ATM Forum Technical Committee
ATM Forum/97-0019

****

TITLE: Proposed Baseline Text for UNI 4.0 Security Addendum

****

SOURCES:

Thomas Tarman*
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185
USA
Phone: +1-505-844-4975
Fax: +1-505-844-9641
Email: tdtarma@sandia.gov

Rao Cherukuri
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC 27709
USA
Phone: +1-919-254-4119
Fax: +1-919-254-5483
Email: raoc@vnet.ibm.com

Mohammad Peyravian
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC 27709
USA
Phone: +1-919-254-7576
Fax: +1-919-254-5483
Email: peyravn@vnet.ibm.com

****

DATE: February 1997, San Diego, CA.

****

DISTRIBUTION: Security, SIG, PNNI, BICI

****

ABSTRACT:

This contribution proposes baseline text for the UNI 4.0 Security Addendum, BTD-SIG-SEC-01.00.

****

****

---

* Mr. Tarman's work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

1. Introduction

This document specifies signaling procedures required to support security services in the Phase I ATM Security Specification [1]. These signaling procedures are in addition to those described in UNI 4.0 Signaling [2].

When establishing point-to-point and point-to-multipoint calls, the call control procedures described in the ATM Forum UNI 4.0 Signaling apply. This document describes the additional information elements and procedures necessary to support security services. This description is in an incremental form with differences from the point-to-point and point-to-multipoint calls with respect to messages, information elements, and signaling procedures.

2. References

[1] ATM Forum/BTD-SEC-01.01, "Phase I ATM Security Specification (DRAFT)," February, 1997.

[2] ATM Forum UNI 4.0 Signaling.

[3] ITU-T Recommendation Q.2931 B-ISDN Point-to-Point Signaling.

[4] ITU-T Recommendation Q.2971 B-ISDN Point-to-Multipoint Signaling.

[5] ITU-T Recommendation Q.2963 B-ISDN Connection Modification Signaling.

3. Definitions

Security Agent The security agent is an entity within the call control plane which is responsible for processing security-related information. As a result of security exchanges, the security agent can elect to accept or reject a call.

4. UNI Signaling Support for Security

4.1 Point-to-Point

The signaling procedures for point-to-point call establishment are described in [2,3,5]. The security message exchange protocols require up to three exchanges [1]. Extension to the ATM signaling specification is defined to support up to three security message exchanges during VCC or VPC establishment phase. This extension largely consists of definition of new information elements (IEs) to carry security-related information.

4.1.1 Modification of Point-to-Point Messages

4.1.1.1 CONNECT

This message is sent by the called user to the network and by the network to the calling user to indicate call acceptance by the called user. See Table 4-1 for additions to the structure of this message from that shown in UNI 4.0 signaling.

Table 4-1: CONNECT Message Additional Contents

DISCLAIMER

Message Type: CONNECT

Significance: Global

Direction: Both

Information Element	Reference	Direction	Type	Length
Broadband Report Type	Q.2963	both	O(1)	4-5
Security Parameters	5.2	both	O(2)	5-?

Note 1 - Included in CONNECT when three-way security information exchange is required.

Note 2 - When required, as described in Section **TBD** of [1], this IE is included in CONNECT to support security information exchange.

4.1.1.2 CONNECTION AVAILABLE

This message is sent from the calling user to the called user to confirm the completion of a call/connection when CONNECT message contains a Broadband report type information element with a Type of Report field coded to "Connection confirm". See Table 4-2 for additions to the structure of this message from that shown in Q.2963.

Table 4-2: CONNECTION AVAILABLE Message Additional Contents

Message Type: CONNECTION AVAILABLE

Significance: Global

Direction: Both

Information Element	Reference	Direction	Type	Length
Security Parameters	5.2	both	O(1)	5-?

Note 1 - When required, as described in Section **TBD** of [1], this IE is included in CONNECTION AVAILABLE to support security information exchange.

4.1.1.3 SETUP

This message is sent by the calling user to the network and by the network to the called user to initiate B-ISDN call and connection establishment. See Table 4-3 for additions to the structure of this message from that shown in UNI 4.0 signaling.

Table 4-3: SETUP Message Additional Contents

Message Type: SETUP

Significance: Global

Direction: Both

Information Element	Reference	Direction	Type	Length
Security Alternate Options	5.2	both	O(1)	5-?
Security Parameters	5.2	both	O(1)	5-?

Note 1 - When required, as described in Section **TBD** of [1], this IE is included in SETUP to support security information exchange.

4.2 Point-to-Multipoint

The signaling procedures for point-to-multipoint call establishment are described in [2,4]. The connection setup for the first party (leaf) in point-to-multipoint connections is the same as the connection setup in point-to-point connections. So, for the first party setup, up to three security message exchanges are supported the same way as in point-to-point connections. The connection setup for the subsequent parties (leaves) only supports up to two security message exchanges.

4.2.1 Modification of Point-to-multipoint Messages

4.2.1.1 ADD PARTY

This message is sent by the calling user to the network and by the network to the called user to add a party to an existing connection. See Table 4-4 for additions to the structure of this message from that shown in UNI 4.0 signaling.

Table 4-4: ADD PARTY Message Additional Contents

Message Type: ADD PARTY

Significance: Global

Direction: Both

Information Element	Reference	Direction	Type	Length
Security Parameters	5.2	both	O(1)	5-?

Note 1 - When required, as described in Section **TBD** of [1], this IE is included in ADD PARTY to support security information exchange.

4.2.1.2 ADD PARTY ACKNOWLEDGE

This message is sent by the called user to the network and by the network to the calling user to acknowledge that the ADD PARTY request was successful. See Table 4-5 for additions to the structure of this message from that shown in UNI 4.0 signaling.

Table 4-5: ADD PARTY ACKNOWLEDGE Message Additional Contents

Message Type: ADD PARTY ACKNOWLEDGE

Significance: Global

Direction: Both

Information Element	Reference	Direction	Type	Length
Security Parameters	5.2	both	O(1)	5-?

Note 1 - When required, as described in Section **TBD** of [1], this IE is included in ADD PARTY ACKNOWLEDGE to support security information exchange.

4.3 Leaf Initiated Join

The signaling procedures for leaf initiated join capability are described in [2].

There are two modes of operation associated with the leaf initiated join capability: root prompted join and leaf prompted join without root notification. The first SETUP message from the root will indicate whether this is the root prompted join or leaf prompted join without root notification.

4.3.1 Root Prompted Join

In this mode of operation, the LIJ (Leaf Initiated Join) request is handled by the root of the connection. The root adds leaves to or removes leaves from a new or established connection using the point-to-multipoint procedures. This type of connection is referred to as a root LIJ connection.

In this mode of operation since the addition (or removal) of a leaf is handled by the root, the point-to-multipoint security procedures described above still apply and no additional enhancement is needed.

4.3.2 Leaf Prompted Join Without Root Notification

In this mode of operation, if the leaf's request is for an existing connection the request is handled by the network. The root is not notified when a leaf is added to or dropped from the connection. This type of connection is referred to as a network LIJ connection.

In this mode of operation since the addition (or removal) of a leaf is not handled by the root, the current point-to-multipoint security procedures described above do not apply. Security support for this mode of operation is not supported.

5. Information Elements

The new and modified information elements for the support of security message exchanges are described in this section. Two new information elements are required to support security: "Security Parameters" and "Security Alternate Options" information elements.

The contents part (i.e., octet 5 and higher) of the security information elements are typically included in the computation of a digital signature, and must remain intact as they travel through the network from the calling party to the called party and vice versa. That is, the network must not change or reorder the contents of octet 5 and higher of the security information elements.

5.1 Broadband Report Type

The purpose of the Broadband Report Type information element is to indicate the type of report requested when included in an appropriate DSS 2 message (e.g. MODIFY ACKNOWLEDGE or CONNECT) when such a report is deemed necessary.

The Broadband report type information element is coded as shown in Figure 1/Q.2963 and Table 8-6/Q.2963. A new codepoint "Connection confirmation" is added to "Type of report" and modified octet 5 coding as shown below.

Type of report (octet 5)

8	7	6	5	4	3	2	1	**Meaning**
0	0	0	0	0	0	0	1	Modification confirmation (NOTE 1)
0	0	0	0	0	0	1	0	Connection confirmation

All other values are reserved

Note 1 - Indicates the addressed user in connection modification requires confirmation of success of the modification.

5.2 Security Parameters

The Security Parameters information element carries the security information required by the security message exchange protocols described in [1] during connection setup. This information element includes security entities identifiers, authentication parameters, security services options, confidential parameters, and access control parameters.

Bits 8	7	6	5	4	3	2	1	Octets
x	x	x	x	x	x	x	x	1
Security Parameters Information Element identifier								
1	Coding		Information Element Instruction Field					
Ext	Standard		Flag	Reserved	Information Element Action Indicator			2
Length of Security Parameters IE contents								3
Length of Security Parameters contents (continued)								4
Security message exchange protocol				Reserved				5
1	0	0	0	0	0	0	1	6*
Initiator distinguished name identifier								
Length of initiator distinguished name								6.1
Initiator distinguished name type								6.2
Initiator distinguished name value								6.3 etc.
1	0	0	0	0	0	1	0	7*
Responder distinguished name identifier								

Length of responder distinguished name	7.1
Responder distinguished name type	7.2
Responder distinguished name value	7.3 etc.

1	0	0	0	0	0	1	1	8*
Initiator random number identifier								
Initiator random number value								8.1
Initiator random number value (cont'd)								8.2
Initiator random number value (cont'd)								8.3
Initiator random number value (cont'd)								8.4
1	0	0	0	0	1	0	0	9*
Responder random number identifier								
Responder random number value								9.1
Responder random number value (cont'd)								9.2
Responder random number value (cont'd)								9.3
Responder random number value (cont'd)								9.4
1	0	0	0	0	1	0	1	10*
Time-variant time stamp identifier								
Time stamp value								10.1
Time stamp value (cont'd)								10.2
Time stamp value (cont'd)								10.3
Time stamp value (cont'd)								10.4
Time stamp value (cont'd)								10.5
Time stamp value (cont'd)								10.6
Time stamp value (cont'd)								10.7
Time stamp value (cont'd)								10.8
1	0	0	0	0	1	1	0	11*
Digital signature identifier								
Length of digital signature contents								11.1
Digital signature value								11.2 etc.
1	0	0	0	0	1	1	1	12*
Security services options identifier								
Data confidentiality service								12.1
Data integrity service								12.2
Authentication service								12.3
Key exchange service								12.4

Session key update service	12.5
Access control service	12.6
1 0 0 0 1 0 0 0 Data confidentiality algorithm identifier	13*
Length of data confidentiality algorithm contents	13.1
Data confidentiality algorithm	13.2
Data confidentiality algorithm mode of operation	13.3
Data confidentiality algorithm details	13.4 etc.
1 0 0 0 1 0 0 1 Data integrity algorithm identifier	14*
Length of data integrity algorithm contents	14.1
Data integrity algorithm	14.2
Data integrity algorithm details	14.3 etc.
1 0 0 0 1 0 1 0 Hash algorithm identifier	15*
Length of hash algorithm contents	15.1
Hash algorithm	15.2
Hash algorithm details	15.3 etc.
1 0 0 0 1 0 1 1 Signature algorithm identifier	16*
Length of signature algorithm contents	16.1
Signature algorithm	16.2
Signature algorithm details	16.3 etc.
1 0 0 0 1 1 0 0 Key exchange algorithm identifier	17*
Length of key exchange algorithm contents	17.1
Key exchange algorithm	17.2
Key exchange algorithm details	17.3 etc.
1 0 0 0 1 1 0 1 Session key update algorithm identifier	18*
Length of session key update algorithm contents	18.1
Session key update algorithm	18.2

Session key update algorithm details								18.3 etc.
1	0	0	0	1	1	1	0	19*
Access control algorithm identifier								
Length of access control algorithm contents								19.1
Access control algorithm								19.2
Access control algorithm details								19.3 etc.
1	0	0	0	1	1	1	1	20*
Master key identifier								
Length of master key								20.1
Master key value								20.2 etc.
1	0	0	1	0	0	0	0	21*
First data confidentiality session key identifier								
Length of first data confidentiality session key								21.1
First data confidentiality session key value								21.2 etc.
1	0	0	1	0	0	0	1	22*
First data integrity session key identifier								
Length of first data integrity session key								22.1
First data integrity session key value								22.2 etc.

* optional octet group - if an octet group is present all the octets within the octet group shall be present

Security message exchange protocol (Octet 5)

8	7	6	5	**Meaning**
0	0	1	0	Two-way security exchange
0	0	1	1	Three-way security exchange

Security Entity Identifier: *The security entity identifier parameters indicate the distinguished names (IDs) of the initiator and responder of the security message exchange protocol.*

Initiator distinguished name (Octet group 6):

This octet group contains the distinguished name (ID) of the initiator of the security message exchange protocol.

Initiator distinguished name length (Octet 6.1):

A binary number indicating the length in octets of the initiator distinguished name type and value fields, contained in octets 6.2, 6.3, etc.

Initiator distinguished name type (Octet 6.2):

8	7	6	5	4	3	2	1	**Meaning**
0	0	0	0	0	0	0	1	ATM end system address

Initiator distinguished name value (Octet 6.3 etc.):

This octet group contains the value of the distinguished name (ID) of the initiator of the security message exchange protocol.

⇒ When the distinguished name type is "ATM address", this field contains the ATM address octets associated with the initiator. 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 **TBD** of [2].

Responder distinguished name (Octet group 7):

This octet group contains the distinguished name (ID) of the responder of the security message exchange protocol.

Responder distinguished name length (Octet 7.1):

A binary number indicating the length in octets of the responder distinguished name type and value fields, contained in octets 7.2, 7.3, etc.

Responder distinguished name type (Octet 7.2):

8	7	6	5	4	3	2	1	**Meaning**
0	0	0	0	0	0	0	1	ATM end system address

Responder distinguished name value (Octet 7.3 etc.):

This octet group contains the value of the distinguished name (ID) of the responder of the security message exchange protocol.

⇒ When the distinguished name type is "ATM address", this field contains the ATM address octets associated with the responder. 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 **TBD** of [2].

Security Authentication Parameters: The security authentication parameters contain information required for authentication of the parties (i.e., the "initiator" and "responder" of the security message exchange protocol).

Initiator/Responder random number (Octet groups 8 and 9):

These fields are coded in 32 bit binary.

Time-variant time stamp (Octet group 10):

This field allows each authentication exchange to be unique. This field consists of two 32 bit (four octet) integers, one for the time stamp (with one second resolution), and the other for a monotonically increasing sequence number. The timestamp shall be encoded in Octets 10.1 - 10.4, and the sequence number shall be encoded in Octets 10.5 - 10.8. Each of these integers are encoded as 32 bit unsigned binary integers, with bit 8 of the first octet being the most significant bit, and bit 1 of the fourth octet being the least significant bit. For further details on using this field, consult Section **TBD** of [1].

Digital signature (Octet group 11):

This octet group contains the signature value computed over the enitre content (i.e., octet 5 and higher) but this octet group of this information element.

Digital signature length (Octet 11.1):

A binary number indicating the length in octets of the digital signature value contained in octets 11.2, etc.

Digital signature value (Octet 11.2 etc.):

This field contains the binary encoding of the signature value. Further details on using this field are found in Section **TBD** of [1].

Security Options: *The security options negotiate the requested security services and algorithms to be used for the connection. This includes the type of security services to be provided for the connection and the algorithms/modes of operation to be used for each security service. In addition, the parameters associated with each algorithm are also included.*

Security services options (Octet group 12):

This octet group indicates whether the data confidentiality service to be provided or can be provided for the connection. This octet group is used for negotiation of data confidentiality service, which is described in detail in Section **TBD** of [1].

Data confidentiality service (Octet 12.1)

8	7	6	5	4	3	2	1	**Meaning**
0	0	0	0	0	0	0	0	Not supported
0	0	0	0	0	0	0	1	require at ATM cell level
0	0	0	0	0	0	1	0	can support at ATM cell level

Data integrity service (Octet 12.2)

8	7	6	5	4	3	2	1	**Meaning**
0	0	0	0	0	0	0	0	Not supported
0	0	0	0	0	0	0	1	require at AAL SDU level with replay/reordering protection
0	0	0	0	0	0	1	0	require at AAL SDU level without replay/reordering protection
0	0	0	0	0	0	1	1	can support at AAL SDU level with replay/reordering protection
0	0	0	0	0	1	0	0	can support at AAL SDU level without replay/reordering protection

Authentication service (Octet 12.3)

8	7	6	5	4	3	2	1	**Meaning**
0	0	0	0	0	0	0	0	Not supported
0	0	0	0	0	0	0	1	require Authentication
0	0	0	0	0	0	1	0	can support Authentication

Key exchange service (Octet 12.4)

8	7	6	5	4	3	2	1	**Meaning**
0	0	0	0	0	0	0	0	Not supported
0	0	0	0	0	0	0	1	require Key Exchange
0	0	0	0	0	0	1	0	can support Key Exchange

Session key update service (Octet 12.5)

8	7	6	5	4	3	2	1	Meaning
0	0	0	0	0	0	0	0	Not supported
0	0	0	0	0	0	0	1	require Session Key Update
0	0	0	0	0	0	1	0	can support Session Key Update

Access control service (Octet 12.6)

8	7	6	5	4	3	2	1	Meaning
0	0	0	0	0	0	0	0	Not supported
0	0	0	0	0	0	0	1	require Access Control
0	0	0	0	0	0	1	0	can support Access Control

Data confidentiality algorithm (Octet group 13):

This octet group indicates an algorithm for the data confidentiality service.

Length of Data Confidentiality Algorithm Contents (Octet 13.1):

A binary number indicating the length in octets of the data confidentiality algorithm/mode fields, contained in octets 13.2, 13.3, 13.4, etc.

Data confidentiality algorithm (Octet 13.2):

8	7	6	5	4	3	2	1	Meaning
0	0	0	0	0	0	0	1	DES with 56 bits effective key
0	0	0	0	0	0	1	0	Triple-DES with 112 bits effective key
0	0	0	0	0	0	1	1	DES with 40 bits effective key
0	0	0	0	0	1	0	0	FEAL, N=32, 64 bit key, no key block parity
1	x	x	x	x	x	x	x	User-defined data confidentiality algorithm (where "x" is "don't care")

Data confidentiality algorithm mode of operation (Octet 13.3):

8	7	6	5	4	3	2	1	Meaning
0	0	0	0	0	0	0	0	Does not apply
0	0	0	0	0	0	0	1	ECB
0	0	0	0	0	0	1	0	CBC
0	0	0	0	0	0	1	1	Counter Mode
1	x	x	x	x	x	x	x	User-defined data confidentiality mode of operation (where "x" is "don't care")

Data confidentiality algorithm/mode details (Octet 13.4 etc.):

These octets indicate coding details for each data confidentiality algorithm. These details are found in Section **TBD** of [1].

Data integrity algorithm (Octet group 14):

This octet group indicates an algorithm for the data integrity service.

Length of Data Integrity Algorithm Contents (Octet 14.1):

A binary number indicating the length in octets of the data integrity algorithm fields, contained in octets 14.2, 14.3, etc.

Data integrity algorithm (Octet 14.2):

8	7	6	5	4	3	2	1	Meaning

0 0 0 0 0 0 0 1	Keyed MD5
0 0 0 0 0 0 1 0	MAC generated using DES in CBC mode
0 0 0 0 0 0 1 1	MAC generated using FEAL in CBC mode
1 x x x x x x x	User-defined data integrity algorithm (where "x" is "don't care")

Data integrity algorithm details (Octet 14.3 etc.):

These octets indicate coding details for each data integrity algorithm. These details are found in Section **TBD** of [1].

Hash algorithm (Octet group 15):

This octet group indicates a hashing algorithm for the authentication service.

Length of Hash Algorithm Contents (Octet 15.1):

A binary number indicating the length in octets of the hash algorithm fields, contained in octets 15.2, 15.3, etc.

Hash algorithm (Octet 15.2):

8 7 6 5 4 3 2 1	**Meaning**
0 0 0 0 0 0 0 1	MD5
0 0 0 0 0 0 1 0	SHA
1 x x x x x x x	User-defined hash algorithm (where "x" is "don't care")

Hash algorithm details (Octet 15.3 etc.):

These octets indicate coding details for each hash algorithm. These details are found in Section **TBD** of [1].

Signature algorithm (Octet group 16):

This octet group indicates a signature algorithm for the authentication service.

Length of Signature Algorithm Contents (Octet 16.1):

A binary number indicating the length in octets of the signature algorithm fields, contained in octets 16.2, 16.3, etc.

Signature algorithm (Octet 16.2):

8 7 6 5 4 3 2 1	**Meaning**
0 0 0 0 0 0 0 1	RSA
0 0 0 0 0 0 1 0	DSA
0 0 0 0 0 0 1 1	Elliptic Curve/DSA
0 0 0 0 0 1 0 0	ESIGN
0 0 0 0 0 1 0 1	DES/CBC
0 0 0 0 0 1 1 0	DES40/CBC
0 0 0 0 0 1 1 1	FEAL/CBC
1 x x x x x x x	User-defined signature algorithm (where "x" is "don't care")

Signature algorithm details (Octet 16.3 etc.):

These octets indicate coding details for each signature algorithm. These details are found in Section **TBD** of [1].

Key exchange algorithm (Octet group 17):

This octet group indicates an algorithm for key exchange. This algorithm is used to encrypt the contents part of the "Security confidential parameters" information element.

Length of Key Exchange Algorithm Contents (Octet 17.1):

A binary number indicating the length in octets of the key exchange algorithm fields, contained in octets 17.2, 17.3, etc.

Key exchange algorithm (Octet 17.2):

8	7	6	5	4	3	2	1	Meaning
0	0	0	0	0	0	0	1	RSA
0	0	0	0	0	0	1	0	Diffie-Hellman
0	0	0	0	0	0	1	1	Elliptic Curve/Diffie-Hellman
0	0	0	0	0	1	0	0	DES/CBC
0	0	0	0	0	1	0	1	FEAL/CBC
1	x	x	x	x	x	x	x	User-defined key exchange algorithm (where "x" is "don't care")

Key exchange algorithm details (Octet 17.3 etc.):

These octets indicate coding details for each key exchange algorithm. These details are found in Section **TBD** of [1].

Session key update algorithm (Octet group 18):

This octet group indicates a session key update algorithm for updating the data confidentiality and data integrity session keys.

Length of Session Key Update Algorithm Contents (Octet 18.1):

A binary number indicating the length in octets of the key exchange algorithm fields, contained in octets 18.2, 18.3, etc.

Session key update algorithm (Octet 18.2):

8	7	6	5	4	3	2	1	Meaning
0	0	0	0	0	0	0	1	SKE with SHA
0	0	0	0	0	0	1	0	SKE with MD5

Session key update algorithm details (Octet 18.3 etc.):

These octets indicate coding details for each session key update algorithm. These details are found in Section **TBD** of [1].

Access control algorithm (Octet group 19):

This octet group indicates an algorithm for the access control service.

Length of access control algorithm contents (Octet 19.1):

A binary number indicating the length in octets of the access control algorithm fields, contained in octets 19.2, 19.3, etc.

Access control algorithm (Octet 19.2):

8	7	6	5	4	3	2	1	Meaning
0	0	0	0	0	0	0	1	CIPSO format
1	x	x	x	x	x	x	x	User-defined data integrity algorithm

(where "x" is "don't care")

Access control algorithm details (Octet 19.3 etc.):

These octets indicate coding details for each access control algorithm. These details are found in Section **TBD** of [1].

Security Confidential Parameters: *The security confidential parameters provide for exchange of confidential information (i.e., keys) used for providing the data confidentiality and data integrity services. The entire confidential parameters is encrypted.*

Master key (Octet group 20):

This octet group contains the key used to encrypt subsequent session keys.

Master key length (Octet 20.1):

A binary number indicating the length in octets of the master key value contained in octets 20.2, etc.

Master key value (Octet 20.2 etc.):

This field contains the binary encoding of the master key value, with bit 8 of the first octet being the most significant bit, and bit 1 of the last octet being the least significant bit. The master key length must be an integer multiple of 8 bits.

First data confidentiality session key (Octet group 21):

This octet group contains the first session key to be used to provide the data confidentiality service.

First data confidentiality session key length (Octet 21.1):

A binary number indicating the length in octets of the first confidentiality session key value contained in octets 21.2, etc.

First data confidentiality session key value (Octet 21.2 etc.):

This field contains the binary encoding of the first data confidentiality session key value, with bit 8 of the first octet being the most significant bit, and bit 1 of the last octet being the least significant bit. The data confidentiality session key length must be an integer multiple of 8 bits.

First data integrity session key (Octet group 22):

This octet group contains the first session key to be used to provide the data integrity service.

First data integrity session key length (Octet 22.1):

A binary number indicating the length in octets of the first integrity session key value contained in octets 22.2, etc.

First data integrity session key value (Octet 22.2 etc.):

This field contains the binary encoding of the first data integrity session key value, with bit 8 of the first octet being the most significant bit, and bit 1 of the last octet being the least significant bit. The data integrity session key length must be an integer multiple of 8 bits.

5.3 Security Alternate Options

The purpose of the Security Alternate Options information element is to specify an alternate set of security options for negotiation of security services algorithms during connection setup.

Bits 8	7	6	5	4	3	2	1	Octets
x	x	x	x	x	x	x	x	1
Security Alternate Options Information Element identifier								
1 Ext	Coding Standard		Information Element Instruction Field: Flag	Reserved	Information Element Action Indicator			2
Length of Security Alternate Options IE contents								3
Length of Security Alternate Options IE contents (continued)								4
Further octets as contents of Security Parameters IE in Section 5.2, octet groups 13, 14, 15, 16, 17, 18, and 19								5* etc. (Note)

* optional octet group - if an octet group is present all the octets within the octet group shall be present

Note - An alternate option octet group can be included only if the first option octet group (i.e., the non-alternate option) is present in the Security Parameters IE.

6. Call/Connection Control Procedures for Point-to-Point

The procedures for point-to-point call/connection control as described in UNI 4.0 and Q.2931 shall apply. Additional procedures to handle point-to-point calls/connections with security capability are described in this section. These procedures shall apply only to devices which are capable of providing security services. Devices which are not capable of providing security services shall pass without modification the security information elementsdefined in Section 5 of this specification. Devices may optionally allow multiple instances of the security information elements to be present in a signaling message.

The timer values defined in UNI 4.0 and Q.2931 remain unchanged for the procedures described in this specification.

6.1 Call/Connection Establishment at the Originator

6.1.1 Call/Connection Request

The procedures of UNI 4.0 and Q.2931 shall apply with the following changes:

The calling party sends a SETUP message which contains the required security information elements. The security information elements are provided by the "security agent" in accordance with the procedures described in [1].

Upon receipt of the SETUP message, the network will process the call as defined in UNI 4.0 and Q.2931 specifications with the following clarification:

1. The network shall not modify/reorder the contents (i.e. Octets 5 and higher) of the security information elements defined in Section 5 of this specification.
2. The network may optionally allow multiple instances of the security information elements defined in this specification.

If the network device provides security capability, then the received security information shall be forwarded to the network device's security agent for security processing. If this processing completes successfully, the security agent shall provide the security information elements, if required, for subsequent processing of the call request. If this processing does not complete successfully, then the network shall clear the call with Cause # **TBD** ("Security Protocol Processing Failure").

6.1.2 Call/Connection Acceptance

Upon receipt of a CONNECT message by the calling party, if security information elements are received in the message shall be forwarded to the security agent for processing. The security agent shall process the information elements and determine if the connection request is allowed to proceed. The information elements will be processed in accordance with the procedures defined in [1], and if any processing errors occur, then the call shall be cleared with Cause # **TBD** ("Security Protocol Processing Failure").

If the calling party requires security capability for a connection, and the CONNECT message does not contain a required security information element, then the calling party shall clear the call with Cause # **TBD** ("Missing Required Security Information Element").

If the calling party receives a CONNECT message which contains the Broadband Report Type information element with the "Type of Report" field containing the codepoint for "Connection Confirmation" (see section 5.1 of this specification), then it shall send a CONNECTION AVAILABLE message in accordance with the procedures established in Q.2963. The CONNECTION AVAILABLE message shall contain the security information element, as provided by the security agent.

Upon receipt of the CONNECTION AVAILABLE message, the network will process the call as defined in UNI 4.0, Q.2931, and Q.2963 specifications with the following clarification:

1. The network shall not modify/reorder the contents (i.e. Octets 5 and higher) of the security information element defined in Section 5 of this specification.
2. The network may optionally allow multiple instances of the security information elements defined in this specification.

If the network device provides security capability, then the received security information shall be forwarded to the network device's security agent for security processing. If this processing completes successfully, the security agent shall provide the security information elements, if required, for subsequent processing of the call request. If this processing does not complete successfully, then the network shall clear the call with Cause # **TBD** ("Security Protocol Processing Failure").

6.2 Call/Connection Establishment at the Destination

6.2.1 Call/Connection Acceptance

The procedures of UNI 4.0 and Q.2931 shall apply with the following changes:

Upon receipt of a SETUP message by the called party, if security information elements ares received in the message shall be forwarded to the security agent for processing. The security agent shall process the information elements and determine if the connection request is allowed to proceed. The information elements will be processed in accordance with the procedures defined in [1], and if any processing errors occur, then the call shall be cleared with Cause # **TBD** ("Security Protocol Processing Failure").

If the called party requires security capability for a connection, and the SETUP message does not contain a required security information element, then the called party shall clear the call with Cause # **TBD** ("Missing Required Security Information Element").

If the connection is allowed to proceed, the called party shall send a CONNECT message in accordance with the procedures established in UNI 4.0 and Q.2931. The CONNECT message shall contain the security information elements if required, as provided by the security agent. Additionally, if three-way security message exchange is required, the CONNECT message shall contain the Broadband Report Type information element of Q.2963 with the "Type of Report" field containing the codepoint for "Connection Confirmation" (see section 5.1 of this specification).

Upon receipt of the CONNECT message, the network will process the call as defined in UNI 4.0 and Q.2931 specifications with the following clarification:

1. The network shall not modify/reorder the contents (i.e. Octets 5 and higher) of the security information elements defined in Section 5 of this specification.
2. The network may optionally allow multiple instances of the security information elements defined in this specification.

If the network device provides security capability, then the received security information shall be forwarded to the network device's security agent for security processing. If this processing completes successfully, the security agent shall provide the security information elements, if required, for subsequent processing of the call request. If this processing does not complete successfully, then the network shall clear the call with Cause # **TBD** ("Security Protocol Processing Failure").

Upon receipt of a CONNECTION AVAILABLE message by the called party, if a security information element is received in the message shall be forwarded to the security agent for processing. The security agent shall process the information elements and determine if the connection request is allowed to proceed. The information element will be processed in accordance with the procedures defined in [1], and if any processing errors occur, then the call shall be cleared with Cause # **TBD** ("Security Protocol Processing Failure").

If the called party requires security capability for a connection, and the CONNECTION AVAILABLE message does not contain a required security information element, then the called party shall clear the call with Cause # **TBD** ("Missing Required Security Information Element").

7. Call/Connection Control Procedures for Point-to-Multipoint

The procedures for point-to-multipoint call/connection control as described in UNI 4.0, Q.2931, and Q.2971 shall apply. Additional procedures to handle point-to-multipoint calls/connections with security capability are described in this section. These procedures shall apply only to devices which are capable of providing security services. Devices which are not capable of providing security services shall pass without modification the security information elements defined in Section 5 of this specification. Devices may optionally allow multiple instances of the security information elements to be present in a signaling message.

These procedures apply only for cases where "leaves" are added to point-to-multipoint calls by the "root" (including "leaf initiated" join procedures). Specifically, "leaf initiated" join procedures where the root is not involved in handling the join request are not supported by this specification.

The timer values defined in UNI 4.0, Q.2931, and Q.2971 remain unchanged for the procedures described in this specification.

7.1 Call/Connection Establishment at the Originator

7.1.1 Call/Connection Request

The first "leaf" of the point-to-multipoint call is added using the procedures of UNI 4.0 and Q.2931, and the security procedures described in Section 6 of this specification.

The procedures of UNI 4.0 and Q.2971 for adding subsequent "leaves" shall apply with the following changes:

The root sends an ADD PARTY message which contains the required security information element. The information element is provided by the "security agent" in accordance with the procedures described in [1].

Upon receipt of the ADD PARTY message, the network will process the call as defined in UNI 4.0 and Q.2971 specifications with the following clarification:

1. The network shall not modify/reorder the contents (i.e. Octets 5 and higher) of the security information element defined in Section 5 of this specification.
2. The network may optionally allow multiple instances of the security information element defined in this specification.

If the network device provides security capability, then the received security information shall be forwarded to the network device's security agent for security processing. If this processing completes successfully, the security agent shall provide the security information element, if required, for subsequent processing of the call request. If this processing does not complete successfully, then the network shall clear the call with Cause # **TBD** ("Security Protocol Processing Failure").

7.1.2 Call/Connection Acceptance

Upon receipt of an ADD PARTY ACKNOWLEDGE message by the root, if a security information element is received in the message shall be forwarded to the security agent for processing. The security agent shall process these information element and determine if the connection request is allowed to proceed. These information element will be processed in accordance with the procedures defined in [1], and if any processing errors occur, then the call shall be cleared with Cause # **TBD** ("Security Protocol Processing Failure").

If the root requires security capability for a connection, and the ADD PARTY ACKNOWLEDGE message does not contain a required security information element, then the root shall clear the call with Cause # **TBD** ("Missing Required Security Information Elements").

7.2 Call/Connection Establishment at the Destination

7.2.1 Call/Connection Acceptance

The procedures of UNI 4.0 and Q.2971 shall apply with the following changes:

Upon receipt of a SETUP message by the leaf, if a security information element is received in the message shall be forwarded to the security agent for processing. The security agent shall process the information element and determine if the connection request is allowed to proceed. The information element will be processed in accordance with the procedures defined in [1], and if any processing errors occur, then the call shall be cleared with Cause # **TBD** ("Security Protocol Processing Failure").

If the leaf requires security capability for a connection, and the SETUP message does not contain a required security information element, then the leaf shall clear the call with Cause # **TBD** ("Missing Required Security Information Elements").

If the connection is allowed to proceed, the leaf shall send a CONNECT message in accordance with the procedures established in UNI 4.0 and Q.2971. The CONNECT message shall contain a security information element if required, as provided by the security agent.

Upon receipt of the CONNECT message, the network will process the call as defined in UNI 4.0 and Q.2971 specifications with the following clarification:

1. The network shall not modify/reorder the contents (i.e. Octets 5 and higher) of the security information element defined in Section 5 of this specification.
2. The network may optionally allow multiple instances of the security information element defined in this specification.

If the network device provides security capability, then the received security information shall be forwarded to the network device's security agent for security processing. If this processing completes successfully, the security agent shall provide the security information element, if required, for subsequent processing of the call request. If this processing does not complete successfully, then the network shall clear the call with Cause # **TBD** ("Security Protocol Processing Failure").