ATM Forum Technical Committee
ATM Forum/97-0040

****

TITLE: Security mechanisms within control plane

****

SOURCE:

Maryline LAURENT and Pierre ROLIN
Telecom Bretagne (ENST-B)
rue de la châtaigneraie - BP 78
35512 CESSON Cedex - France
Phone: 33 2 99 12 70 20
Fax: 33 2 99 12 70 30
E-mail: {Maryline.Laurent,Pierre.Rolin}@enst-bretagne.fr

Laurent STOFFEL
France Telecom
38-40 rue du General Leclerc
92131 Issy les Moulineaux - France
Phone: 33 1 45 29 62 02
E-mail : laurent.stoffel@Issy.cnet.fr

****

DATE: February 1997, San Diego, CA

****

DISTRIBUTION: SEC, SIG, PNNI and B-ICI Working Groups

****

ABSTRACT:

This contribution proposes 2 new Security Information Elements (SIE) to replace 7 security IEs defined in [AFSEC] and to perform, additionally to the security services offered in [AFSEC], signaling's confidentiality. The SIE's format is based on the Authentication IE (AIE) defined in [AFSEC], however it solves AIE's limitations and security problems mentioned in the contribution.

****

****

1 Introduction

This contribution proposes 2 new Security Information Elements (SIE) to replace 7 security IEs defined in [AFSEC] and to perform, additionally to the security services offered in [AFSEC], signaling's confidentiality as mentionned in table 1.

	[AFSEC]	The proposed solution
Security services offered[a]	A, I, AC, KE, RD SSN:I+C+A+KE	A, I, AC, KE, RD, C SSN:I+C+A+KE+TP
Modifications required within [AFSIG]	7 new IEs	2 new IEs to offer either end-to-end or hop-by-hop security services
Information to be encrypted within signaling	keys	keys+security services parameters being negotiated+access control's security levels+IEs+other information such as end-user's identity and end-stations' addresses

Table 1 : Comparisons between [AFSEC] and the recommended solution

a. Abbreviations used :

A Authentification	AC Access Control
C Confidentiality	I Integrity
KE Key Exchange	RD Replay Detection
TP Traffic Padding	SSN:X X Security Service Negotiation

Two SIEs are defined to realize either end-to-end or hop-by-hop security services, thus enabling end-to-end, switch-to-switch or endpoint-to-switch authentication, signaling secrecy and security services negotiation. SIEs may be inserted within all signaling messages (SET UP, CONNECT, RELEASE, etc.).

Motivations for defining such SIEs are as follows:

(1) We suggest to replace 7 security IEs defined in [AFSEC] with 2 security IEs, so that modifications required within [AFSIG] are limited to 2 new IEs introduction only. Moreover, this brings performance increase since the fewer IEs in the signaling message, the less time ATM switches spend examining signaling message's IE headers to know whether the IE is used for signaling message's processing.

(2) We suggest to define two new SIEs with two IEs' identifiers to distinguish end-to-end and hop-by-hop SIEs instead of using the E/E bit technics (chosen in [AFSEC] to distinguish end-to-end and hop-by-hop Authentication IE). As mentionned in section 2 point (2), this increases performance.

(3) The SIEs proposed allow to encrypt part of signaling. That is, additionally to keys encryption performed within signaling in [AFSEC], we propose to encrypt within signaling IEs:

- all the security parameters used to negotiate security services which are in the clear in [AFSEC]. Such parameters carry sensitive information - such as the encryption algorithm level or the security services list (chosen to secure user data) - which gives information about the user data sensitivity level (If a high encryption algorithm is required or if all security services are needed, it is likely that sensitive data will be exchanged). With such cleartext parameters within signaling messages, an intruder eavesdropping signaling traffic may deduce information nature that will be exchanged and can easily select the connection to disrupt or to eavesdrop.

- the security level included within the access control IE defined in [AFSEC] which directly informs of the user data sensitivity level.

- ordinary IEs. Any IE may be moved in the SIE to be encrypted within hop-by-hop SIE whereas only IEs that are not analyzed by the public network (e.g. Broadband low layer information IE) may be encrypted within end-to-end SIE.

Also other information may be encapsulated within the encrypted part of the signaling SIEs and thus confidentiality protected during their transfer over the network. For instance, it is possible to protect end-user's identity against disclosure in case a specific SIE's field is used to carry user's identifiers. Also, in the LANs environment, where two companies need to communicate, signaling encryption may allow companies to keep their addresses mappings secret although they communicate over the network (see section 3.1).

(4) Additionally to the security services negotiated in [AFSEC] to protect user data exchanges, the SIE proposes to negotiate traffic padding services.

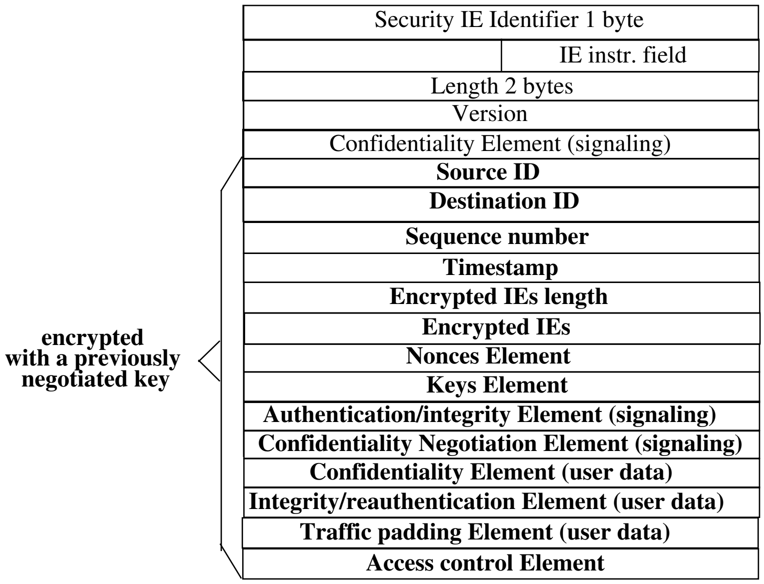

Figure 1 : Security Information Element SIE

(5) The SIEs format is based on the Authentication IE (AIE) defined in [AFSEC], however it solves AIE's limitations and security problems described in section 2.

The remainder of the contribution is organized as follows. Section 2 gives AIE's limitations. Section 3 describes new SIE's formats and section 4 concludes.

2 The AIE's limitations and security problems

The Authentication IE (AIE) defined in [AFSEC] is inaccurate and flawed since:

(1) the IEs ordering that should be enforced when generating the signature is not specified in case signaling messages include repeated IEs.

(2) it would be more efficient to distinguish end-to-end AIE from hop-by-hop AIE by assigning each a specific IE identifier instead of using the *E/E* bit, since switches would no longer have to examin the AIE fields up to the *E/E* bit to know if authentication is to be performed.

(3) the AIE enables stations authentication only since no fields are available within AIE to carry user or user group identifier.

(4) there is one scenario that results in a malicious station, say C, masquerading as another station, say A. Assume that station A authenticates to station B within SET UP message with an AIE whose signature is not computed over B's address (B's called entity's address IE or the security entity identifier IE described in [AF96-1244]). C (a station eavesdropping the network or even B) may retrieve the AIE and reuse it to authenticate to another station, say D as A. This assumes that the *Sequence number* is appropriate and C is quick enough so that the *Timestamp* remains valid.

Each of these points are solved in section 3 to define new security IEs.

3 The SIE's format

The SIE is described in figure 1 and is organized into security elements, each of which supports signaling security services (Authentication/integrity Element (signaling), Confidentiality Element (signaling), Access control Element, Nonces Element) or security services negotiation to secure signaling exchange (Authentication/integrity Element (signaling), Confidentiality Negotiation Element (signaling), Nonces Element) or user data exchange (Confidentiality Element (user data), Integrity/reauthentication Element (user data), Traffic padding Element (user data), Nonces Element, Keys Element).

Since security services may be implemented end-to-end or hop-by-hop and thus SIE may have end-to-end or hop-by-hop significance, two network entities are distinguished:

- The **SIE originator** which generates the SIE. This is a switch in case of switch-to-switch or switch-to-endpoint SIE or a station in case of end-to-end or endpoint-to-switch SIE.

- The **SIE retriever** which retrieves the SIE within signaling messages for analysis, decryption, etc. This is a switch in case of switch-to-switch or endpoint-to-switch SIE or a station in case of end-to-end or switch-to-endpoint SIE.

Before part of signaling messages encryption or authentication can take place between SIE originator and retriever, with symmetric key algorithms, SIE originator and retriever need to have a shared secret key. With asymmetric key algorithms, they only need to know each other's public keys.

SIE's fields are described hereafter with (M) and (O) standing for Mandatory and Optional information.

3.1 SIE's first eleven fields

(M) Security Information Element ID : This field is specified for all UNI 3.1 signaling messages (see [AFSIG], section 5.4.5.1). Different IEs identifiers should be used to distinguish end-to-end and hop-by-hop SIEs, thus solving the AIE's point (2) flaw described in section 2.

(M) IE Compatibility Instruction Indicator: This field is specified for all UNI 3.1 signaling messages (see [AFSIG], section 5.4.5.1).

(M) Length : This field is specified for all UNI 3.1 signaling messages (see [AFSIG], section 5.4.5.1), and allows the Authentication IE to be variable length.

(M) Version : This octet denotes the specification to which this SIE is compliant. For the SIE specified here, this field SHALL be set to 1 since the AIE corresponds to version 0.

(O) Confidentiality Element (signaling) : see section 3.2.

(M) Source ID/Destination ID : These fields identify the signaling messages source/destination. Source/Destination ID may be source/destination user names so that user authentication is allowed in SIE contrary to AIE (see AIE's point (3) flaw section 2).

(M) Sequence Number/Timestamp : These fields allow each SIE to be unique.

(M) Encrypted IEs length : In case the SIE is encrypted, this field provides the number of IEs that are encrypted within the "Encrypted IEs" field. If the "Encrypted IEs " field is omitted, then the Encrypted IEs length MUST be 0.

(O) Encrypted IEs : This field includes signaling message's ordinary IEs that need confidentiality protection. These ordinary IEs are moved in the SIE's "Encrypted IEs" field to be encrypted with the SIE. In case switches are located between the SIE originator and retriever, this requires that these IEs are not used (read or modified) by the public network. That is, the field "Encrypted IEs" must not include IEs such as calling/called entity address IEs, however it may include IEs such as "Broadband low layer information" IE and the "security entity identifier" IE defined in [AF96-1244].

In the LANs environment, encrypting the "security entity identifier" IE [AF96-1244] between end-LANs' switches is of interest when two companies (i.e. LANs) need to communicate and want to keep secret their own addresses mappings. This is realized by defining one global address common to all company's stations (i.e. a proxy's address). Thus, as described in figure 2, when setting up a connection with that company, the only clear address within the SET UP message (in the "called entity number" IE) is the global one. The real stations' addresses ("security entity identifier" IE) are encrypted within the "Encrypted IEs" field of the SIE. This assumes that the receiving company's switch decrypts the SIE with the algorithm specified within the "confidentiality element (signaling)" (see section 3.2) before forwarding the set up request to the appropriate station. The switch acts as a secure proxy.

In case the "security entity identifier" IE is not accepted by the ATM Forum, the previous problem may be solved by defining one additional field within the SIE or using the "Source ID/Destination ID" fields to carry real company's stations addresses.

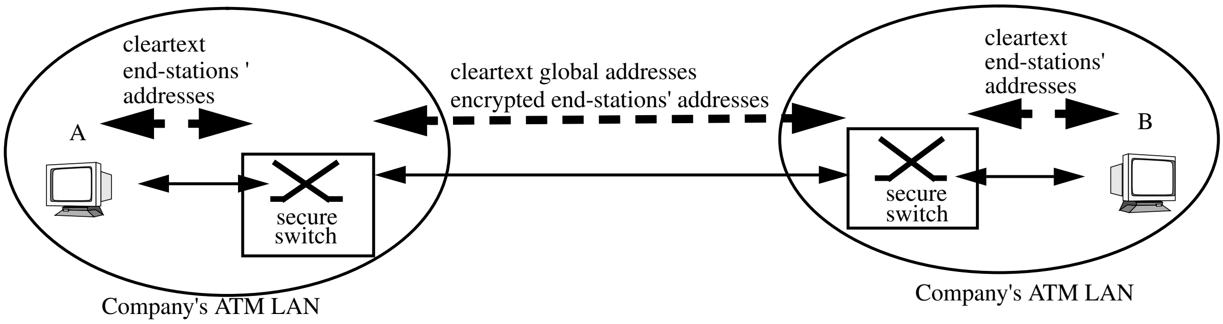

Figure 2 : By encrypting the SIE between their secure ingress switches and defining one global address per company, end-stations' addresses may be hiden over the public network. Only global addresses are in the clear.

3.2 SIE's Confidentiality Element (signaling)

(O) The Confidentiality Element (signaling) in figure 1 includes information regarding signaling's encryption.

In case the SIE is encrypted, the confidentiality element must be present and placed just before the SIE's encrypted part (i.e. fields written in bold in figure 1). This element identifies either the security context (i.e. the encryption algorithm, keys, etc. used to encrypt) which should have been previously negotiated securely or the encryption algorithm used to encrypt the SIE. Thus it should include either a security context identifier or an encryption algorithm code.

If the SIE is not encrypted, the confidentiality element may be present and specify the security context identifier that will be later used to refer to the security context being negotiated.

This field is described in figure 3 and is optional. But, if present, the subfields of figure 3 are Mandatory (M):

(M) Confidentiality Element ID : This field identifies the confidentiality element.

(M) Confidentiality Element's length : This field gives the confidentiality element's lengtht, excluding the element identifier and length fields.

(M) Content type : This field informs of the type of the "identifier" field, that is, whether it contains a security context or encryption algorithm identifier.

(M) Identifier : This field includes either the security context identifier or the encryption algorithm code.

Confidentiality Element ID 1 oct
Length 2 oct
Content type
Identifier

Figure 3 : Confidentiality element (signaling)

3.3 SIE's nonces element

(O) The nonces Element in figure 1 is used to negotiate security parameters between SIE originator and retriever. This element includes the calling and called party random numbers contained in the security authentication parameters IE described in [AFSEC] section 8.4.2.3.

This field is described in figure 4 and is optional. But, if present, the subfields of figure 4 are either Optional (O) or Mandatory (M).

(M) Nonces Element ID : This field identifies the nonces element.

(M) Length : This field allows to specify the length of the element, excluding the element identifier and the length field.

(M) Calling party random number : the random number generated by the SIE originator requiring the connection set up (see [AFSEC] section 4.1).

(O) Called party random number : the random number generated by the SIE retriever receiving the SET UP message. If the three-way security messages exchange protocol is chosen, the called party random number field is mandatory (see [AFSEC] section 4.1.1), otherwise it is omitted (see [AFSEC] section 4.1.2). The "Lenght" field of figure 4 indicates whether the called party random number field is present.

Nonces Element ID 1 oct
Length 2 oct
Calling party random number
Called party random number

Figure 4 : Nonces element

3.4 SIE's keys element

(O) The keys Element in figure 1 includes similar information than those contained in the security confidential parameters IE described in [AFSEC] section 8.4.2.4.

This field is described in figure 5 and is optional. But, if present, the subfields described in figure 5 are either Optional (O) or Mandatory (M). Such fields are described in details in [AFSEC] section 8.4.2.4.

(O) Master key ID : If present, both master key lenght and value are mandatory.

(O) First data confidentiality session key ID : same remark than the "Master key ID" field's.

(O) First data integrity session key ID : same remark than the "Master key ID" field's.

Keys Element ID 1 byte
Length 2 bytes
Master key ID 2 bytes
Length of master key
Master key value
First data confidentiality session key ID
Lenth of first data session key
First data confidentiality session key value
First data integrity session key ID
Length of first data integrity session key
First data integrity session key value

Figure 5 : Keys Element

3.5 SIE's Authentication/integrity element (signaling)

(O) The authentication/integrity Element (signaling) in figure 1 includes information regarding signaling's integrity and origin authentication.

This field is described in figure 6 and is optional. But, if present, the subfields of figure 6 are either Optional (O) or Mandatory (M):

(M) Authentication/integrity Element ID : This field identifies the authentication/integrity element.

(M) Authentication/integrity Element's length : This field gives the authentication/integrity element's lengtht, excluding the element identifier and length fields.

(M) Length of the field "List of algorithms to be used for signature": This field provides the length of the "List of algorithms to be used for signature". Since the list of algorithms should include the algorithm used to generate the signature, this field is always greater than 0 and the field "List of algorithms ..." is never omitted.

(M) List of algorithms to be used for signature : This field indicates a list of algorithms (with their respective parameters) ordered according to preferences. The first instance in the list is the algorithm code used to generate SIE's signature. As such if the SIE retriever does not support that algorithm, it can choose another algorithm among the list and sends it back within a SIE. The SIE originator will then use that algorithm to authenticate in further signaling messages.

Authentication/integrity Element ID 1 byte
Length 2 bytes
Length of "list of algorithms to ..." 1 byte
List of algorithms to be used for signature
Mutual authentication indication
Length of "List of algorithms to ..." 1 byte
List of algorithms to be used by the called entity if mutual authentication is required
IEs list length
IEs list
Digital Signature

Figure 6 : Authentication/Integrity Element

(M) Mutual authentication indication : This field indicates if the SIE originator demands the SIE retriever to authenticate. If no authentication is required, the field "List of algorithms to be used by the SIE retriever if mutual authentication is required" is omitted.

(M) Length of the field "List of algorithms to be used by the SIE retriever if mutual authentication is required" : This field provides the length of the "List of algorithms to be used ..". If the field "List of algorithms to be used .." is omitted, then the length MUST be 0.

(O) List of algorithms to be used by the SIE retriever if mutual authentication is required : This field includes a list of algorithms (with their respective parameters) ordered according to preferences that the SIE retriever should use to authenticate. Then the SIE retriever needs to authenticate with the first algorithm in the list that is suitable for him.

(M) IEs list length : This field provides the length of the IEs list. If the "IEs List" field is omitted, then the IEs list length MUST be 0.

(O) IEs list : This field contains a list of information elements identifiers that specifies the IEs over which the digital signature was computed. The IEs List also denotes the ordering of IEs during signature generation and validation. The AIE's repeated IEs' problem that raises in section 2 (AIE's point (1) flaw) may be solved by introducing as many repeated IEs identifiers as repeated IEs to be signed into the IEs list. That is, if n repeated IEs' identifiers are introduced into the IEs list, the signature is generated over the n first repeated IEs that appear within the signaling message. This is possible since repeated IEs' order is kept along the connection.

In order to solve the AIE's point (4) flaw, it is necessary that the signature be generated over the "security entity identifier" IE [AF96-1244] in case this IE is accepted by the ATM Forum and this IE is not included in the "Encrypted IEs" field. Otherwise the signature should be computed over the SIE containing end-stations' addresses.

If the "IEs list" field is omitted, then the digital signature is calculated over the contents of the SIE ONLY, and the content of the "IEs List Length" field MUST be 0.

(M) Digital Signature : This field contains the digital signature for the message. The signature scope includes the IEs denoted in the "IE List" field, and the contents of the SIE itself. This scope allows the message originator to "sign" the integrity (or "correctness") of the non-variant information contained within the signaling message.

3.6 SIE's confidentiality negotiation element (signaling)

(O) The confidentiality Negotiation Element (signaling) in figure 1 is used to negotiate or renegotiate security parameters to ensure the signaling confidentiality service.

This field is described in figure 7 and is optional. But, if present, the subfields of figure 7 are Mandatory (M).

(M) Confidentiality Negotiation Element ID : This field identifies the confidentiality negotiation element specific for signaling.

(M) Confidentiality Negotiation Element's length : This field gives the element's length, excluding the element identifier and length fields.

(M) Length of the field "list of encryption algorithms to be used" : This field provides the length of the "List of

Confidentiality Negotiation Element ID 1 oct
Length 2 oct
Length of the list of encryption algorithms
List of encryption algorithms to be used

Figure 7 : Confidentiality element (signaling)

encryption algorithms to be used". Since the list of encryption algorithms should include one algorithm to encrypt signaling at least, this field is always greater than 0 and the field "List of algorithms ..." is never omitted.

(M) List of encryption algorithms to be used : This field indicates a list of algorithms (with their respective parameters) ordered according to preferences. That is, during connection set up, the SIE originator indicates within SET UP a set of algorithms that could be used for that connection to provide signaling confidentiality and the SIE retriever sends back within CONNECT the chosen encryption algorithm, provided that one is suitable.

3.7 SIE's confidentiality element (user data)

(O) The confidentiality Element (user data) in figure 1 is used to negotiate security parameters between SIE originator and retriever to encrypt user data.

This field includes the same structure as the one in figure 7. This field is optional but if present, its subfields are Mandatory (M).

(M) Confidentiality Element ID : This field identifies the confidentiality element specific for user data exchanges.

(M) Confidentiality Element's length : This field gives the element's length, excluding the element identifier and length fields.

(M) Length of the field "list of encryption algorithms to be used" : This field provides the length of the "List of encryption algorithms to be used". Since the list of encryption algorithms should include one algorithm to encrypt user data at least, this field is always greater than 0 and the field "List of encryption algorithms ..." is never omitted.

(M) List of encryption algorithms to be used : This field indicates a list of algorithms (with their respective parameters) ordered according to preferences. That is, during connection set up, the SIE originator indicates within SET UP a set of algorithms that could be used for that connection to provide user data confidentiality and the SIE retriever sends back within CONNECT the chosen encryption algorithm, provided that one is suitable.

3.8 SIE's integrity/reauthentication element (user data)

(O) The integrity/reauthentication Element (user data) in figure 1 is used to negotiate security parameters to ensure user data's integrity and origin authentication.

This field includes similar structure as this depicted in figure 7. This field is optional but, if present, the following subfields are Mandatory (M).

(M) Integrity/reauthentication Element ID : This field identifies the integrity/reauthentication element specific for user data exchanges.

(M) Integrity/reauthentication Element's length : This field gives the integrity/reauthentication element's length, excluding the element identifier and length fields.

(M) Length of the field "list of mechanisms to be used" : This field provides the length of the "List of mechanims to be used". Since the list of mechanisms should include one mechanism to ensure user data integrity/reauthentication at least, this field is always greater than 0 and the field "List of mechanisms ..." is never omitted.

(M) List of mechanisms to be used : This field indicates a list of mechanisms (with their respective parameters) ordered according to preferences. That is, during connection set up, the SIE originator indicates within SET UP a set of mechanisms that could be used for that connection to provide user data integrity/reauthentication and the SIE retriever sends back within CONNECT the chosen mechanism, provided that one is suitable.

3.9 SIE's traffic padding element (user data)

(O) The traffic padding Element (user data) is used to negotiate security parameters to secure user data exchanges by injecting spurious data within user data flow.

This field includes similar structure as this depicted in figure 7. This field is optional but, if present, the following subfields are Mandatory (M).

(M) Traffic padding Element ID : This field identifies the traffic padding element specific for user data exchanges.

(M) Traffic padding Element's length : This field gives the traffic padding element's length, excluding the element identifier and length fields.

(M) Length of the field "list of mechanisms to be used" : This field provides the length of the "List of mechanims to be used". Since the list of mechanisms should include one mechanism to ensure user data traffic padding service at least, this field is always greater than 0 and the field "List of mechanisms ..." is never omitted.

(M) List of mechanisms to be used : This field indicates a list of mechanisms (with their respective parameters) ordered according to preferences. That is, during connection set up, the SIE originator indicates within SET UP a set of mechanisms that could be used for that connection to provide user data traffic padding service and the SIE retriever sends back within CONNECT the chosen mechanism, provided that one is suitable.

3.10 SIE's access control element

(O) The access control Element contains similar fields than these included in the access control IE described in [AFSEC] section 4.5.4.

This element is optional.

4 Conclusion

Implementation of SIE has been done at Telecom Bretagne, Rennes, France, in SUN's ATM drivers environment. For further details relative to the implementation, refer to [Lau97] which additionally presents a survey of existing solutions aiming to secure communications over ATM networks.

5 References

[AF96-1244] Peyravian, M et al., "Security Entity Identifier Information Element", ATM Forum/96-1244, October 1996.

[AFSEC] Phase 1 ATM Security Specification (Draft), ATM Forum/95-1473R5, October 1996.

[AFSIG] The ATM Forum Technical Committee, "User-Network Interface (UNI) Specification", Version 3.1, September, 1994.

[Lau97] Laurent M., Paul O. and Rolin P., "Securing communications over ATM networks", IFIPSEC'97, Copenhagen, Denmark, May 1997. [Online] Available http://www.rennes.enst-bretagne.fr/~mlaurent/index-engl.html.