The ATM Forum

Technical Committee

UNI Signaling 4.0 Security Addendum

AF-CS-0117.000

May, 1999

The ATM Forum
Worldwide Headquarters
2570 West El Camino Real, Suite 304
Mountain View, CA 94040-1313
Tel:+1-650-949-6700
Fax: +1-650-949-6705

Acknowledgments

The editor would like to acknowledge the members of the CS working group and the Security working group who have contributed to this document during the meetings, via email and with written contributions. The following members have made significant contribution to this effort:

Malcolm Wiles (CS WG Chairperson)

Robert B. Dianda

Rob Rennison

Richard F. Graveman (Security WG Chairperson)

Tom Tarman

Brian Rosen

The assistance of these members and all who participated in the ATM UNI Signaling 4.0 Security Addendum is greatly appreciated

Carter Bullard, Editor

Table of Contents

1. Introduction

This document is the Security Addendum to the ATM User-Network Interface (UNI) Signaling Specification Version 4.0 [SIG 4.0]. This document describes additional optional capabilities to basic point-to-point and point-to-multipoint calls. This document defines extensions to messages, an additional information element, and UNI signaling procedures to support security services.

The ATM Security Specification, Version 1.0 [SEC 1.0], specifies a collection of security services for ATM VC/VPs. The concepts and reference models for ATM security services and their impact on ATM signaling are described in detail in the ATM Security Specification.

Security services are provided by the ATM Security Agent. An ATM security agent is an abstract object that provides the methods needed to initiate and maintain the collection of ATM security services outlined in the ATM Forum Security Specification [SEC 1.0]. The procedures outlined in this document are a specification for an implementation of the ATM security agent function with respect to UNI Signaling.

The ATM Forum security agent provides a number of security services and mechanisms that may have either direct or indirect impacts on existing UNI 4.0 signalling procedures. Section 2.3 of [SEC 1.0] decomposes the functions of the Security Agent into four components. Of these components, SA_{sme} includes the functions of the Security Agent that perform the Security Message Exchange. SA_{sme} functions can be categorized into three basic types; those that should be processed prior to, during, and after the existing set of UNI 4.0 signalling procedures. These security agent functions are shown in the reference models in [SEC 1.0], Sections 3.1, 3.2, and 3.3. The Security Specification Version 1.0 [SEC 1.0] control plane security services and the In-Band security message exchange procedures of the security agent do not require modification to the existing UNI 4.0 signalling procedures.

2. References

[SIG 4.0] ATM Forum Technical Committee, “User-Network Interface (UNI) Signalling Specification”, Version 4.0, af-sig-0061.000, ~~April~~ July 1996.

[SEC 1.0] ATM Forum Technical Committee, “ATM Security Specification Version 1.0”, AF-SEC-, 0100.001, February, 1999. ~~(Note 1)~~

[Q.850] ITU-T Q.850 Usage Of Cause And Location In The Digital Subscriber Signalling System No. 1 And The Signalling System No. 7 ISDN User Part, March 1993

[Q.2931] ITU-T Q.2931 B-ISDN DSS2 User-Network Interface (UNI) Layer 3 Specification for Basic Call/Connection Control.

[Q.2971] ITU-T Q.2971 B-ISDN DSS2 UNI Layer 3 Specification for Point-to-Multipoint Call/Connection Control.

~~*Note 1* – This document is in course of preparation for publication in 1999.~~

3. Coding Requirements

This section lists the messages and information elements whose contents have been modified to support ATM Security Services capability.

In this specification, subclauses, annexes, appendices, etc. of referenced documents, such as Q.2931, are identified by the actual subclause/annex/appendix number from that document, the document number and the title of the subclause/annex/appendix. For example, an exception to procedures in section 3.1.3 of Q.2931 is identified below by a statement titled "3.1.3/Q.2931 CONNECT".

~~1.1.~~3.1. Basic Point-to-Point Calls

Add the following sections:

3.1.1/Q.2931 ALERTING:
Add the following to Table 3-2/Q.2931:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

3.1.3/Q.2931 CONNECT:
Add the following to Table 3-4/Q.2931:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

3.1.5/Q.2931 RELEASE:
Add the following to Table 3-6/Q.2931:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

3.1.7/Q.2931 SETUP:
Add the following to Table 3-8/Q.2931:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

~~1.2.~~3.2. Point-to-Multipoint Calls

Add the following sections:

8.1.2.1/Q.2971 ADD PARTY:
Add the following to Table 8-10/Q.2971:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

8.1.2.2/Q.2971 ADD PARTY ACKNOWLEDGE:
Add the following to Table 8-11/Q.2971:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

8.1.2.3/Q.2971 PARTY ALERTING:
Add the following to Table 8-12/Q.2971:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

8.1.2.4/Q.2971 ADD PARTY REJECT:
Add the following to Table 8-13/Q.2971:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

8.1.2.5/Q.2971 DROP PARTY:
Add the following to Table 8-14/Q.2971:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

8.1.2.6/Q.2971 DROP PARTY ACKNOWLEDGE:
Add the following to Table 8-15/Q.2971:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

6.6.1.1.3.1/SIG4.0 LEAF SETUP FAILURE:
Add the following to Table 6.5/SIG4.0:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

6.6.1.1.3.2/SIG4.0 LEAF SETUP REQUEST:
Add the following to Table 6.6/SIG4.0:

Information Element name	Reference	Direction	Type	Length
Security Services information element	4	both	O	12-512

~~1.3.~~3.3. Security Service Cause Code

The Diagnostic for Cause #21 is modified as follows:

2.2.6.4/Q.850 CODING OF CALL REJECTED DIAGNOSTIC
Add the following to the end of Figure 2/Q.850:

Security Exception Diagnostic	x+3* etc. (Note 3)

Note 3 This octet may be present only if the Rejection reason in octet x indicates Security exception.

Add the following codepoint to the Rejection reason (octet x in Table 2/Q.850):

Bits									Meaning
	7	6	5	4	3				
	1	1	1	0	0				Security Exception

Add the following at the end of Table 2/Q.850:

Security Exception Diagnostic (octet x+3)

Coded according to the security service, subject to the maximum length of the Cause information element.

4. Security Service Information Element

This section describes a new information element for the Security Services capability. The purpose of the Security Services Information Element (SSIE) is to exchange security relevant information between peer ATM Forum security agent functions, as defined in Section 5.1 of the ATM Forum Security Specification [SEC 1.0]. The SSIE is used to transport messages between ATM Forum security agents to initiate and establish a diverse set of ATM security services that may be employed on a single VC. The format of the SSIE is defined in this document, and the contents of the SSIE fields that are intended for the ATM security agent function are described in detail in Section 5.1.3 of [SEC 1.0]. The contents of the SSIE shall not be modified by any entity other than an ATM Forum security agent in the ATM network.

The minimum size of the SSIE is 12 bytes. The maximum length of the SSIE, when used in signaling is 512 octets, allowing 508 octets of security information. Only one instance of the Security Services Information Element can exist in a signaled message.

<table>
<tr><td colspan="8">Bits</td><td></td></tr>
<tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>Octets</td></tr>
<tr><td colspan="8">Security Services Information Element</td><td rowspan="2">1</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td colspan="8">Information element identifier</td><td rowspan="2">2</td></tr>
<tr><td rowspan="2">1
Ext</td><td rowspan="2">Coding
Standard</td><td colspan="4">Information Element Instruction Field</td></tr>
<tr><td>Flag</td><td>Reserved</td><td colspan="2">Information Element Action Indicator</td></tr>
<tr><td colspan="8">Length of Security Services Information Element</td><td>3</td></tr>
<tr><td colspan="8">Length of Security Services Information Element (cont.)</td><td>4</td></tr>
<tr><td colspan="8">Further content as defined in [SEC 1.0]</td><td>5 – N.n</td></tr>
</table>

Coding standard (octet 2)

Bits								Meaning
	7	6						
	1	1						ATM Forum specific

5. Signalling Procedures in Support of Security Services

This section describes the call/connection control procedures to support the establishment of ATM security services. The procedures for basic call/connection control as described in section 2 of [SIG 4.0] shall apply. Only additional procedures to handle the point-to-point and point-to-multipoint call/connections that use ATM security services are described in this section.

Upon receipt of a message, if there is a security agent present, the signaling entity shall send the message to the SA_{sme} immediately after entering the appropriate state, eg. N1 in the case of a SETUP message and updating appropriate timers, but prior to any other processing of the message. The SA_{sme} shall either return a possibly modified message, or an indication to reject the call, together with the cause #21 "Call Rejected", with the rejection reason indicating Security Exception, and a diagnostic, as specified in [SEC 1.0]. If the SA_{sme} does not reject the call, the signaling entity shall progress the message received from the SA_{sme}.

Prior to transporting a message, if there is a security agent present, the signaling entity shall send the message to the SA_{sme}. The SA_{sme} will either return a possibly modified message, or return an indication to reject the call together with the cause #21 "Call Rejected", with the rejection reason indicating Security Exception, and a diagnostic. If the SA_{sme} does not reject the call, the signaling entity shall transmit unchanged the message received from the SA_{sme} to its peer.

Implementation Note: The SA_{sme} may not return a message sent to it for an extended period of time. For example, it may hold a CONNECT message while an In-Band Security Message Exchange is completed. Implementation of the sending primitives between the signaling entity and the SA_{sme} may need to be asynchronous.

When there is no security agent present, and an SSIE is present in a received message, if the signaling entity is an ATM endpoint, the SSIE shall be discarded, otherwise the SSIE shall be progressed with the message without modification.

If the Security Services information element cannot be transported because of interworking considerations, the call shall progress without the SSIE.