The ATM Forum

Technical Committee

Addendum to Security Specification v1.1 – In-Band Security for Simplex Connections

af-sec-0187.000

July 2002

The ATM Forum
Worldwide Headquarters
572 B Ruger Street
San Francisco, CA 94129-0920
Tel: +1.415.561.6275
Fax: +1.415.561.6120

Acknowledgments

The production of this specification would not be possible without the enormous amount of effort provided by many individuals. Special acknowledgements for their hard work and dedication go to Richard Graveman and Wolfgang Klasen, the current chair and vice-chair.

In addition, the following individuals (listed alphabetically), among others, contributed their time and expertise to the development of this specification:

Asher Altman
Kim Hebda
Jeffery See
Thomas Tarman
Edward Witzke

Preface

This specification uses three levels for indicating the degree of compliance necessary for specific functions, procedures, or coding. They are indicated by the use of key words as follows:

- **Requirement:** "Shall" indicates a required function, procedure, or coding necessary for compliance. The word "shall" used in text indicates a conditional requirement when the operation described is dependent on whether or not an objective or option is chosen.
- **Objective:** "Should" indicates an objective which is not required for compliance, but which is considered desirable.
- **Option:** "May" indicates an optional operation without implying a desirability of one operation over another. That is, it identifies an operation that is allowed while still maintaining compliance.

Table of Contents

1 Introduction

This addendum extends the in-band security establishment mechanism specified in [1] to support simplex connections. The in-band security approach in [1] is only supported on duplex connections.

The signaling-based security mechanism defined in [1] does not support the Three-Way Security Message Exchange (SME) protocol. Therefore, signaling-based security cannot support algorithm negotiation or certificate exchange and requires time synchronization. The main reason for this limitation is that the number of end-to-end flows (messages) that are required to support these services does not match the number of end-to-end flows in signaling. These services require three signaling flows and an acknowledgment flow. Adding a fourth flow to the signaling protocols to support security would solve this problem but would have a larger impact than the approach listed here.

The simplex in-band approach, specified herein, supports the use of the Three-Way SME protocol for securing simplex VCs (that is, VCs with zero return bandwidth). This approach uses the in-band mechanism specified in [1], which solves the limitations of the signaling approach (which was previously the only approach available for securing simplex VCs). However, to support the in-band SME protocol, the intervening network and security agents must support and establish duplex VCs. Furthermore, since this mechanism uses the Security Services Information Element (SSIE) in signaling messages, the network that connects the Security Agents (SAs) must support transport of the SSIE in signaling.

The in-band simplex security approach is named such because the SME protocol is not performed in signaling, but “in-band” on a separate temporary duplex connection.

1.1 References

[1] ATM Forum Technical Committee, “ATM Security Specification”, Version 1.1, af-sec-0100.002, March 2001.

[2] ATM Forum Technical Committee, “User-Network Interface (UNI) Specification,” Version 3.1, af-uni-0010.002, September 1994.

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

[4] ATM Forum, “UNI Signaling 4.0 Security Addendum,” af-cs-0117.000, May 1999.

1.2 Abbreviations and Acronyms

SCSS - Simplex Connection Security Setup
SSAI - Simplex Security Association Identifier

2 Changes to Security Specification Version 1.1

The following additions and changes are made to [1].

2.1 Overview

An overview of the concept of in-band security for simplex connections is provided in this section.

Figure 1 shows the signaling for In-band simplex connection security.

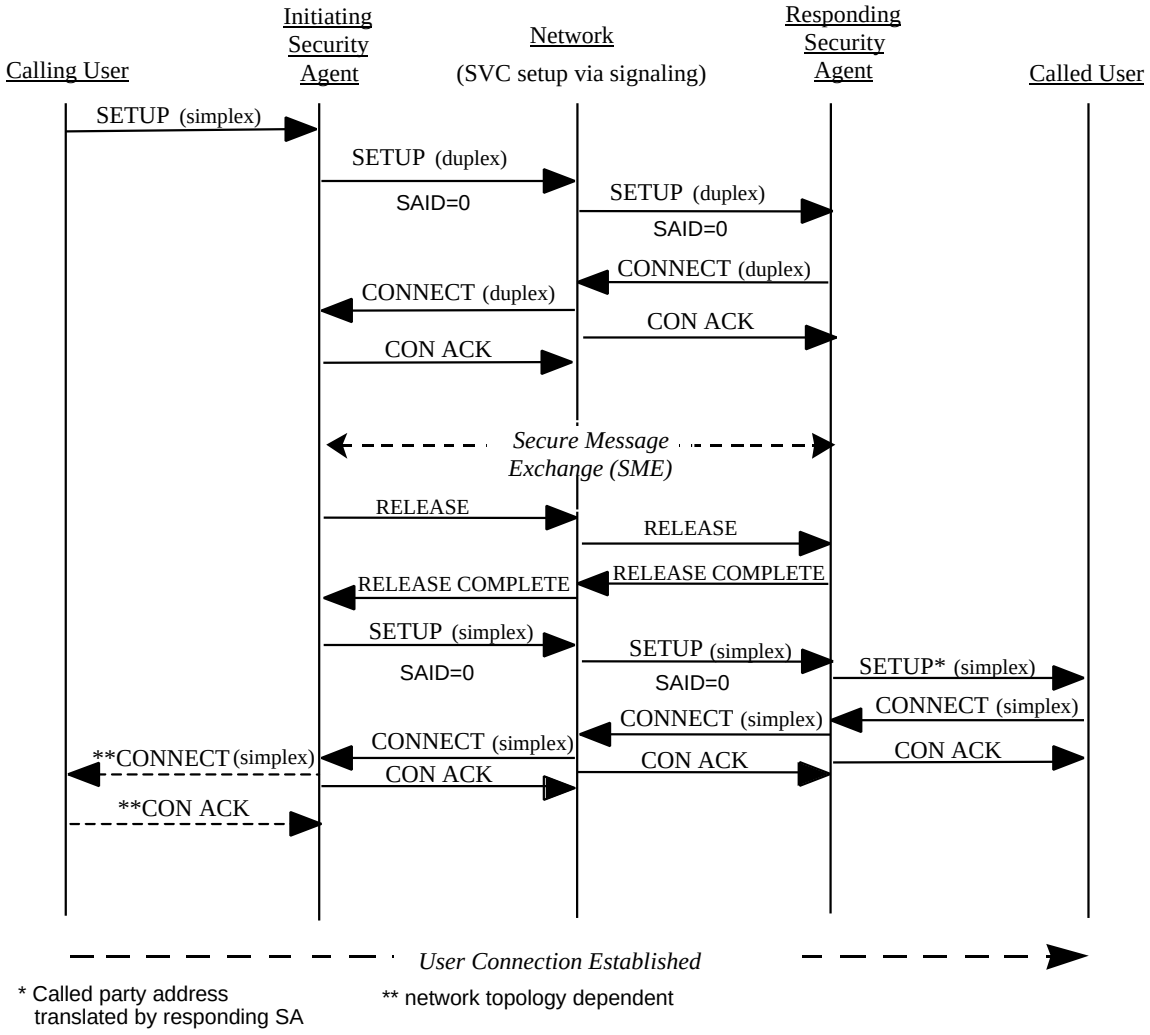

Figure 1: Signaling for In-band Security for Simplex Connections

If security policy dictates a requirement for Three-Way SME and a SETUP message indicates a simplex connection, then the SA at the initiating interface shall hold up the SETUP message. The SA shall initiate a temporary duplex connection to the Called party (destination) address contained in the received SETUP message for the simplex connection. The SA shall include a Security Services Information Element (SSIE) that indicates the SETUP message is for a temporary duplex connection for the purpose of a simplex connection security setup. A new Security Association Section (SAS) type (as defined in Section 2.2 of this document) will be added for this purpose. This new SAS type provides an indication to the remote security agent that intercepts the SETUP message that the normal signaling procedures of forwarding the SETUP message to the Called party (destination) should be altered. The SA at the responding interface shall respond with a CONNECT message and wait for an in-band SME on the temporary duplex connection. A security association for the simplex connection is established over the temporary duplex connection.

The initiating SA, on the receipt of the CONNECT message, initiates an in-band SME. During the in-band SME, the responding SA will assign a Simplex Security Association ID (SSAI) to the security association developed during the exchange. This SSAI is used to correlate the security association developed during the in-band SME performed on the temporary duplex connection, with the simplex connection that will be secured. In FLOW2-3WE of the SME, the responding SA sends its ATM address and the SSAI to the initiating SA. A new octet group (as defined in Section 2.3 of this document) in the SSIE will be added for this purpose. The initiating SA saves the responding SA's ATM address so that it can address the SETUP message for the simplex connection to the same SA that it performed the SME with. The address of the responding SA is needed because in some networks there may be multiple paths (protected by multiple SAs) to the destination. Not forcing the SETUP message for the simplex connection to a specific SA could result in sending the user's traffic to a SA different from the SME participant.

After a successful conclusion of the SME, the initiating SA releases the temporary duplex connection on which it performed the SME and replaces the Called party (destination) address in the received simplex SETUP message with the responding SA's address that it received in FLOW2-3WE of the SME.

The initiating SA also includes a SSIE containing the new SAS type (as defined in Section 2.2 of this document) in the SETUP message. The initiating SA will include (as defined in Section 2.3 of this document) in the SAS the SSAI that it received in FLOW2-3WE of the SME. The initiating SA then forwards the modified SETUP message to the network.

The responding SA, upon receipt of the SETUP message containing its own address (Called party), will examine the SSIE for the SSAI and use it to lookup the previously saved security parameters and destination address associated with the SSAI. It will replace its own address (Called party) that was in the SETUP message with the saved destination address and forward the modified setup message to the destination.

The destination accepts (or rejects) the connection and the initiating and responding SAs complete the simplex connection by relaying the Connect and Connect Acknowledgement messages along the path of the connection. At this point the user may send traffic over the secured simplex connection.

When there are multiple (nested) SA pairs between the source and destination interfaces, the inner SA pairs will secure the temporary duplex connection initiated by the outer SA pairs using the in-band security approach that is contained in [1]. The Relative ID (contains SAID) in the

SSIE is used as a means of addressing a peer SA when there are multiple SAs in the path of the connection.

When a nested initiating SA receives the SETUP message for the simplex connection, it and its peer SA performs the actions as described above for the non-nested SAs.

A signaling diagram for the case when there is one level of nested SAs is shown in Figure 2.

Note that there are three SMEs in the diagram. The inner SA pair performs two SMEs, and the outer SA pair performs one SME. First, on receipt of a simplex connection request from the Calling party, the outer SA pair establishes a temporary duplex connection used to perform a SME to secure the simplex connection. The inner SA pair then performs a SME on the temporary duplex connection to secure the duplex connection using the in-band security exchange procedures as specified in [1]. The outer SA pair then performs a SME, on the temporary duplex connection (secured between the inner SA pair but not the outer SA pair), to develop a security association to secure the simplex connection. The temporary duplex connection is released. The outer initiating SA propagates the simplex setup, and another temporary duplex connection is established between the inner SA pair. The inner SA pair then performs a SME on the second temporary duplex connection, initiated by the inner SA, to develop a security association to secure the simplex connection. The second temporary duplex connection is released, the simplex set up is forwarded to the called user, and a connect message is sent back to the calling user. At this point, the user may send traffic over the secured simplex connection.

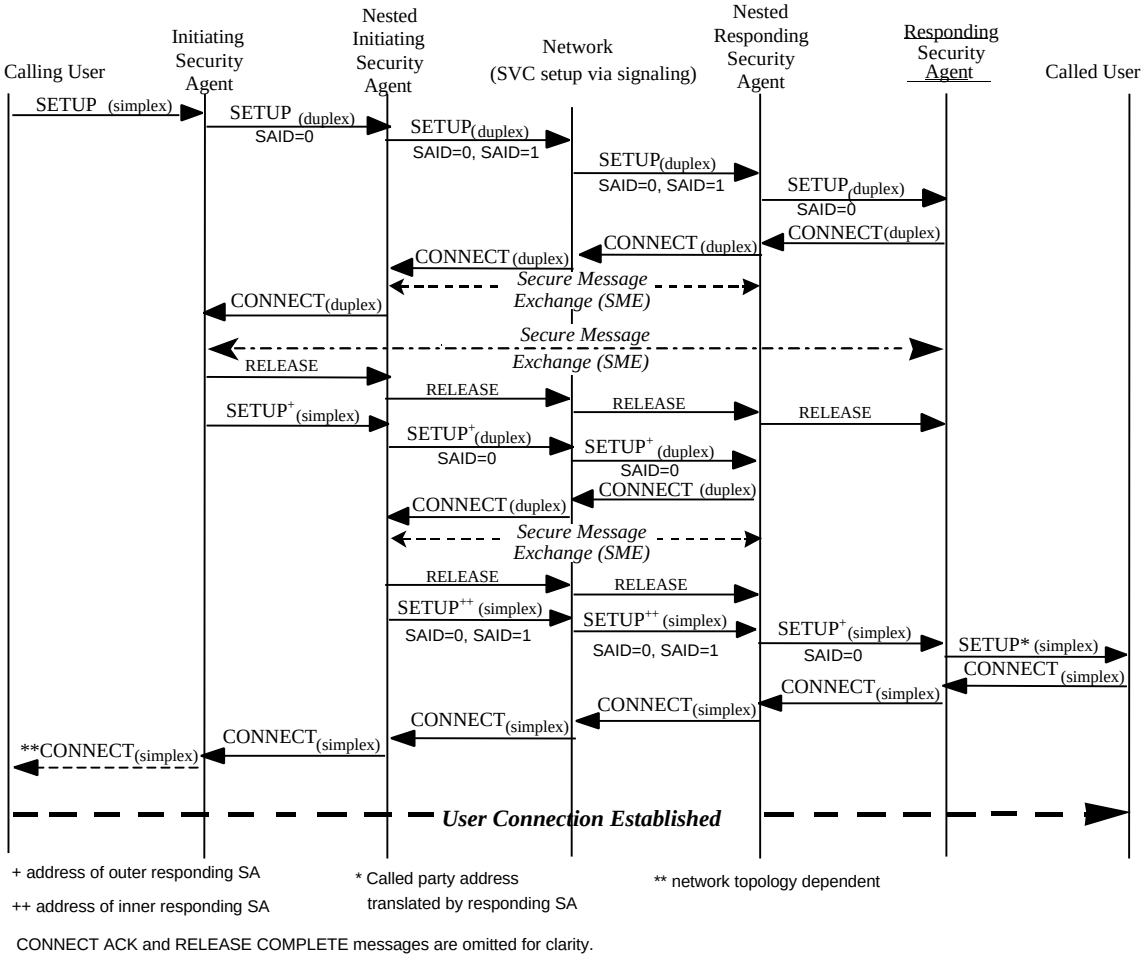

Figure 2: Signaling – Nested Security Agents

2.2 New Security Association Section Type

In Section 5.1.3.2.1 of [1], add the following new Security Association Section Type:

Security Association Section Type

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Meaning**
0	0	0	0	0	0	1	1	ATM Forum Security Service, Simplex Connection Security Setup

The new Simplex Connection Security Setup SAS Type is used in the following three ways:

1. It is used to identify the temporary duplex connection that is used to perform the SME to secure a simplex connection. The initiating SA will set the SAS Type to Simplex Connection Security Setup in the SSIE included in the SETUP message for the temporary duplex connection.

2. It is used to identify the SAS in FLOW2-3WE of the SME performed between the initiating and responding SAs during the temporary duplex connection. The responding SA will assign a SSAI to the security association established for the simplex connection and include the SSAI along with its own ATM address in the Simplex Connection Security Setup SAS contained in the SSIE of FLOW2-3WE of the SME.

3. It is used to identify the SAS in the SSIE included in the SETUP message for the simplex connection. This SAS contains the SSAI for the simplex connection.

2.3 New Simplex Connection Security Setup Data Section

In Section 5.1.3.2.10 of [1], modify the second sentence as follows:

The Security Services Data Section may contain either a security message exchange data section, ~~or~~ label-based access control section, or simplex connection security setup data section.

Add the following new section to [1]:

5.1.3.2.10.3 Simplex Connection Security Setup Data Section

The Simplex Connection Security Setup Data Section is used to transport the SSAI and the responding SA's ATM address from the responding SA to the initiating SA and to transport the SSAI from the initiating SA to the responding SA.

Bits								
8	7	6	5	4	3	2	1	Octet(s)
0	0	1	0	1	0	0	1	
Simplex Connection Security Setup Identifier								5.9
SSAI								5.9.1
SSAI (cont.)								5.9.2
Responder's ATM Address								5.9.3, etc.

SSAI (Octet 5.9.1 and 5.9.2)

This octet contains the Simplex Security Association Identifier assigned to this simplex connection.

Responder's ATM Address (Octet 5.9.3, etc.)

This field contains the ATM address associated with the responding SA. The address is coded as described in ISO 8348, Addendum 2, using the preferred binary encoding. For further details on using this field, consult Section 3.0 of [3].

Add the following entry to Table 18 in Appendix section IV.2 of [1] between codepoint values 00101000 and 00110001:

Codepoint	Reference	Size of Length field	Use of Value field	Name
0010 1001	5.1.3.2.10.3	--	type + data	Simplex Connection Security Setup

2.4 Security Agent Procedures for Simplex Connections

Add the following sections to [1]:

5.1.5.4 Security Agent Procedures for Simplex Connections

5.1.5.4.1 Initiating Security Agent Procedures

5.1.5.4.1.1 Receipt of a SETUP Message for a Simplex Connection

Upon receipt of a SETUP message for a simplex connection, an initiating SA shall:

1. Hold up the received SETUP message.
2. Create a new SETUP message for a temporary duplex connection based on the information contained in the received SETUP message.
3. Set the Called party address in the new SETUP message for the temporary duplex connection to the same value as in the received SETUP message for the simplex connection.
4. Determine whether the received SETUP message contains a SSIE and:
    a. if false – include a SSIE, that contains a SAS Type set to SCSS, in the new SETUP message.
    b. if true – add a new SAS to the SSIE with SAS Type set to SCSS.
5. Assign a value to the SAID in the Relative ID field of the new SAS as described in [1].
6. Forward the new SETUP message for the temporary duplex connection to the network.

5.1.5.4.1.2 Receipt of a SETUP Message for a Temporary Duplex Connection

Upon receipt of a SETUP message for a temporary duplex connection, an initiating SA shall:

1. Add a new SAS to the SSIE with SAS Type set to SCSS.
2. Assign a value to the SAID in the Relative ID field of the new SAS as described in [1].
3. Forward the SETUP message for the temporary duplex connection, which includes the SSIE containing the added SAS, to the network.

Note: The only way an initiating SA will receive a SETUP message for a temporary duplex connection is if it is initiating an inner nested association.

5.1.5.4.1.3 Receipt of a CONNECT Message for a Temporary Duplex Connection

Upon receipt of a CONNECT message for a temporary duplex connection, containing a SSIE with a SAS Type that is set to SCSS, an initiating SA shall inspect the SSIE and:

1. If the SSIE contains SCSS Type SASs with no SAID values greater than zero (0),
    a. perform the relative ID procedures as described in [1].
    b. initiate the in-band SME protocol with its peer SA as described in [1] for the desired security services.
    c. modify the processing of FLOW2-3WE of the SME to include an examination of the Simplex Connection Security Setup Data Section in the SSIE contained in FLOW2-3WE.
    d. extract the ATM address of its peer SA and the Simplex Security Association Identifier (SSAI) from the Simplex Connection Security Setup Data Section in the SSIE contained in FLOW2-3WE and retain them for subsequent use (see (f) and (i) below).
    e. upon successful completion of the SME, release the temporary duplex connection.
    f. modify the original SETUP message for the simplex connection to change the Called party address to its peer SA's address (obtained as described in (d) above).
    g. determine if the received SETUP message contains a SSIE and:
        i. if false – include a SSIE, that contains a SAS Type set to SCSS, in the modified SETUP message.
        ii. if true – add a new SAS to the SSIE with SAS Type set to SCSS.
    h. assign a value to the SAID in the Relative ID field of the new SAS as described in [1].
    i. include the SSAI (obtained as described in (d) above) in the Simplex Connection Security Setup Data Section of the new SAS.
    j. forward the SETUP message for the simplex connection to the network.

2. If the SSIE contains a SCSS Type SAS with a SAID value greater than zero (0),
    a. perform the relative ID procedures in [1].
    b. initiate the in-band SME protocol with its peer SA as described in [1] for the desired security services.
    c. upon successful completion of the SME, pass on the CONNECT message as modified by the relative ID procedures as described in [1].

5.1.5.4.2 Responding Security Agent Procedures

5.1.5.4.2.1 Receipt of a SETUP Message for a Temporary Duplex Connection

Upon receipt of a SETUP message, for a temporary duplex connection, containing a SSIE with a SAS Type that is set to SCSS, a responding SA shall inspect the SSIE and:

1. If the SSIE contains SCSS Type SASs with no SAID values greater than zero (0),
    a. retain the Called party address contained in the SETUP message, but do not forward the message.
    b. respond with a CONNECT message and wait for its peer SA to begin the in-band SME.

c. include a SAS with SAS Type set to SCSS, along with the SASs for other security services, in the SSIE in FLOW2-3WE of the in-band SME.
d. assign a unique SSAI to the security association and include it, along with the ATM address of the responding SA, in the SCSS Data Section of the SCSS SAS described in (c) above.
e. retain the security parameters, i.e., cryptographic keys and algorithms negotiated during the SME for later use on the simplex connection.

2. If the SSIE contains a SCSS Type SAS with a SAID value greater than zero (0), process the SETUP message as described for the relative ID procedures in [1].

5.1.5.4.2.2 Receipt of a SETUP Message for a Simplex Connection

Upon receipt of a SETUP message, for a simplex connection, which contains a SSIE with a SAS Type set to SCSS, a responding SA shall:

1. Perform the relative ID processing as described in [1].
2. For the SCSS Data section of the SCSS SAS that is intended for this responding SA, use the SSAI value to access the security parameters for the simplex connection.
3. Replace the Called party address (its own address) in the SETUP message with the Called party address that was previously saved with the corresponding SSAI.
4. Forward the SETUP message.