Secure Communications in ATM Networks

Maryline Laurent, IRISA
Ahmed Bouabdallah, Christophe Delahaye, ENST de Bretagne
Herbert Leitold, Reinhard Posch, IAIK
Enrique Areizaga, Fundacion Robotiker
Juàn Manuel Mateos, Inelcom Ingeniera

Abstract

The ATM Forum international consortium recently approved the first version of its security specifications aiming to protect communications over Asynchronous Transfer Mode (ATM) networks by offering data confidentiality, partners authentication, etc. This paper describes the architecture of one of the first ATM Forum compliant security prototypes being currently developed in the European project SCAN (Secure Communications in ATM Networks). Additionally to the security management functions specified by the ATM Forum to exchange encryption keys and negotiate security services, SCAN implements the possibility for end-users to modify the data flow encryption algorithm during a connection in progress, and the possibility to keep the encryption algorithm choice confidential. Moreover a flexible implementation is offered allowing future users to develop their own security protocols and their own ATM security monitoring applications.

1. Introduction

The Asynchronous Transfer Mode (ATM) technology success is due to its ability to support multimedia applications needs offering high bit rates and real time guarantees. Another ATM interesting feature is the early introduction of security services into ATM specifications, thus resulting in an efficient security solution to protect the ATM traffic against eavesdropping, traffic tampering, and masquerade. The introduction of the confidentiality, integrity, and authentication services into ATM appears helpful for the deployment of security sensitive multimedia applications such as the telemedecine applications where patient files are expected to be kept confidential, and modified only by authorized persons **[1]**.

This paper describes the architecture and choices elected in project SCAN (Secure Communications in ATM Networks) to develop a prototype ensuring ATM traffic encryption at 155 Mbps, with inherent security management. This prototype is expected to be at least ATM Forum compliant, offering data encryption on a connection basis, and allowing security information to be exchanged through ATM signaling. The prototype is limited to point-to point communications environment, and additionally to the ATM Forum specifications, it implements the possibility to modify the data encryption algorithm during a connection in progress, and to improve the security level by maintaining security sensitive information secret.

This paper focuses mainly on security management aspects detailing the solutions chosen for updating session keys, and for negotiating the security services and mechanisms that will be used to protect subsequent exchanges. Attention is paid to describe the open interfaces of the prototype, which provide flexibility so that future users can develop their own security protocols fitting their own security needs, and national legislation.

More precisely, section 2 introduces ATM and the ATM security needs allowing readers to understand the remainder of the paper. Section 3 describes the security services and functions specified in current ATM Forum specifications. The following sections give a SCAN technical description, presenting the data encryption mechanism (section 4), the session key update (section 5), the security parameters negotiation (section 6), and the signaling protection (section 7). The security parameters monitored by users are presented in section 8 as SCAN security policy. The architecture of the SCAN prototype is provided in section 9, along with its open interfaces in section 10. Finally, section 11 gives some conclusions, and section 12 a list of useful acronyms.

2. Introduction to ATM security

The ATM technology is connection-oriented, that is, prior to any data exchange, it is necessary to set up connections (or virtual channels) over which data are later sent. To distinguish between connection monitoring operations and data exchange processing, the ATM protocol reference model is divided into planes. As depicted in figure 1, three planes are defined:

- The control plane to monitor signaling information that is, to set up, release, and control ATM connections
- The user plane to transfer data through data channels.
- The management plane to maintain the ATM network operational, propagating possible alarms and ATM traffic statistics.

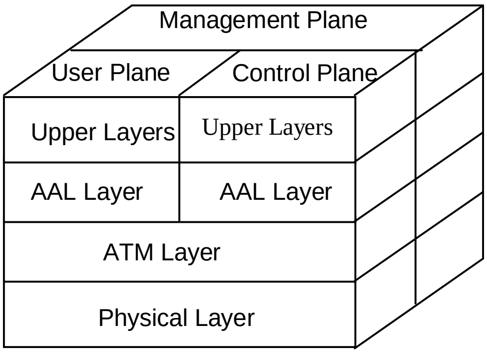

Figure 1 The ATM reference model

The management and control planes communicate over the ATM network through reserved virtual channels. However possibility is given to the management planes to exchange management information over the data channel being managed. As such, the management flow is the only one offering synchronization with the data flow.

Remote entities′ control planes communicate thanks to signaling messages. Signaling messages contain a header specifying the message type, and many signaling IEs (Information Elements) informing of connection specific needs such as the quality of service, the upper application type, etc. Signaling messages include setup, connect, status, and release messages. The setup message is sent by the connection initiator, and propagates through the ATM network to the responder which should send back a connect message to complete the connection establishment. For a connection to be released, two processes are available. The soft one is to send a release message, waiting for a release complete message to release the resources allocated to the connection. The other approach is to send a release complete prior to deallocating the resources. Other signaling messages are defined, such as status informing of the control plane state associated to a specific connection, and restart to reinitialize a connection.

ATM is a cell-switching network. That is, any information sent over the network is in the form of 53-byte ATM cells including a header which specifies the ATM connection identifiers called VPI/VCI for Virtual Path/Circuit Identifiers. For the management planes to communicate, specific OAM (Operation And Maintenance) cells are defined. However for user planes and control planes to communicate, it is necessary to segment data frames, and signaling messages into ATM cells. As such, three layers modeling the processing to be done to obtain those ATM cells are defined in the ATM reference model: the physical layer mainly responsible for information transportation; the ATM layer mainly in charge of multiplexing and switching functions; the ATM Adaptation Layer (AAL) whose main function is to adapt services needs to ATM streams by performing segmentation into (/reassembly of) cells for instance.

The ATM model analyzis leads to the conclusion that the ATM traffic divides into three ATM flows types, data, management, and signaling flows. As such, three flows can be subject to attacks while in transit

[2]. Data flows can be eavesdropped, and tampered, resulting in more or less severe losses. Signaling messages, and especially setup messages are vulnerable to eavesdropping, tampering, and masquerade. Eavesdropping setup messages informs the eavesdropper of the end-entities that need to communicate, and the type of application that will be used. Masquerades consist in constructing setup messages with a bogus source ATM address. The management flow is vulnerable to tampering attacks, since injecting alarms into the ATM network for instance may lead to improper connections releases.

It is clear that ATM flows require protection. However, since connections are expected to be of various sensitivity levels, it is necessary that first the security services used to protect data are negotiated. As a result, ATM security studies expect to introduce the following protections:

- Signaling protection by offering the authentication, integrity, and confidentiality services.
- Data protection, ensuring the confidentiality, integrity, and authentication of data.
- Security parameters negotiation. Three approaches may be considered whether security parameters are exchanged between security equipments through signaling messages, data channel, or OAM cells.

The OAM cells protection is not studied in current works, since OAM cells are not implemented in most of current ATM equipments, and since the OAM cells size is fixed thus precluding any authenticator or integrity check value to be introduced.

The next section describes the ATM Forum security specifications 1.0 emphasizing the required security services.

3. The ATM Forum specifications 1.0

Since 1995, the security working group of the ATM Forum has been working on ATM security aspects approving the first version of the ATM security specifications **[3]** **[4]** in

February 1999. Those specifications aim to provide confidentiality of data, and integrity, and authentication of both data and signaling messages. Required services are as follows:

- Data confidentiality. Data are encrypted on a cell-by-cell basis encrypting only the 48-byte ATM cell payload. The encryption algorithms being considered include DES (Data Encryption Standard), TripleDES, and FEAL, and the operational modes offered are the ECB (Electronic CodeBook), CBC (Cipher Block Chaining), and the counter mode. Because of US legislation exportation restrictions, DES is expected to be used either with 40-bit or 56-bit effective keys.
- Data integrity, and authentication. AAL frames are protected by appending a cryptographic checksum to AAL frames. Possibility is given to provide replay/reordering protection by introducing a sequence number into AAL frames before calculating the cryptographic checksum.
- Security parameters negotiation.

  Two approaches are allowed, whether the security parameters are sent through signaling messages, or in-band through the data channel. The first one consists in appending a security IE (SIE) to setup, and connect messages. This SIE exchange allows the connection partners to negotiate the security services, and mechanisms, and to exchange the encryption keys to be used to protect their data transfer. For the encryption keys to remain confidential, and for the connection partners to be sure of their respective identity, existing two-way Security Message Exchange (SME) protocols are used.

  Protocols considered in the ATM Forum specifications refer to three levels of key: the session key used to encrypt data, the master key used to encrypt session keys when updating session keys during a connection, and the top-level key which is an asymetric key used to authenticate and initialize the first session key, and master key securely.

  An alternative to the signaling approach is to block the data traffic as soon as the connection is established, to realize the security negotiation through the data channel, and finally to unblock the data transfer. To avoid that the called partner considers incoming security information as data, the connection initiator indicates that the negotiation is done in-band thanks to a SIE within the set up message. The negotiation is done encapsulating the same SIEs than in the signaling approach, into simplified signaling messages. One advantage over the signaling approach is that the SIE length is not limited in the in-band approach, thus allowing long-length information such as keys certificates to be included into the SIE. For reliable SIE exchanges, additional in-band control messages are defined such as CONFIRM-AP to acknowledge the final SIE, and FAULT to indicate why the negotiation fails. The in-band approach is expected to use three-way SME protocols.
- Signaling protection. Any signaling messages may be authenticated and integrity protected by introducing a digital signature into an SIE. Especially, if an SME protocol is employed, protection is offered for setup and connect messages by calculating the signature over the SIE fields specified by the SME protocol. It is still offered for any other signaling messages (release, status, restart), and for setup and connect messages (if the SME protocol is not used) by introducing a signature calculated over part of the SIE.
- Session key update through OAM cells. For encrypted connections to be as secure as possible, session keys are expected to be updated from time to time. Because of their synchronization with the data flow, OAM cells were selected to carry session keys. Two steps are defined for session key updating. Firstly, a session key is sent encrypted under the master key through a specific OAM cell called SKE (Session Key Exchange) cell. Secondly, the session key is activated thanks to an SKC (Session Key Changeover) cell. During SKC cells transmission, the data traffic is blocked over the connection so that the data following the first SKC OAM cell received are decrypted under the new session key. Obviously if only one pair of SKE/SKC cells is sent, and one of them is lost during transfer, this results in subsequent data remaining undecryptable for the receiving end-station. To counteract that, the ATM Forum proposes to send a flow of similar SKE cells followed by a flow of similar SKC cells so that at least one SKE and one SKC cells are assumed to be received, thus resulting in a correct session key update. To preclude possible bursts from erasing all the transmitted OAM cells flows in the network, SKE and SKC cells are sent with a delay between each transmission.

In the security specifications of February 1999, it is envisaged that access control is offered by appending a security label to the setup and connect messages, which indicates the sensitivity level of the connection (public data, proprietary, company confidential, etc.). Security equipments (switches, end-stations) are expected to check this label against the label assigned to the links used to reach the destination. If no links have the sufficient level, the connection is aborted.

Project SCAN security aspects are close to the ATM Forum specifications, so that next sections describing SCAN security functions are closely related to the present section.

4. Data confidentiality

A hardware cryptographic unit called HADES (see section 9) is embedded into an ATM NIC card and is used to encrypt data traffic up to 155 Mbps with compliance with the ATM Forum. That is, it encrypts ATM cell payloads only. Available encryption algorithms are DES, and TripleDES with the ECB or CBC operational modes.

One problem to be solved when considering data cells encryption at 155 Mbps is the key agility problem presented for the first time in [5]. This problem arises when fast session keys change is required. This happens when each incoming cell needs to be encrypted with a session key different from the previous one. This means that in the worst case, a session key needs to be downloaded every 2.83 µs ((53*8)/ (149.76*10^6)) [6]. SCAN solves this problem using fast access CAM (Content Access Memory) memory.

Since session keys as defined in the ATM Forum are unidirectional, each connection is provided with a pair of keys, one for encryption, and one for decryption. Session keys are downloaded from the NIC card drivers (the IE/OAM module described in section 9) using SCAN specific session key downloading cells (later referred to as AAL0 cells). AAL0 cells inform the HADES unit of the algorithm and mode of operation to be used over one VPI/VCI connection, and the session key(s) that should be employed for either encryption or decryption. AAL0 cells include two 64-bit session key fields, both of them being required when the TripleDES encryption algorithm is selected. AAL0 cells include also a 64-bit Initialization Vector useful for the CBC mode of operation.

AAL0 cells are locally identified by some specific connection identifiers M-VPI/M-VCI, and a specific payload type. These M-VPI, and M-VCI values are selected by the NIC card driver at the HADES unit initialization thanks to a configuration-VC cell which is identified itself by the means of the unused connection identifiers VPI/VCI=0/0. Upon reception of an AAL0 cell, the HADES unit downloads the new session key for encryption or decryption, and discards it, so that AAL0 cells remain local to the ATM end-station.

5. Session key update

Session keys used to encrypt data are updated during connections in progress with compliance with the ATM Forum specifications using the SKE/SKC cells (cf. section 3). In SCAN, session keys are updated either periodically, or depending on the amount of data cells being sent encrypted under the same session key over the connection. Session keys are unidirectional so that each party is responsible for updating its encryption key as frequently as it needs. As part of the security policy parameters, the session key update period expressed in seconds or in number of cells can be configured by each party from the user space using a specific interface (see sections 9 and 10).

Once the session key update completes, the HADES cryptographic unit should be informed of the new encryption or decryption key to be considered over one unidirectional connection. That is, after SKC cells transmission, and prior to unblocking the data traffic, it is necessary that the HADES unit is informed of the new encryption session key to be considered thanks to an AAL0 session key download cell. The remote party should download the same session key for decryption after the first corresponding SKC cell is received.

6. Security parameters negotiation

Like in the ATM Forum specifications 1.0, two approaches are considered in SCAN for negotiating the security parameters used to protect subsequent data transfers. These are the following:

- Negotiation through signaling messages. This approach being supported in the ATM Forum specifications 1.0 allows the future SCAN prototype to interoperate with other non-SCAN ATM security equipments at the condition that the SIE being constructed is ATM Forum compliant (see section 6.1). Like in the ATM Forum, only two-way SME protocols are supported in the signaling approach.
- Negotiation through OAM cells. This approach is SCAN specific, and consists in encapsulating security parameters into newly defined "negotiation OAM cells" dedicated to security. This approach is interesting if permanent connections are considered as no security parameters negotiation through setup signaling messages is allowed. Negotiation through OAM cells is also interesting when master keys (cf. section 3) need to be updated during a connection in progress, when the security officer modifies the security policy to be enforced over the connection, or when a great number of errored data cells are received, thus implying that the previous session key update was errored.

Contrary to the ATM Forum in-band approach supporting only the three-way SME protocols, the SCAN OAM cell negotiation approach enables both the two and three-way SME protocols to be used. Another advantage is that the negotiation can occur at any time during the connection, and not only when establishing a connection. As such, end-stations are allowed to renegotiate security parameters as often as they need. Actually, in SCAN, possibility is given to initiate a new security parameters negotiation either periodically, or depending on the percentage of cells received with an errored-content, thus allowing possible improper session key updates to be detected.

Since the negotiation OAM cells aim is similar to what is done in the ATM Forum security specifications 1.0 at connection setup through the SIE, it was decided that the SIE is reused to realize a context negotiation by encapsulating the SIE within negotiation OAM cells. Since the SIE may be bigger than the 46-byte payload offered in OAM cells, SIE segmentation should take place before its encapsulation into negotiation OAM cells. As such the principle adopted by the ATM Forum for the session keys exchange which consists of sending the same session key updates OAM cells several times to be sure that at least one cell arrives at the destination does not apply for the negotiation OAM cells. The solution elected in SCAN to ensure that reliable SIE exchanges through negotiation OAM cells is to define a cell-loss recovery protocol based on sequence numbers and acknowledgement OAM cells. This protocol has been validated, and is described in section 6.2.

Since the OAM cell negotiation approach allows connection partners to initiate a new session key update or a new security context negotiation at any time during a connection, collisions between those mechanisms can occur, leading to improper session keys updates for instance. As such a collision manager is introduced, to decide which mechanism is to be stopped to allow the other one to complete. The general rule enforced is that a negotiation has precedence over a session key update, and when two negotiations are initiated simultaneously, the connection partner with the greater ATM address should stop the negotiation it initiated.

6.1 SCAN Security IE

One aim of SCAN is to be at least ATM Forum compliant. As such, to realize security parameters negotiation, SCAN constructs the SIE as specified in version 1.0 of the specifications **[3]**, using the two and three-way RSA-based SME protocols. The ATM Forum SIE format is given in figure 2. Only fields meaningful for SCAN are present and are explained hereafter:

- The SIE identifier identifies the SIE from other signaling IEs.
- The 2-bit Coding Standard is used to distinguish between the ITU-T and the ATM Forum compliant SIE.
- The remaining SIE fields are divided into Security Association Sections (SAS). Each SAS includes the security information that is exchanged between two security agents, which may be either end-stations as considered in SCAN or intermediary equipments.
- The Version field identifies the ATM Forum specifications to which the SIE is compliant.
- The Scope, Target Security Entity ID, and Security Entity ID fields allow one security agent to identify itself as the SIE target security agents.
- The Relative ID field identifies the security association the SAS refers to.
- The following fields relative to the SME protocol are identified by the SME Format-SME Type fields. SME Type identifies whether the SME protocol is two or three-way exchange.
- The Security Services Specification Section includes the security parameters relative to the data protection (encryption algorithm, and mode of operation, etc.) and the SIE construction (SME protocol, signature algorithms, etc.).
- The Confidentiality Section includes the master key, and session keys, which are all encrypted by the means of the SME protocol.
- The Authentication Section contains a timestamp, a random number, and the digital signature calculated over the fields specified by the selected SME protocol.

Security IE Identifier			
	Coding Standard		
Length			
Security Association Section ID			
SAS Length			
Version			
Scope			
Relative ID			
Target Security Entity ID			
SME Format-SME Type			
Security Entity ID			
Security Services Specification Section			
Confidentiality Section			
Authentication Section			

Figure 2 The SIE of the ATM Forum

Besides the security parameters, end-partners authentication, and secure keys transfer, SCAN provides end-partners with the possibility to ensure the confidentiality of security services and parameters being negotiated during a connection in progress or at connection setup. This possibility is interesting because an eavesdropper positioned at a point on the network can easily select sensitive connections to disrupt by filtering setup signaling messages or negotiation OAM cells according to the security services required. Indeed more security services are needed over a connection, more likely it is that the connection is sensitive. By encrypting some of those security parameters, this eavesdropping attack becomes less efficient. To do that, a new section called SCAN Confidentiality Section is introduced in the SIE replacing the ATM Forum Confidentiality Section. The distinction between the SCAN specific SIE and the ATM

Forum compliant SIE is done thanks to the Coding Standard field.

The SCAN Confidentiality Section includes the ATM Forum Confidentiality Section and subpart of the Security Services Specification Section relative to data protection. The encryption is done over the content of the SCAN Confidentiality Section so that the keys and data protection parameters (data encryption algorithm, and mode of operation, session key update mechanism) remain confidential. The encryption algorithm used is the same as this employed for keys encryption, that is, it is specified in the Security Services Specification Section in cleartext.

6.2 The cell-loss recovery protocol

The purpose of this protocol is to ensure that a SIE being exchanged over the network encapsulated into negotiation OAM cells is received with no losses and correctly ordered. As such, when segmenting a SIE, each SIE segment is numbered with a sequence number and each negotiation OAM cell includes the sequence number associated to the SIE segment it carries. A group of negotiation OAM cells are acknowledged at the same time by a newly defined "acknowledgement OAM cell" which includes the sequence number of the next negotiation OAM cell expected.

The complexity of the protocol is due to possible losses occurring in the network, and the SIE processing time being undefined since dependent on the SME protocol security mechanisms used. The difficulty is that session keys should be updated at the end of the SIE exchanges, but should only take place after the last SIE is processed for the decryption session key to be decrypted and ready to be downloaded into the cryptographic unit. Because of it, and because of the specific role of the acknowledgement cell in the last SME flow, three kinds of acknowledgement cells are defined:

- Intermediate acknowledgement cells are used to acknowledge negotiation OAM cells which are not the last one in the last SME flow. For bandwidth optimization purpose, their transmission is done when a cell loss is detected, or when no negotiation OAM cells have been received for a long time while the SIE is not fully received yet.
- Final acknowledgement cells are sent to acknowledge the last negotiation OAM cell of the last SME flow.
- Other acknowledgement cells are sent to specify that a partner is ready for session key changeover processing.

Since no means is used to be sure that the latter two kinds of acknowledgement cells arrive to the destination, the same mechanism as this used for session keys downloading SKE/SKC cells transmission is employed (cf. section 5). That is, a number of similar acknowledgement OAM cells are sent with a delay between their transmission.

In order to preclude that both partners wait indefinitely for negotiation OAM cells or acknowledgement cells because of possible losses during transfer, two periods are introduced: IePeriod and AckPeriod. IePeriod (respectively AckPeriod) is the maximum delay between a full SIE transmission and the acknowledgement cell reception (resp. intermediate acknowledgement cell transmission and SIE reception). When IePeriod (resp. AckPeriod) elapsed, the SIE (resp. intermediate acknowledgement cells) is fully transmitted again. To avoid infinite SIE (resp. intermediate acknowledgement cells) transmissions, a maximum number of SIE transmissions MaxTryIe (resp. MaxTryAck for the maximum of intermediate acknowledgement cells retransmissions) is defined as part of the local security policy.

Once the negotiation is completed and the corresponding acknowledgement cells are sent, the new session keys exchanged by the SME protocol can be activated. One solution would be to block the data traffic over the connection during the negotiation duration so that the session keys can be downloaded into the cryptographic unit after the negotiation completion. The problem is that the negotiation duration is not known and that it is inappropriate to block the data traffic for a long time. As such, a better solution is to realize session key exchange in two steps, as being done when updating a new session key. That is, once the negotiation is completed, each connection partner activates its new session key using the SKC (Session Key Changeover) cells (see section 5).

7. Signaling protection

Like in the version 1.0 of the ATM Forum specifications, SCAN proposes that any signaling message (setup, connect, release, status, etc.) is protected proving the origin and integrity of the message. This protection is already ensured if the SME protocol is selected, but it remains limited to the setup and connect messages. As such, it is important to provide another method to ensure authentication and integrity of any signaling messages. This method is later referred to as "**authentication only**", and consists in introducing a digital signature into the SIE Authentication Section field (cf. figure 2). Contrary to the signature generated by the SME protocol, the signature generated for the authentication only is calculated over the entire Security Association Section. The available signature generation algorithm in SCAN is the RSA algorithm.

8. SCAN security policy

Users (e.g. the security officer) are allowed to define the security services and mechanisms to be used over connections from the user space (the Security Policy module mentioned in section 9). That is, each possible ATM destination is provided with a list of authorized encryption algorithms, and modes of operation, a list of authentication algorithms, a list of "in-band" SME protocols to be used for negotiation through OAM cells, and a list of out of band SME protocols to negotiate through ATM signaling, all of them being ordered according to preferences. For SCAN, six encryption algorithms/modes of operation, one authentication algorithm (RSA), four "in-band" SME protocols (two or three-way RSA-based SME protocols + security parameters confidentiality) and two out-of-band SME protocols (two-way RSA- based SME protocol + security parameters confidentiality) are implemented.

Moreover possibility is given to users to monitor security management parameters local to end-stations from the user space. Those parameters include the periodicity rules for new session key update and new security parameters negotiation expressed in seconds, number of cells encrypted under the same session key or percentage of errored-data cells received.

Other security management parameters are session key update oriented, such as the maximum number of SKC/SKE cells to be sent to be sure that at least one arrives at the destination, and the delay between two SKC/SKE cells transmissions. Also they include the cell-loss protocol parameters AckPeriod, IePeriod, MaxTryIe, and MaxTryAck defined in section 6.2.

9. SCAN architecture

Realizing the high-speed ATM cells encryption prototype requires developing an ATM NIC (Network Interface Card) card, the NIC monitoring drivers, and some security management software modules. A SCAN specific ATM NIC card development was necessary to plug a cryptographic unit realizing the High-speed ATM DES/TripleDES (HADES). This HADES unit intercepts the ATM cells flow between the AAL and ATM layers, at the ATM Forum standardized UTOPIA (Universal Test and Operations Physical Interface for ATM) interface for encryption.

The prototype is expected to be operational in the Windows NT 5.0 and Windows98 environments. Drivers are developed using Network Driver Interface Specification (NDIS) version 5. As depicted in figure 3, additionally to the NIC driver, the SCAN software includes three security management modules:

- The SP (Security Policy) module allows users (or the security officer) to inform the IE/OAM module of the security policy (cf. section 8) to be applied for a specific ATM destination.
- The IE/OAM module is responsible for most of the SCAN security management aspects, that is, session keys update, session keys download into the HADES unit, and the security parameters negotiation either through OAM cells or signaling.
- The KM (Key Management) module implements the RSA-based SME protocol, and the RSA authentication service, and therefore participates to the SIE construction together with the IE/OAM module.
- The NIC driver manages the NIC hardware resources, and the NDIS driver memory. It should deviate signaling messages so that all of them go through the IE/OAM module. Contrary to the IE/OAM module, it has access to the data traffic so it is required to inform the IE/OAM of the number of data cells being sent over a connection or the percentage of errored-content data cells received, to make it initiate new session keys updates or new negotiations.

What makes the SCAN prototype attractive with respect to other market ATM security products is its flexibility. Implementing the SP module in the user space allows future users to easily develop their own SP module, as part of an application for instance, with their own user interface to specify their security policy. The KM module being in the user space makes it possible to use SME protocols (respectively, authentication algorithms) other than the SCAN ones by merely replacing the KM module with another module. The latter aspect is interesting considering that some SME protocols (resp.

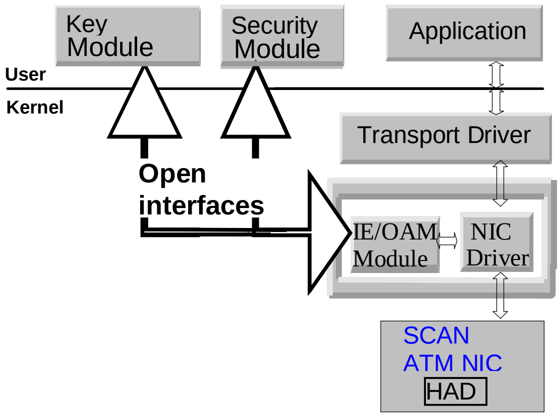

Figure 3 The software modules architecture

authentication algorithms) are prohibited in some countries and the communications protection level may strongly vary depending on people's security needs. Inherent interfaces between the KM and IE/OAM modules, and between the SP and IE/OAM modules are described in the next section.

10. Open interfaces

In SCAN, future users are allowed to develop their own SP and KM modules (see section 9), to integrate them in some applications, and to select more appropriate SME protocols and authentication algorithms than those proposed in SCAN. As such, two interfaces, one between the IE/OAM and SP modules and one between the IE/OAM and KM modules are specified and made publicly available in documents **[7]** and **[8]**. Messages exchanged at those interfaces along with their respective propagation direction, the parameters they contain, and their functions are specified in tables 1 and 2.

What clearly appears in table 1 is that the SP module can be used as a connections monitoring tool since it is informed of the security parameters being negotiated over a connection, and it is allowed to release any connections in progress.

For a better understanding of the KM/IEOAM interface, the following notions need first be explained:

- **Indexes**. Details of the SME protocols and authentication algorithms are only known by the KM module. The SME protocols and authentication algorithms being available in the KM module are referred to as indexes in the SP and IE/OAM modules and are listed in a configuration file along with their description in natural language. As such, when defining the security policy, the SP module consults the available protocols and algorithms along with their description in the configuration file. To preclude the SP (users) from selecting a three-way SME protocol for negotiation through signaling, and a protocol realizing some security parameters confidentiality while the ATM Forum compliance is required, 1-byte SME protocol indexes include in their first two bits the two/three-way exchange information, and the provision of the security parameters confidentiality.
- **Partial SIE construction**. The SIE is partly constructed in the IE/OAM and the KM. That is, the IE/ OAM is responsible for all the data protection aspects (negotiation of the data confidentiality service, and session key update mechanisms) while the KM is responsible for the SME protocol and authentication service ones (algorithms selection, signature generation/verification). As such, the IE/OAM constructs a partial SIE, and sends it to the KM for completion. To do that, it is required that the KM informs the IE/OAM of the fields to be included, as mentioned in the first four messages of table 2.

Message type	Direction	Message content	Functions
Security Policy Consultation Request	IE/OAM -> SP	Local connection ID ATM partner address	Request for the security policy to be enforced with that ATM partner
Security Parameters	IE/OAM <- SP	Local connection ID Security parameters (SME index, local parameters, etc.)	Response to the previous request message, or Notification of the security policy modifications
Security Parameters Negotiation Result	IE/OAM -> SP	Local connection ID Security parameters (SME index, confidentiality algorithm)	Notification of the security parameters resulting from the negotiation
Release Connection	IE/OAM <-> SP	Local connection Ids	Release of one or more connection(s)

Table 1 : Messages at the SP/IEOAM interface

Message type	Direction	Message content	Functions
SME Protocol Features Consultation Request	IE/OAM -> KM	Local connection ID SME protocol index	Request the SME protocol features useful for the partial SIE construction

SME Protocol Features Consultation Response	IE/OAM <- KM	Local connection ID SME protocol index SME protocol features	Inform of the fields of the partial SIE when an SME protocol is selected depending on the flow number
Authentication Service Features Consultation Request	IE/OAM -> KM	Local connection ID	Request the authentication service features useful for the partial SIE construction
Authentication Service Features Consultation Response	IE/OAM <- KM	Local connection ID Authentication service index Authentication service features	Inform the fields of the partial SIE when the authentication service is selected
SIE for Security Negotiation	IE/OAM <-> KM	Local connection ID SME protocols list SIE	Includes the partial or full SIE used for negotiating the security parameters
SIE for Authentication Only	IE/OAM <-> KM	Local connection ID Authentication algorithms list SIE	Includes the partial or full SIE used only for authentication
Release Connection	IE/OAM <-> KM	Local connection IDs	Release of one or more connection(s)

Table 2 : Messages at the KM/IEOAM interface

Security services and mechanisms	Version 1.0 of the ATM Forum specifications	SCAN
Data confidentiality	ATM layer over the cell payload DES/TripleDES ECB/CBC/ Counter mode	ATM layer over the cell payload DES/TripleDES ECB/CBC
Data integrity	AAL layer	
Session key update	OAM cells MD5/SHA-1	OAM cells MD5
Security parameters negotiation	Through signaling or the data channel	Through signaling or OAM cells
Possible SME protocols	2-way protocol (signaling) 3-way protocol (data channel)	2-way protocol (signaling) 2/3-way protocol (OAM cells) 2/3-way RSA-based protocols (+MD5) SME protocols may include security parameters confidentiality
Signaling protection	Access control Authentication MD5/SHA-1/RIPEMD-160 +RSA/DSA/DESCBC/ DES40CBC/ Triple DES CBC/ FEAL CBC	Authentication MD5+RSA algorithm

Table 3 : Security service placements and security mechanisms offered in SCAN vs the ATM Forum

11. Conclusions

In this paper, we describe the technical choices elected in project SCAN to ensure the ATM traffic encryption at 155 Mbps providing ATM Forum compliance and offering a flexible implementation. This paper presents first the security services and mechanisms currently supported by the version 1.0 of the ATM Forum security specifications **[3]**, and then it details the SCAN security functions being currently under development.

As depicted in table 3, SCAN implements the data encryption and session keys update as specified in the ATM Forum specifications, however it does not support the integrity service proposed by the ATM Forum. Like in the ATM Forum, SCAN proposes that the negotiation of security services used to protect subsequent data exchanges is done at connection setup by introducing a SIE (Security Information Element) dedicated to security into setup signaling messages. What differs from the ATM Forum specifications is the possibility to renegotiate the security services during a connection in progress by encapsulating the same SIE into SCAN specific "negotiation OAM cells". Because of the limited OAM cells payload size, SIEs are segmented prior to their encapsulation. To allow a reliable SIE transfer through OAM cells, a cell-loss recovery protocol has been defined, and validated.

In SCAN two kinds of SIE are implemented. One is ATM Forum compliant, allowing parties to authenticate to each other, to negotiate security parameters, and to exchange keys securely. The other one is SCAN specific. Additionally to the ATM Forum SIE functions, it ensures the confidentiality of part of the negotiated security parameters. Therefore SCAN improves the ATM connections security level since possible eavesdroppers can no longer deduce the data encryption algorithm used, and thus it makes it more difficult for them to break the encryption keys and to filter ATM connections.

Flexibility is targeted in SCAN implementation and is offered by exporting two security management software modules into the user space. One software module implements the security protocol related mechanisms, and the other one manages the security policy. The interfaces between those modules and the kernel space are publicly available, thus making it possible for future SCAN users to develop their own security protocols and their own security policy monitoring applications.

12. Acronyms

DES: Data Encryption Standard
CBC: Cipher Block Chaining
ECB: Electronic CodeBook
IE: Information Element
OAM: Operation And Maintenance
SIE: Security IE
SKC: Session Key Changeover
SKE: Session Key Exchange
SME: Security Message Exchange

13. Acknowledgements

Project SCAN (Secure Communications in ATM Networks) is funded by the European Commission, Directorate General XIII, ACTS Programme 3rd call, project number AC330.

14. References

[1] R.J. Anderson, "A security policy model for clinical information system", *IEEE Symposium on security and privacy,* pp. 30-43, 1996.

[2] M. Laurent, O. Paul, P. Rolin, «Securing Communications over ATM Networks: The Remote ATM Private Networks Inter connection Example», *Annales des télécommunications,* N°9-10, September-October 1998.

[3] ATM Forum, "ATM Security Specification Version 1.0", February 1999.

[4] T.D. Tarman, R.L. Hutchinson, L.G. Pierson, P.E. Sholander, E.L. Witzke, "Algorithm- Agile Encryption in ATM Networks", *IEEE computer,* Vol.31 N°9, pp. 57-64, September 1998.

[5] D. Stevenson, N. Hillery and G. Byrd, "Secure Communications in ATM Networks", *Communications of the ACM*, Vol.38, N°2, 1995.

[6] H. Leitold, R. Posch, E. Areizaga, A. Bouabdallah, M. Laurent, J.M. Mateos, O. Molino, "Security Services in ATM Networks", Interoperable Communication Networks ICON Journal, Baltzer Science Publishers, 1999.

[7] M. Laurent, "The Key Management Module Interface", ACTS deliverable D64, project SCAN, March 1999.

[8] M. Laurent, "The Security Policy Module Interface", ACTS deliverable D63, project SCAN, March 1999.