NPL Report CISE 3/95

December 1995

A Security Target for the X.435 Protocol

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

ABSTRACT

A security target for the X.435 (Pedi) protocol is developed in terms of possible threats and required services for a range of implementations. This forms the basis for a full test suite to be described in related documents.

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

1 INTRODUCTION

This document defines a partial security target for an implementation of an X.435 protocol specifically for EDI (P_{edi} or Pedi). The target is "partial" in the sense that considerations of physical access, catastrophic failure, loss of service and other such issues are not considered. This security target is therefore derived in terms of the security which can be achieved by virtue of the adherence of a particular implementation to the standards required for conformance to Recommendation X.435. Further security may need to be added outside the limits of this protocol for a desired level of EDI security overall.

All the threats which the X.435 standard aims to meet and the security services it provides are given in sections 3, 4, 5 and 6. In section 7 a subset of these is considered which provides a minimal but complete security target for end-to-end Pedi security.

2 FUNCTIONAL AND ENVIRONMENTAL CONSIDERATIONS

This security target assumes that the X.435 (Pedi) protocol (i.e. not X.435 for P1/0 or P2) is operating over any system where the structure and transmission of electronic mail messages conforms to the 1988 X.400 Series of Recommendations of the CCITT (Ref. 1).

The messaging environment consists of the message handling system (MHS) comprising User Agents (UAs) which are computer programs which accept and initiate messages for users and Message Transfer Agents (MTAs) which actually move these messages from one location to another. In addition there may be Message Stores (MSs) inserted between UAs and MTAs or elsewhere. The network of MTAs form the Message Transfer System (MTS). The user platform and links to the UAs (including, for example the EDIFACT translator) and their inherent insecurities are considered to be outside this MHS environment. It is considered that any particular implementation may use any subset of all those security services which are described by the X.400 Series of Recommendations.

3 SECURITY OBJECTIVES AND THREATS

There are four security objectives to be met by the X.435 standard. Their associated threats are given acronymic references of three letters.

3.1 Data Integrity (DIN):
That the data sent by the originator is precisely the data which arrives at the recipient. Please note that this does not correspond to the category of 'Data Integrity' defined in X.402 but includes the 'Message Sequencing' category given there. Message Addition could, arguably, be part of Origin Authentication.

Threats:	MMO	Message Modification
	MAD	Message Addition
	MDS	Message Destruction
	MRE	Message Replay
	MPR	Message Preplay
	MRO	Message Re-ordering within a sequence
	MDE	Message Delay
	MRC	Message Routing Corruption

3.2. Authentication (AUT):
That the message origin, source or recipient can be confirmed. These threats are known generally under the term of 'Masquerade'.

Threats:		
	IMS	Impersonation & Misuse of the MTS
	FAR	Falsely Acknowledge Receipt
	FOM	False Origination of Message
	IAU	Impersonation of an MTA to an MTS User
	IAA	Impersonation of an MTA to an MTA

3.3. Non-Repudiation (NRP):
That neither the sending nor the receipt of the message can be repudiated at a later date.

Threats:		
	DOR	Denial of Origin & Content Originated
	DSU	Denial of Submission
	DDE	Denial of Delivery
	DNO	Denial of EDI Notification
	DRT	Denial of Retrieval
	DTR	Denial of Transfer
	DCR	Denial of Content Received
	LNA	Lack of EDI Notification Authentication
	LRA	Lack of Retrieval Authentication
	LTA	Lack of Transfer Authentication

3.4. Confidentiality (CFD):
That the disclosure of message contents be made possible only to the intended recipient.

Threats:		
	LOC	Loss of Confidentiality
	LOA	Loss of Anonymity
	MOM	Misappropriation of Messages
	TRA	Traffic Analysis

3.5 Further Security Issues (FSI):
That the ability of the MHS to pass messages and to manage the security of messages is not impaired.

Threats:		
	OCL	Originator Clearance for Message Security Label
	MCL	MTA/MTS Clearance
	DLP	Differing Label Policies
	MRT	Misrouting
	DCM	Denial of Communications
	TAF	MTA Flooding

TSF	MTS Flooding
AIF	Ambiguous/Insecure Functions

Most of the above threats were derived from Table 1 of Annex D of X.402 (Ref. 1) and X.435 (Ref. 2) and fuller definitions can be found in those documents. Other threats have been added as appropriate.

4. PROVISION OF SECURITY SERVICES TO COUNTER THREATS

In this section the security services which are provided by the X.400 Series of Recommendations will be listed according to the threats against which they provide protection. These shall be given an acronym reference and are listed according to the security objective they help to meet.

The basis for this listing is Table 1 of Annex I of X.435 (Ref. 2) which contains enhancements to Table 7 in §10 of X.402 (Ref. 1).

Note that:
1: Non-Repudiation of Content Originated is met by the Non-Repudiation of Origin security service.
2. Non-Repudiation/Proof of Content Received cannot be met by the simple copying of the content integrity check of the subject EDIM into the resultant EDIN (as suggested by X.435) unless it is checked before the EDIN is generated.

Objective: **DIN** Data Integrity

MMO	Connection Integrity	CXI
	Content Integrity	CTI
	Message Sequence Integrity	MSI
MAD	Connection Integrity	CXI
	Content Integrity	CTI
	Message Sequence Integrity	MSI
	Message Origin Authentication	MOA
MDS	Connection Integrity	CXI
	Content Integrity	CTI
	Message Sequence Integrity	MSI
	Message Sequence Integrity	MSI
	Message Sequence Integrity	MSI
	Connection Integrity	CXI
	Content Integrity	CTI
	Message Sequence Integrity	MSI
MRC	None Available Provided by lower layers.	
MDE	Message Sequence Integrity	MSI

Objective: **AUT** Authentication

IMS	Message Origin Authentication	MOA
	Probe Origin Authentication	POA
	Secure Access Management:	
	Peer Entity Authentication/Security Context	PEA/SCX
	Proof of Delivery	PDE
FOM	Message Origin Authentication	MOA
	Proof of Submission	PSU
	Report Origin Authentication	ROA
	Report Origin Authentication	ROA
	Secure Access Management:	
	Peer Entity Authentication/Security Context	PEA/SCX

Objective: **NRP** Non-Repudiation

	Non-Repudiation of Origin	NRO
DSU	Non-Repudiation of Submission	NRS
	Non-Repudiation of Delivery	NRD
DNO	Non-Repudiation of EDI Notification	NRN
DRT	Non-Repudiation of Retrieval	NRR
	Non-Repudiation of Transfer	NRT
	Non-Repudiation of Content	NRC
	Proof of EDI Notification	PNO
	Proof of Retrieval	PRT
LTA	Proof of Transfer	PTR

Objective: **CFD** Confidentiality

LOC	Connection Confidentiality	CXC
	Content Confidentiality	CTC
LOA	Message Flow Confidentiality	MFC
MOM	Secure Access Management:	
	Peer Entity Authentication/Security Context	PEA/SCX
TRA	Message Flow Confidentiality	MFC

Objective: **FSI** Further Security Issues

Secure Access Management:	
Peer Entity Authentication/Security Context	PEA/SCX
Message Security Labelling	MSL
Secure Access Management:	
Peer Entity Authentication/Security Context	PEA/SCX
None Available	
Secure Access Management:	
Peer Entity Authentication/Security Context	PEA/SCX
Message Security Labelling	MSL

DCM None Available

None Available

None Available

Encryption/Decryption/Digital Signature/Hash Functions

In addition, as part of the management of the security system to meet these threats there are also:

Security Management Services:	
Change Credentials	SCC
Register	SRG
MS-Register	SSR

Please note that §10 of X.402 (Ref. 1) specifies that the use of encryption should be supported where required.

5. PROVISION OF SECURITY MECHANISMS TO SUPPORT SERVICES

There now follows a listing of all those mechanisms and security elements (SEs) which are required to support particular security services. Because these services can sometimes be useful against several threats, they are given in alphabetical order of the acronym. Those services marked † shall not form part of this security target for the reasons supplied in the notes provided.

CTI Content Integrity

Overall Service Mechanism
Encryption
Digital Signature
Hash Function

Security Elements

Content Integrity SE	cti
Message Argument Integrity SE	mai
Message Argument Confidentiality SE	mac
Message Origin Authentication SE	moa

Content Confidentiality

Overall Service Mechanism
Message Content Encryption

Security Elements

Content Confidentiality SE	ctc
Message Argument Confidentiality SE	mac

Connection Integrity

Overall Service Mechanism
Only available by implementing lower layer security. Some assurance given by Authentication Exchange SE (see PEA) and receipt of EDINs.
This service shall not form part of this security target.

Security Elements
None available

CXC † Connection Confidentiality

Overall Service Mechanism
Only available by implementing lower layer security.
Some assurance given by Authentication Exchange SE (see PEA).
This service shall not form part of this security target.

Security Elements
None available

MFC † Message Flow Confidentiality

Overall Service Mechanism
Requires that a 'Double Enveloping' technique be included in the implementation whereby a complete message is included within another message to hide addressing information. Also requires 'traffic padding' which is beyond the scope of X.402.
This service shall therefore not form part of this security target.

Security Elements

Double Enveloping Technique	det

MOA Message Origin Authentication

Overall Service Mechanism
Encryption
Hash Function
Signed-Data within Message Token

Security Elements
Message Origin Authentication SE moa
Message Argument Integrity SE mai

Message Sequence Integrity

Overall Service Mechanism
Security Reference Number
Encryption
Signed-Data within Message Token

Security Elements
Message Sequence Integrity SE msi
Message Argument Integrity SE mai
Message Argument Confidentiality SE mac

Message Security Labelling Service

Overall Service Mechanism
Security Labels attached to all entities within the MHS for the implementation of the Security Policy.

Security Elements
Message Security Label SE msl

Non-Repudiation of Content

Overall Service Mechanism
EDI Notification Requests
Non-Repudiation of Origin security service (NRO)
Proof of EDI Notification security service (PNO)
Hash Function
Encryption
Notarisation

Security Elements
As required by the NRO and PNO security services.

NRD Non-Repudiation of Delivery

Overall Service Mechanism
Proof of Delivery Request by the Originator to the Recipient.
Provided by the Proof of Delivery security service.

Security Elements
Proof of Delivery SE pde

Non-Repudiation of Origin

Overall Security Mechanism
Encryption

Hash Function

Security Elements

Content Integrity SE	cti
Message Argument Integrity SE	mai
Message Argument Confidentiality SE	mac
Message Origin Authentication SE	moa

NRN Non-Repudiation of EDI Notification

Overall Service Mechanism
Uses Non-Repudiation of Origin and Submission (NRO and NRS) on the EDIN.
Encryption
Hash Function

Security Elements
As required by the NRO and NRS security services.

NRR † Non-Repudiation of Retrieval

Overall Service Mechanism
Provided by Service Primitives of F.435 (Ref. 3).
This service shall not form part of this security target

Security Elements
None available

Non-Repudiation of Submission

Overall Service Mechanism
Request for Proof of Submission

Security Elements
Proof of Submission SE psu

NRT † Non-Repudiation of Transfer

Overall Service Mechanism
Provided by Service Primitives of F.435 (Ref. 3).
This service shall not form part of this security target.

Security Elements
None available.

Proof of Delivery

Overall Service Mechanism
Request for Proof of Delivery

Security Elements
Proof of Delivery SE

PEA Peer Entity Authentication

Overall Service Mechanism
Passwords
Encrypted tokens

Security Elements
Authentication Exchange SE aux

PNO Proof of EDI Notification

Overall Service Mechanism
Examination of the Content Integrity check of the EDI Notification.

Security Elements
Content Integrity SE cti
Message Argument Confidentiality SE mac
Message Argument Integrity SE mai

POA Probe Origin Authentication

Overall Service Mechanism
Encryption
Hash Function

Security Elements
Probe Origin Authentication SE

PRT † Proof of Retrieval

Overall Service Mechanism
Provided by Service Primitives of F.435 (Ref. 3).
This service shall not form part of this security target.

Security Elements
None available

PSU Proof of Submission

Overall Service Mechanism
Request for Proof of Submission.
Hash Function on message, Message Submission Identifier, Message Submission Time.

Security Elements
Proof of Submission SE psu

PTR † Proof of Transfer

Overall Service Mechanism
Provided by Service Primitives of F.435 (Ref. 3).
This service shall not form part of this security target.

Security Elements
None available

ROA Report Origin Authentication

Overall Service Mechanism
To be determined.

Security Elements
Report Origin Authentication SE roa

Change Credentials

Overall Service Mechanism
As determined by the Security Policy.

Security Elements
Change Credentials SE chc

Security Context

Overall Service Mechanism
Limitation of the passage of messages as determined by the Security Policy using Security Labels provided by the MSL security service.

Security Elements
Security Context SE scx
Register SE srg

Register

Overall Service Mechanism
As determined by the Security Policy for the MTS-user.

Security Elements
Register SE srg

SSR MS-Register

Overall Service Mechanism
As determined by the Security Policy for the MS-user.

Security Elements
Security labels shall be provided for the MS User.

6. SECURITY ELEMENTS USED TO PROVIDE SECURITY SERVICES.

The following security elements are used to provide security services. They are listed in alphabetical order of the acronym. The way in which they do this, i.e. their 'Detailed Security Mechanism', is given in §10.3 of X.402 (Ref. 1). These security elements often work by providing message arguments in the message envelope (see §8.2.1.1.1 of X.411 in Ref. 1) and these are specified where this is the case.

	Authentication Exchange SE	
	Arguments:	
	Initiator Credentials	InCr
	Responder Credentials	ReCr
	Originator-certificate	OrCe
chc	Change Credentials SE	
	Arguments:	
	None	
cti	Content Integrity SE	
	Arguments:	
	Content Integrity Check	CICh
	Content Confidentiality SE	
	Arguments:	
	Content Confidentiality Algorithm Identifier	CCAI
	Double Envelope Technique	
	Arguments:	
	Content Type	CnTy
mac	Message Argument Confidentiality SE	
	Arguments:	
	Message Token: all arguments	MTok_all
mai	Message Argument Integrity SE	
	Arguments:	
	Message Token	MTok_all
moa	Message Origin Authentication SE	
	Arguments:	
	Message Origin Authentication Check	MOAC
msi	Message Sequence Integrity SE	
	Arguments:	
	Message Token: message_sequence_number	MTok_msn
msl	Message Security Label SE	
	Arguments:	
	Message Security Label	MSLb
	Message Token: message_security_label	MTok_msl
pde	Proof of Delivery SE	
	Arguments:	
	Proof of Delivery Request	PDeR

Probe Origin Authentication SE
Arguments:
Probe Origin Authentication Check POAC

Proof of Submission SE
Arguments:
Proof of Submission Request PSuR

Report Origin Authentication SE
Arguments:
Report Origin Authentication Check ROAC

Security Context SE
Arguments:
Message Security Label MSLb

Register SE
Arguments:
To be confirmed.

7. THE DEFINITION OF THE SECURITY TARGET

The previous sections have indicated how an implementation of X.435 security for EDIFACT messages might be achieved using the security services and security elements provided by X.435 and its supporting standards. Many of these services however, are concerned with security over some link of the MHS and do not provide evidence of security outside this link. One example is the Proof of Submission Service which only guarantees that a message was passed from the UA to the MTS and has no information that it was transferred through the MTS to the recipient. The Proof of Transfer and Delivery services also need to be invoked to give security comfort.

However, use of a smaller subset of the available services and judicious use of EDI Notifications can give confirmation of the required security objectives from end-to-end and the security target shall be limited to these services alone.

This approach reflects the fact that, in practice, an originator of EDIFACT messages may not have influence over the security of the MHS that is used and may wish to impose security on a 'per message' basis with methods that will guarantee a given level of security over the whole life of the message.

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 made explicit in Ref. 4.

Since the implementation of security in X.435 is entirely optional it shall be the choice of the implementation which services shall be supplied. Some threats cannot be met by X.435/X.400 services alone and these threats have therefore been excluded. This security target shall consider the following subset:

Data Integrity (DIN):

Threats:	MMO	Message Modification
	MAD	Message Addition
	MDS	Message Destruction
	MRE	Message Replay
	MPR	Message Preplay
	MRO	Message Re-ordering within a sequence
	MDE	Message Delay

Authentication (AUT):

Threats:	FAR	Falsely Acknowledge Receipt
	FOM	False Origination of Message

Non-Repudiation (NRP):

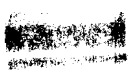
Threats:	DOR	Denial of Origin & Content Originated
	DNO	Denial of EDI Notification
	DCR	Denial of Content Received
	LNA	Lack of EDI Notification Authentication

Confidentiality (CFD):

Threats:	LOC	Loss of Confidentiality
	LOA	Loss of Anonymity

Further Security Issues (FSI):

Threats:	AIF	Ambiguous/Insecure Functions



8. REFERENCES

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

4. Test Suite Structure and Test Purposes for the Security Features of the X.435 (Pedi) Protocol. DSG\D\332\V 1.0. Author: S.Hehir. 30/9/95.