitted to the IUT containing a certificate validity end timestamp which is greater than the current date and time.*/;

EDIS/REC/NRO/CVET/EDIS_REC_NRO_CVET_3_Iv

/* A message is submitted to the IUT containing a certificate validity end timestamp which is less than the current date and time.*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_1_Va

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid cryptographic mode of operation (MDC2).*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_1_Vb

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid cryptographic mode of operation (HDS1).*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_1_Vc

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid cryptographic mode of operation (HDS2).*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_1_Vd

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid cryptographic mode of operation (SQM).*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_1_Ve

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid cryptographic mode of operation (MCCP).*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_1_Vf

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid cryptographic mode of operation (DSMR).*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_1_Vg

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid cryptographic mode of operation (ZZZ).*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing an invalid cryptographic mode of operation.*/;

EDIS/REC/NRO/CMO/EDIS_REC_NRO_CMO_3_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) for which the cryptographic mode of operation is inconsistent with the use of algorithm identifier.*/;

EDIS/REC/NRO/MOCI/EDIS_REC_NRO_MOCI_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a mode of operation code list identifier which is inconsistent with the cryptographic mode of operation.*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_1_Va

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm identifier (DES).*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_1_Vb

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm identifier (MD4).*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_1_Vc

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm identifier (MD5).*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_1_Vd

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm identifier (RIPEMD).*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_1_Ve

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm identifier (AR/DFP).*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_1_Vf

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm identifier (RAB).*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_1_Vg

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm identifier (ZZZ).*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing an invalid algorithm identifier.*/;

EDIS/REC/NRO/AI/EDIS_REC_NRO_AI_3_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing an algorithm identifier which is inconsistent with the use of algorithm.*/;

EDIS/REC/NRO/ACLI/EDIS_REC_NRO_ACLI_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing an algorithm code list identifier which is inconsistent with the algorithm identifier.*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Va

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (MOD).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vb

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (EXP).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vc

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (MLN).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vd

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR1).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Ve

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR2).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vf

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR3).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vg

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR4).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vh

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR5).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vi

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR6).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vj

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR7).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vk

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR8).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vl

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PR9).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_1_Vm

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and a valid algorithm parameter qualifier (PRA).*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_2_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing a valid algorithm parameter, and an algorithm parameter qualifier which is inconsistent with the algorithm.*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_3_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing an algorithm parameter which is inconsistent with the algorithm, and a valid algorithm parameter qualifier.*/;

EDIS/REC/NRO/AP/EDIS_REC_NRO_AP_4_Iv

/* A message is submitted to the IUT (with Gr. 2 use of algorithm identifier set to one of ISG or IHA) containing an algorithm parameter and algorithm parameter qualifier which are both inconsistent with the algorithm.*/;

EDIS/REC/NRO/SR/EDIS_REC_NRO_SR_1_V

/* A message is submitted to the IUT containing a valid Gr. 2 security result.*/;

EDIS/REC/NRO/SR/EDIS_REC_NRO_SR_2_Iv

/* A message is submitted to the IUT containing an invalid Gr. 2 security result.*/;

EDIS/REC/NRR/RT/EDIS_REC_NRR_RT_2_Iv

/* A message is submitted to the IUT containing an invalid response type.*/;

EDIS/REC/NRR/MUSH/EDIS_REC_NRR_MUSH_2_Iv

/* A message is submitted to the IUT for which each USH has a different response type.*/;

EDIS/REC/ANON/AM/EDIS_REC_ANON_AM_1_V

/* A message is submitted to the IUT where the UNH segment has no sender identification.*/;

2.3.2 Originator tests

Note that many of the originator tests are similar to the recipient tests. Therefore, rather than provide test purposes for these, we present a selection of the more interesting tests. Specifically, these are general security tests, tests of the anonymity service, and tests to check the behaviour of the IUT when it receives an AUTACK message when the non-repudiation of receipt service has been selected.

EDIS/ORG/GEN/SVN/EDIS_ORG_GEN_SVN_1_V

/* The IUT is requested to generate messages containing a range of valid security structure version numbers.*/;

EDIS/ORG/GEN/SVN/EDIS_ORG_GEN_SVN_2_Iv

/* The IUT is requested to generate a message containing an invalid security structure version number.*/;

EDIS/ORG/GEN/OPI/EDIS_ORG_GEN_OPI_1_V

/* The IUT is requested to generate a message with a valid originator identification.*/;

EDIS/ORG/GEN/OPI/EDIS_ORG_GEN_OPI_2_Iv

/* The IUT is requested to generate a message with an originator identification which denotes another originator (masquerade attempt).*/;

EDIS/ORG/GEN/OPI/EDIS_ORG_GEN_OPI_3_Iv

/* The IUT is requested to generate a message with a non-existent originator identification.*/;

EDIS/ORG/MSI/AP/EDIS_ORG_MSI_AP_1_Iv

/* A message is submitted to the IUT for which an AUTACK acknowledgement is requested. However, the acknowledgement is prevented from reaching the IUT (meaning IUT is tricked into replaying original message).*/;

EDIS/ORG/NRR/ASVN/EDIS_ORG_NRR_ASVN_2_Iv

/* The IUT requests the NRR service, and the AUTACK response contains an invalid security structure version number.*/;

EDIS/ORG/NRR/RT/EDIS_ORG_NRR_RT_2_Iv

/* The IUT is requested to generate a message with an invalid response type.*/;

EDIS/ORG/NRR/AICR/EDIS_ORG_NRR_AICR_2_Iv

/* The IUT requests the NRR service, and the AUTACK response contains an interchange control reference which refers to the wrong interchange.*/;

EDIS/ORG/NRR/AICR/EDIS_ORG_NRR_AICR_3_Iv

/* The IUT requests the NRR service, and the AUTACK response contains an interchange control reference which refers to a non-existent interchange.*/;

EDIS/ORG/NRR/Gr3ASDT/EDIS_ORG_NRR_Gr3ASDT_2_Iv

/* The IUT requests the NRR service, and the AUTACK response contains a Gr 3 security date and time which is greater than the current date and time.*/;

EDIS/ORG/NRR/Gr3ASDT/EDIS_ORG_NRR_Gr3ASDT_3_Iv

/* The IUT requests the NRR service, and the AUTACK response contains a Gr 3 security date and time which is older than current date and time window which denotes a fresh message (replay attack).*/;

EDIS/ORG/NRR/ASRL/EDIS_ORG_NRR_ASRL_4_Iv

/* The IUT requests the NRR service, and the AUTACK response (where security function = NRR) contains an invalid security result link.*/;

EDIS/ORG/NRR/ASF/EDIS_ORG_NRR_ASF_1_Iv

/* The IUT requests the NRR service, and the AUTACK response contains an invalid security function.*/;

EDIS/ORG/NRR/AKNMS/EDIS_ORG_NRR_AKNMS_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MS) contains an invalid key name.*/;

EDIS/ORG/NRR/APIMS/EDIS_ORG_NRR_APIMS_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MS) contains an invalid party identification.*/;

EDIS/ORG/NRR/ACLQMS/EDIS_ORG_NRR_ACLQMS_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MS) contains an invalid code list qualifier.*/;

EDIS/ORG/NRR/ACLRAMS/EDIS_ORG_NRR_ACLRAMS_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MS) contains an invalid code list responsible agency.*/;

EDIS/ORG/NRR/AKNMR/EDIS_ORG_NRR_AKNMR_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MR) contains an invalid key name.*/;

EDIS/ORG/NRR/APIMR/EDIS_ORG_NRR_APIMR_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MR) contains an invalid party identification.*/;

EDIS/ORG/NRR/ACLQMR/EDIS_ORG_NRR_ACLQMR_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MR) contains an invalid code list qualifier.*/;

EDIS/ORG/NRR/ACLRAMR/EDIS_ORG_NRR_ACLRAMR_2_Iv

/* The IUT requests the NRR service, and the AUTACK response (with security party qualifier set to MR) contains an invalid code list responsible agency.*/;

EDIS/ORG/NRR/Gr1ASDT/EDIS_ORG_NRR_Gr1ASDT_2_Iv

/* The IUT requests the NRR service, and the AUTACK response contains a Gr 1 date and time which is greater than the current date and time.*/;

EDIS/ORG/NRR/Gr1ASDT/EDIS_ORG_NRR_Gr1ASDT_3_Iv

/* The IUT requests the NRR service, and the AUTACK response contains a Gr 1 date and time which is less than the current date and time.*/;

EDIS/ORG/NRR/ASR/EDIS_ORG_NRR_ASR_1_Iv

/* The IUT requests the NRR service, and the AUTACK response contains an incorrect signature */;

EDIS/ORG/ANON/AM/EDIS_ORG_ANON_AM_1_V

/* The IUT is requested to generate a message where the UNH segment has no sender identification.*/;