NPL Report CISE 6/95

December 1995

Test Suite Structure and Test Purposes for the Security Features of the X.435 Protocol

Stephen Hehir
Centre for Information Systems Engineering
National Physical Laboratory
Teddington
Middlesex
United Kingdom
TW11 0LW

ABSTRACT

The Test Suite Structure and the Test Purposes for the Security Features of the X.435 (Pedi) protocol is developed from the Security Target described in a separate document. The tests are described in English in preparation for a semi-formal description given in a related document. The names given to each test describe its place within the Test Suite Structure.

NPL Report CISE 6/95

ISSN 1361-407X

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

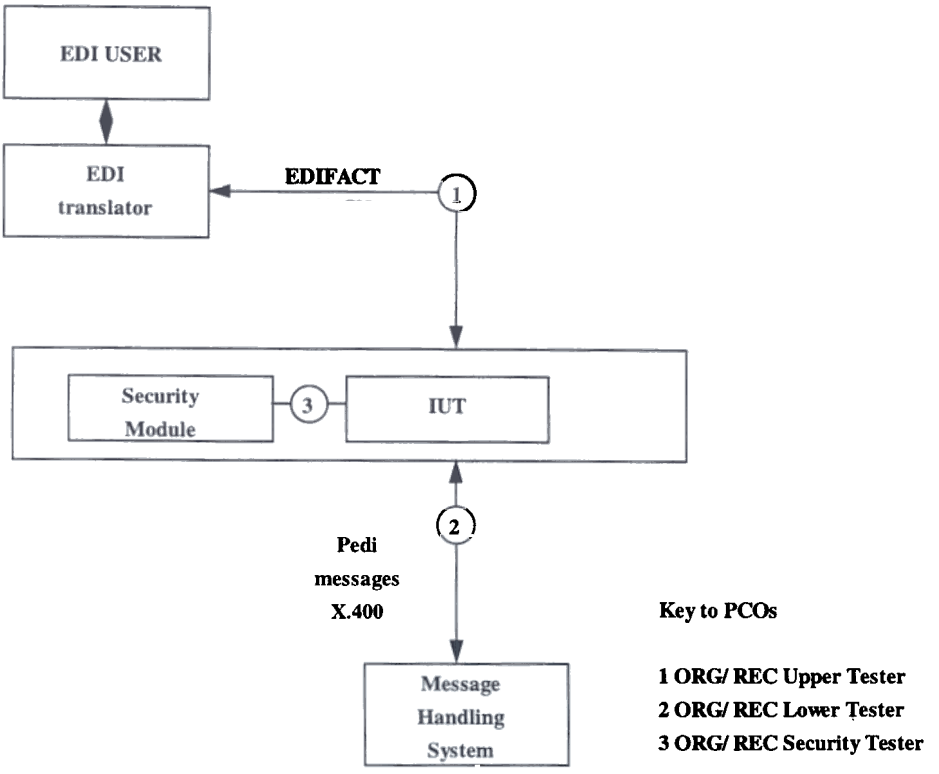
Approved on behalf of the Managing Director of NPL,
by Mr A R Colclough, Director, Centre for Mechanical and Optical Metrology

1. INTRODUCTION

This document defines the Test Suite Structure (TSS) and the Test Purposes (TP) for the Security Features of the Pedi Protocol for transferring EDI messages over a Message Handling System (MHS) conforming to the X.400 Series of Recommendations of 1988 [1] and the X.435 CCITT Standard of 1991 [2]. This document meets the Security Target described in [3] which is concerned with the end-to-end security for EDI messages and not the internal security of the message-handling-system.

2. TEST CONFIGURATION

The Test Configuration concerns the deployment of Points of Control and Observation (PCOs) which enables the examination of all aspects of security of the Implementation Under Test (IUT).



PCOs are located above and below the IUT with an additional PCO (3) for communication between the security module and the IUT.

3 TEST SUITE STRUCTURE AND TEST PURPOSES FOR SECURE PEDI

3.1 LIMITATIONS ON THE SECURITY POLICY

It is necessary that some restrictions be placed on the security policy in force to ensure the achievement of several of the security objectives. These are now listed

1 Data Integrity Required.

1.1. If data integrity is required messages shall not be forwarded with responsibility accepted except by preferred recipients. I.e. only preferred recipients may add or drop body parts from EDIMs. In addition, to comply with §18.8.1 of [2] an MS shall not perform the "forwarding with responsibility accepted" Autoaction.

1.2 The presence of the content-integrity-check, content-integrity-algorithm-identifier, message-sequence-number, message-origin-authentication-check, message-origin-authentication-algorithm-identifier and message-security-label shall be mandatory.

2. Authentication Required.

2.1 Message-security-labels or other mechanisms shall be used so that requested EDINs can be uniquely matched to their subject EDIM.

2.2 The presence of the content-integrity-check, content-integrity-algorithm-identifier, message-sequence-number, message-origin-authentication-check, message-origin-authentication-algorithm-identifier and message-security-label shall be mandatory.

3. Non-Repudiation Required.

3.1 Originator-certificates shall be notarised.

3.2 Content-integrity-check functions may be copied directly into the Content Integrity Check fields of EDINs as stated in §17.1.3 of Ref 2. However, an independent verification of the CIC must be performed for this to help in the non-repudiation security service.

3.3 The presence of the content-integrity-check, content-integrity-algorithm-identifier, message-sequence-number, message-origin-authentication-check, message-origin-authentication-algorithm-identifier and message-security-label shall be mandatory.

4. Confidentiality Required.

4.1 Physical access to passwords, content-confidentiality-keys and the formats of content-confidentiality-algorithm-identifiers shall be restricted.

4.2 Plaintext messages or other information shall not be transmitted together with their encrypted forms, even in the case of asymmetric ciphers

4.3 The presence of the content-confidentiality-algorithm-identifier shall be mandatory.

5. General Requirements.

5.1 The IUT shall maintain the sequence of EDIMs despite the statement in Annex C2.2 of [4]. This does not necessarily place a requirement on the MHS but states that the IUT should recover from messages being delivered out-of-sequence.

5.2 The security policy shall determine the clearances for each originator-recipient pair and for each type of EDIFACT message to be transferred.

5.3 The security policy shall determine the safe distribution of cryptographic keys, where necessary.

5.4 The security policy shall determine which routing addresses to prohibit or allow. Routing addresses shall not be tested.

5.5 It shall form part of the security policy to use content-integrity-check functions which have a performance which is known and adequate for the implementation.

5.6 It shall form part of the security policy to use hash functions for the signed-data of the message-token which have a performance which is known and adequate for the implementation.

5.7 It shall form part of the security policy to use encryption functions for the signed-data of the message-token which have a performance which is known and adequate for the implementation.

3.2 NOTATION & STRUCTURE

Tests are described in the format:

AAAA/BBB/CCC/DDD/EEE/FFF/ggg/HhHh/(No)_Val

where:

AAAA is always PEDI for Pedi tests - i.e. EDI over X.400.

is always SEC to indicate tests regarding the security of Pedi.

is:
REC for recipient
ORG for originator
SEC for the Security Module.

is the security objective:

DIN	Data Integrity	
AUT	Authentication	
NRP	Non-Repudiation	
CFD	Confidentiality	
FSI	Further Security Issues	or

may also have the value:

GEN	General (usually to test syntax).

the threat to the security objective, listed in Section 3 of [2]. (Optional).

is the security service to combat the threat, listed in Section 4 of [2]. (Optional)

is the security element supporting the security service, listed in Section 5 of [2]. (Optional).

HhHh is the argument used by the security element, listed in Section 6 of [2]. (Optional).

(No)_Val is a 2-digit number of the test and whether the test consists of sending a valid message or an invalid message to the IUT. Val takes the values Iv for invalid and V for valid test messages.

*** in any optional field is used where no particular threat, security service, element of argument is referred to.

The structure of the tests is implied by their identifier notation. Although syntax tests are sometimes included, these are generally considered to be part of ordinary conformance testing. There are some inherent assumptions in the tests. For example, it is considered unlikely that some of the threats to data integrity will be guarded against and not others. Again, a requirement for authentication of content will usually go hand-in-hand with a requirement for data integrity, and so on. However, where an evaluator has already performed ordinary conformance testing, the IUT may be tested against any one of the proposed threats without restriction, i.e. independently.

3.3 RECIPIENT TESTS

Objective: **Data Integrity**

Threat: Message Modification

PEDI/SEC/REC/DIN/MMO/CTI/cti/CICh/...
That the IUT can detect when the content of a message it has received has been changed.

/01_Iv
The content-integrity-check is missing from the message-token.

/02_Iv
The content_integrity_check has an incorrect value than that computed through the use of the content-integrity-algorithm-identifier.

/03_Iv
The content-integrity-algorithm-identifier is missing from the content-integrity-check.

/04_Iv
The content-integrity-check is present and in the correct message-token argument but does not have the correct format - i.e. it does not have the correct bit-length.

PEDI/SEC/REC/DIN/MMO/MSI/msi/MSqN...
That the IUT can detect modifications to the message sequence.

/01_V
Two valid EDIFACT messages are sent to the IUT to test whether the message sequence numbers are consecutive.

/02_V
The message-sequence-number has its starting value after the previous message has caused the sequence to restart.

/01_Iv
The message-sequence-number is missing from the message-token.

/02_Iv
The message-sequence-number has a valid format but is the wrong number.

/03_Iv
The message-sequence-number has an invalid bit-length.

Threat: Message addition

PEDI/SEC/REC/DIN/MAD/moa/MOAC/...
It is to be shown that the IUT has the mechanisms in place to detect the possible addition of messages.

/01_Iv
An EDIM is sent to the IUT in which the message-origin-authentication-check is missing.

/02_Iv
An EDIM is sent to the IUT in which the message-origin-authentication-algorithm-identifier is missing from the message-origin-authentication-check.

/03_Iv
An EDIM is sent to the IUT with the wrong value of the message-origin-authentication-check.

PEDI/SEC/REC/DIN/MAD/MOA/moa/MSLb...

/01_Iv
An EDIM is sent to the IUT in which the message-security-label is missing from the MOAC calculation.

/02_Iv
An EDIM is sent to the IUT in which the message-security-label included in the MOAC calculation has the wrong value.

Threat: Message Destruction

PEDI/SEC/REC/DIN/MDS/MSI/msi/MSqN...
It is to be tested whether the IUT can detect that it has not received messages which it should have received.

/01_Iv
A message is deleted from within a sequence of messages.

Threat: Message Replay

PEDI/SEC/REC/DIN/MRE/MSI/msi/MSqN...
It is to be tested whether the IUT can detect message repetitions.

/01_Iv
Two identical valid EDIMs are sent with the same message-sequence-number and message-security-labels.

/02_Iv
A sequence of valid EDIMs is sent to the IUT and this sequence is then sent again within the expiry time of the first sequence.

Threat: Message Preplay

PEDI/SEC/REC/DIN/MPR/MSI/msi/MSqN...
It is to be tested whether the IUT can detect errors in message sequences due to a preplay attack e.g. from copying messages out of a message store.

/01_Iv
A valid EDIM from within a sequence of messages is sent to the IUT thus giving rise to missing sequence numbers.

Threat: Message Re-Ordering within a sequence

PEDI/SEC/REC/DIN/MRO/MSI/msi/MSqN...
It is to be tested whether the IUT can recover from problems in sequence numbering caused by the reordering of messages.

/01_Iv
Two valid EDIMs within a sequence are reversed in order of delivery.

Threat: Message Delay

PEDI/SEC/REC/DIN/MDE/MSI/msi/ExTi...
It is to be tested whether the IUT rejects messages which arrive after their expiry time.

/01_Iv
A valid EDIM is sent to the IUT with an expiry-time less than the current time.

PEDI/SEC/REC/DIN/MDE/MSI/msi/MSqN...
It is to be tested whether message delays are detected by the IUT through errors in message sequencing.

/01_Iv
A valid EDIM from a sequence of valid EDIMs is delayed, causing changes to message sequencing.

Objective: **Authentication**

Threat: False Origination of Message

PEDI/SEC/REC/AUT/FOM/MOA/moa/MOAC...
It is to be tested whether the MOAC mechanism, if used, is properly examined by the IUT.
These are the same tests as for:
PEDI/SEC/REC/DIN/MAD/moa/MOAC/(01-03)_Iv

/01_Iv
An EDIM is sent to the IUT in which the message-origin-authentication-check is missing.

/02_Iv
An EDIM is sent to the IUT in which the message-origin-authentication-algorithm-identifier is missing.

/03_Iv
An EDIM is sent to the IUT with the wrong value of the message-origin-authentication-check.

PEDI/SEC/REC/AUT/FOM/MOA/moa/MSLb...
It is to be tested whether the IUT makes proper use of the message-security-label.

/01_Iv
An EDIM is sent to the IUT in which the message-security-label is missing from the MOAC calculation.

/02_Iv
An EDIM is sent to the IUT in which the message-security-label included in the MOAC calculation has the wrong value.

PEDI/SEC/REC/AUT/FOM/MOA/aux/OrCe...
It is to be tested whether the IUT examines the syntax of the originator-certificate.

/01_Iv
An EDIM is sent to the IUT with an originator-certificate in which the subject-public-key is missing.

/02_Iv
An EDIM is sent to the IUT with an originator-certificate in which the subject-public-key holds the wrong key.

PEDI/SEC/REC/AUT/FOM/MOA/mai/CICh...
It is to be tested whether the IUT makes proper use of the CICh for authentication.

/01_V
A valid EDIM is sent to the IUT in which the message-security label and the content-integrity-check are included in the signed-data of the message-token.

/01_Iv
An EDIM is sent to the IUT in which the content-integrity-check has been included in the signed-data but the message-security-label is not present. This tests whether the association between the content of the message and the message-security-label has been maintained.

Objective: **Non-Repudiation**

Threat: Denial of Origin

PEDI/SEC/REC/NRP/DOR/NRO/mai/CICh
It is to be tested whether the IUT is making proper use of the CICh when meeting the NRO security objective with the signed-data of the message-token.

/01_V
A valid EDIM is sent to the IUT in which the message-security label and the content-integrity-check are included in the signed-data of an asymmetric message-token.

/01_Iv
An EDIM is sent to the IUT in which the content-integrity-check has been included in the signed-data but the message-security-label is not present or is included in the encrypted data of an asymmetric message-token. This tests whether the association between the content of the message and the message-security-label has been maintained.

/02_Iv
An EDIM is sent to the IUT in which the content-integrity-check has been included in the encrypted data but the message-security-label is not present or is included in the signed-data of an asymmetric message-token. This tests whether the association between the content of the message and the message-security-label has been maintained.

/03_Iv
This test purpose applies when:
Content Confidentiality is required.
An EDIM is sent to the IUT in which the content-integrity-check is missing. This ensures that NRO is not being attempted by the MOA security service.

PEDI/SEC/REC/NRP/DOR/NRO/mac/CICh...
It is to be tested whether the IUT is making proper use of the CICh when meeting the NRO security objective with the encrypted-data of the message-token.

/01_V
A valid EDIM is sent to the IUT in which the message-security-label and the content-integrity-check are included in the encrypted-data of an asymmetric message-token.

/01_Iv
An EDIM is sent to the IUT in which the content-integrity-check has been included in the signed-data but the message-security-label is not present or is included in the encrypted data of an asymmetric message-token. This tests whether the association between the content of the message and the message-security-label has been maintained.

/02_Iv
An EDIM is sent to the IUT in which the content-integrity-check has been included in the encrypted data but the message-security-label is missing from the message-token. This tests whether the association between the content of the message and the message-security-label has been maintained.

Objective: **Confidentiality**

Threat: Ambiguous/Insecure Functions

PEDI/SEC/REC/CFD/LOC/CTC/mac/MTed...
It is to be tested whether the IUT gives errors when the mechanisms used to supply confidentiality are missing or misused.

/01_Iv
This test purpose applies when:
Content Confidentiality is required and
Content Confidentiality is achieved by a symmetric key sent with the message.
An EDIM is sent to the IUT with a missing content-confidentiality-algorithm-identifier.

/02_Iv
This test purpose applies when:
Content Confidentiality is required and
Content Confidentiality is achieved by a symmetric key sent with the message.
An EDIM is sent to the IUT with a missing content-confidentiality-key.

/03_Iv
This test purpose applies when:
Content Confidentiality is required and
Content Confidentiality is achieved by a symmetric key sent with the message.
An EDIM is sent to the IUT with an invalid content-confidentiality-algorithm-identifier.

/04_Iv
This test purpose applies when:
Content Confidentiality is required and
Content Confidentiality is achieved by a key not sent with the message.
An EDIM is sent to the IUT with a missing content-confidentiality-algorithm-identifier.

/05_Iv
This test purpose applies when:
Content Confidentiality is required and
Content Confidentiality is achieved by a key not sent with the message.
An EDIM is sent to the IUT with the wrong content-confidentiality-algorithm-identifier.

Threat: Loss of Connection Confidentiality

PEDI/SEC/REC/CFD/LOC/CXC/aux/

The authentication exchange SE provides lower layers with a mechanism for connection confidentiality across each link of the MHS. Tests for this service shall therefore not be included.

PEDI/SEC/REC/CFD/LOC/CTC/ctc/CCAI/...
It is to be tested whether the IUT includes the CCAI.

/01_Iv
An EDIM is sent to the IUT with the CCAI missing.

Threat: Loss of Anonymity

PEDI/SEC/REC/CFD/LOA/MFC/det/CtTy/

/01_V
A valid EDIM is sent to the IUT with the Content Type set to content-is-inner-envelope.

/01_Iv
An invalid EDIM is sent to the IUT in which the Content Type is set to content-is-inner-envelope but the double enveloping technique has not been applied.

N.B. The double enveloping technique does not guarantee anonymity unless it is supported by traffic padding but it is a useful service - therefore, it was felt that, if supplied with the IUT, the double enveloping technique should be tested and work properly.

Threat: Traffic Analysis
This threat cannot be completely eradicated by the use of the double-enveloping technique but if this technique is available it should prove useful and be tested.

PEDI/SEC/REC/CFD/TRA/MFC/det/CtTy/...

As met by PEDI/SEC/REC/CFD/LOA/MFC/det/CtTy/... tests.

Objective: **Further Security Issues**

Most of these issues are outside the considerations of end-to-end security. Denial of Communications can be achieved by flooding the MHS i.e. originating false messages or repeating valid ones and may be thwarted by the security features against those threats. Clearances for the origination of messages is clearly a security policy issue and arranging the proper interpretation of message security labels between two users is an administration issue. Problems of misrouting are internal to the MHS but are best combated with an audit trail on message routes taken to see if they are routed to MTAs where different security policies abide. Tests shall not be included for these issues.

3.4 ORIGINATOR TESTS

Objective: Data Integrity

PEDI/SEC/ORG/DIN/MMO/PNO/cti/CICh...
It is to be tested whether the notification-time is properly examined by the IUT.

/01_Iv
An invalid EDIN (PN) is returned to the IUT as requested with the content-integrity-check argument included in the mai or mac components of the message-token.

The notification-time of the EDIN is < date-and-time-of-preparation of subject EDIM.

/02_Iv
An invalid EDIN (PN) is returned to the IUT as requested with the content-integrity-check argument included in the mai or mac components of the message-token.

The notification-time of the EDIN is > current-time.

PEDI/SEC/ORG/DIN/MRE/PNO/cti/CICh...
It is to be tested whether the IUT automatically replays messages for which no PN nor NN have been received. This may be desirable or undesirable depending on the security policy but shall be assumed undesirable.

/01_Iv
No PN nor NN is received from a valid EDIM although they were requested. The IUT shall not automatically replay the message. This meets threats involving suppression of EDINs.

Threat: Message Re-Ordering within a sequence

PEDI/SEC/ORG/DIN/MRO/MSI/msi/MSqN...
It is to be tested whether the IUT assigns message-sequence-numbers correctly.

/01_V
Several sequences of two valid EDIFACT messages are sent to the IUT to see whether the message-sequence-numbers are assigned in the correct order.

Threat: Message Delay

PEDI/SEC/ORG/DIN/MDE/MSI/msi/ExTi...
It is to be tested whether the IUT compares the notification-time of the EDIN with the expected time.

/01_Iv
An invalid EDIN (PN) is returned to the IUT as requested with the content-integrity-check argument included in the mai or mac components of the message-token.
The notification-time of the EDIN is > expiry-time of the subject EDIM

Objective: **Authentication**

Threat: Falsely Acknowledge Receipt

PEDI/SEC/ORG/AUT/FAR/PCR/cti/Cont...
It is to be tested whether the IUT compares data from EDINs with their subject-EDIM.

/01_Iv
A valid EDIM message (without content-integrity-check) is sent by the IUT with PNs and NNs requested and the Notification Security field set to "Proof", but prior to transmission, the content field of the EDIN is modified by changing the value of 1 bit. The content included with the PN should be found to be at fault when compared with the subject EDIM. This tests whether an originator is made aware of changes to the message content.

PEDI/SEC/ORG/AUT/FAR/PCR/cti/CICh...
It is to be tested whether the IUT compares data from EDINs with their subject-EDIM.

/01_V
This test purpose applies when the content-integrity-check is the mechanism used to authenticate content and Content Confidentiality is not required.
A valid EDIM is sent by the IUT with PNs and NNs requested and the Notification Security field set to "Proof". The content-integrity-check is present. The returning EDIN shall contain the content-integrity-check as copied from the subject EDIM as suggested by the X.435 standard.
The CICh of the EDIN shall be compared to the CICh of the subject EDIM.

/02_V
This test purpose applies when the content-integrity-check is the mechanism used to authenticate content and Content Confidentiality is required.
A valid EDIM is sent by the IUT with PNs and NNs requested and the Notification Security field set to "Proof". The content-integrity-check is present. The returning EDIN shall contain the content-integrity-check of the subject EDIM. This shall be the content-integrity-check as copied from the subject EDIM as suggested by the X.435 standard.
The encrypted CICh of the EDIM shall be compared to the received CICh in the EDIN.

/01_Iv
An EDIM is sent by the IUT with PNs and NNs requested and the Notification Security field set to "Proof", but the content field of the EDIN is modified by changing the value of 1 bit. The content-integrity-check is not included. The content included with the PN should be found to be at fault when compared with the subject EDIM. This tests whether an originator is made aware of changes to the message content.

Objective: **Non-Repudiation**

Threat: Denial of EDI Notification

PEDI/SEC/ORG/NRP/DNO/CTI/cti/CICh...

This threat is met by meeting the DCR threat as next described

Threat: Denial of Content Received

PEDI/SEC/ORG/NRP/DCR/CTI/cti/Cont...
It is to be tested whether the IUT compares data from EDINs with their subject-EDIM and check the originator-certificate.

/01_V
This test purpose applies when the content-integrity-check is not the mechanism used to authenticate content and Content Confidentiality is not required.
A valid EDIM is sent by the IUT with PNs and NNs requested and the Notification Security field set to "Non-Repudiation". The content-integrity-check is not present. The returning EDIN shall contain the full content of the subject EDIM in the original-content field which is compared with the original content of the subject EDIM.
The EDIN's originator-certificate is also checked.

/01_Iv
A valid EDIM is sent by the IUT as above, but the content field of the EDIN is modified by changing the value of 1 bit.

PEDI/SEC/ORG/NRP/DCR/CTI/cti/CICh...
It is to be tested whether the IUT compares data from EDINs with their subject-EDIM and check the originator-certificate.

/01_V
This test purpose applies when the content-integrity-check is the mechanism used to authenticate content and Content Confidentiality is not required.
A valid EDIM is sent by the IUT with PNs and NNs requested and the Notification Security field set to "Non-Repudiation". The content-integrity-check is present. The returning EDIN shall contain the recipient's digitally-signed content-integrity-check of the content of the subject EDIM. This shall be the content-integrity-check as copied from the subject EDIM as suggested by the X.435 standard.
The digitally-signed CICh of the EDIN shall be decrypted by the originator and shall then be compared to the CICh of the subject EDIM.
The EDIN's originator-certificate is also checked.

/02_V
This test purpose applies when the content-integrity-check is the mechanism used to authenticate content and Content Confidentiality is required.
A valid EDIM is sent by the IUT with PNs and NNs requested and the Notification Security field set to "Non-Repudiation". The content-integrity-check is present. The returning EDIN shall contain the recipient's encrypted content-integrity-check of the plaintext content of the subject EDIM i.e. after the recipient's decryption. This shall be the content-integrity-check as copied from the subject EDIM as suggested by the X.435 standard.
The encrypted CICh of the EDIN shall be decrypted by the originator using the algorithm indicated by the EDIN content-confidentiality-algorithm-identifier and shall then be compared to the CICh of the subject EDIM.
The EDIN's originator-certificate is also checked.

/01_Iv
A valid EDIM is sent by the IUT as above (01_V), Content Confidentiality is not required, but the CICh field of the EDIN is modified by changing the value of 1 bit.

/02_Iv
A valid EDIM is sent by the IUT as above (02_V), Content Confidentiality is required, but the CICh field of the EDIN is modified by changing the value of 1 bit.

Objective: **(FSI) Further Security Issues.**

Threat: Ambiguous/Insecure Functions

PEDI/SEC/ORG/FSI/AIF.

/01_Iv
It is to be tested whether the security module gives an error with an invalid content-confidentiality-algorithm-identifier.

3.5 General Tests: Originating EDIMs

PEDI/SEC/ORG/GEN/ORM/...

/01_Iv
An invalid EDIFACT message is sent to the IUT with "Message Type" missing from the UNH segment.

/02_Iv
An invalid EDIFACT message is sent to the IUT with the elements of the "Service String Advice" from the UNA segment disordered.

/03_Iv
An invalid EDIFACT message is sent to the IUT with a missing "Syntax Identifier" from the UNB segment.

/04_Iv
An invalid EDIFACT message is sent to the IUT with a missing "Syntax Version" from the UNB segment.

/05_Iv
An invalid EDIFACT message is sent to the IUT with a missing "Interchange Sender" from the UNB segment.

/06_Iv
An invalid EDIFACT message is sent to the IUT with a UTCTime greater than the current time.

/07_Iv
An invalid EDIFACT message is sent to the IUT with a missing "Application Reference" from the UNB segment.

4 REFERENCES

CCITT Blue Book, Vol VIII. Data Communication Networks - Message Handling Systems. Recommendations X.400 - X.420. 1988.

2. CCITT Data Communication Networks - Message Handling Systems. Recommendation X.435. 1991.

3. A Security Target for the X.435 (Pedi) Protocol. NPL DSG\D\328\V 2.0. Author: S. Hehir. 16\8\95.

4. CCITT Message Handling Service - Operations and Definition of Service. Recommendation F.435. 1991.