The ATM Forum
Technical Committee

ATM Security Framework 1.0

AF-SEC-0096.000

February, 1998

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and The ATM Forum is not responsible for any errors. The ATM Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither The ATM Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by The ATM Forum or the publisher as a result of reliance upon any information contained in this publication.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

- Any express or implied license or right to or under any ATM Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
- Any warranty or representation that any ATM Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
- Any form of relationship between any ATM Forum member companies and the recipient or user of this document.

Implementation or use of specific ATM standards or recommendations and ATM Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in The ATM Forum.

The ATM Forum is a non-profit international organization accelerating industry cooperation on ATM technology. The ATM Forum does not, expressly or otherwise, endorse or promote any specific products or services.

NOTE: The user's attention is called to the possibility that implementation of the ATM interoperability specification contained herein may require use of an invention covered by patent rights held by ATM Forum Member companies or others. By publication of this ATM interoperability specification, no position is taken by The ATM Forum with respect to validity of any patent claims or of any patent rights related thereto or the ability to obtain the license to use such rights. ATM Forum Member companies agree to grant licenses under the relevant patents they own on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. For additional information contact:

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

Contents

0. Preface to ATM Security Framework 1.0

The aim of the ATM Security Framework 1.0 is to derive generic security requirements for security services provided within ATM networks. Therefore the framework does not take into consideration specific security aspects of ATM users and applications like wireless ATM, residential broadband, network management over ATM.

The ATM Security Framework 1.0 reflects the state of the ATM Security Specification 1.0 (see [1]). The parts of the phase 1 framework marked with "TBD“ will be handled in phase 2.

The topics in Table 1 are covered in this document. Topics that are partly covered in this document are denoted with a partly status, while topics to be covered in the next version of the framework are denoted with a phase 2 status.

Topic	**Reference**	**Status**
Generic security objectives	chapter 2	stable
Generic threats	chapter 3	stable
Functional security requirements and security services	chapter 4	stable
Plane specific interpretation of functional security requirements · User plane · Control plane · Management plane	chapter 5	 stable partly / phase 2 phase 2
Requirements for support services	chapter 6	partly / phase 2

Table 1: Contents of ATM Security Framework 1.0

1. Introduction and Scope

ATM networks require adequate security features to protect the involved systems, their interfaces, and the information they process. The security requirements for ATM networks originate from the following sources:

- customers / subscribers who require confidence in the ATM network and the services offered (for example, accurate billing),
- the public communities / authorities who demand security using directives and legislation to ensure availability of services, fair competition and privacy protection, and
- network operators / service providers who require security to safeguard their business interests, and to meet their obligations to their customers and the public.

This framework identifies:

- generic security objectives of the customers / subscribers, network operators / service providers and public communities / authorities for an ATM network (Chapter 2),
- generic threats to these objectives (Chapter 3),
- resulting principal functional security requirements to counteract these threats (Chapter 4),
- an ATM terminology formulation of functional security requirements (Chapter 4, AF SEC-1 to AF SEC-10),
- a list of generic security services that have the potential to counteract all of these threats for ATM networks (Chapter 4), and
- plane specific interpretation of functional security requirement (Chapter 5).

This framework **does not include**

- a mapping of the security services to the ATM network architecture, especially to the ATM user, control and management plane, and
- the identification of mechanisms and algorithms to realize the security services.

This shall be included in further steps.

Remark: In a concrete ATM network instance, not all of these threats may become major risks that endanger the security objectives. In this case, only the functional security requirements must be fulfilled, which are related to the threats leading to a major risk. This implies, that in a concrete ATM network instance probably not all security services will be used.

The following sections are based on work done in the standardization bodies ETSI ([4] [5]) and ITU-T ([7]).

2. Generic Security Objectives for ATM Networks

The purpose of this chapter is to describe the objectives of security mechanisms within an ATM network. The focus of this exercise is to describe what security mechanisms will achieve rather than how they are implemented. These generic security objectives will form the basis of the generic threat analysis in the next chapter.

In this chapter, security objectives are derived from more general objectives that have an impact on security. The objectives of the following groups were considered;

- customers (service subscribers and users),
- operators (network operators and service providers), and
- public communities / authorities.

General constraint objectives like performance, cost, and user friendliness are outside the scope of this document.

2.1. Customer Objectives

Customer objectives are not uniform since each customer has its set of objectives. For example, an enterprise does not always have the same objectives as a private person. The following list gives examples of objectives that may have security implications:

- availability and correct functionality of service subscription, activation and deactivation,
- availability and correct functionality of the ATM network services,
- correct and verifiable billing,
- data integrity and data confidentiality / privacy, and
- capability to use a service anonymously.

2.2. Operator Objectives

The goal of network operators and service providers is to make good revenue by operating an ATM network. This goal implies maximum revenue for supplying network services and a minimum of expenditures due to unauthorized use of network services.

The following list gives examples of objectives for achieving this goal. These objectives may have security implications:

- availability and correct functionality of the ATM network services,
- availability and correct functionality of the ATM network management,
- correct and verifiable billing, above all no possibility of fraud,

- non-repudiation for all used ATM network services and for all management activities,
- preservation of reputation (above all preservation of customers' and investors' trust),
- accountability for all activities, and
- data integrity and data confidentiality / privacy.

2.3. Public Community Objectives

The goal of the public communities / authorities is to guarantee the following example objectives which may have security implications:

- availability and correct functionality of the ATM network services, and
- data confidentiality / privacy.

2.4. Main Security Objectives

The objectives listed above can be expressed by one or by a combination of the following main security objectives:

- **Confidentiality:**
  Confidentiality of stored and transferred information,
- **Data Integrity:**
  Protection of stored and transferred information,
- **Accountability:**
  Accountability for all ATM network service invocations and for all ATM network management activities; any entity should be responsible for any actions initiated, and/or
- **Availability:**
  All legitimate entities should experience correct access to ATM facilities.

3. Generic Threats

A threat is a potential violation of a security objective. Three kinds of threats may be distinguished:

ñ An accidental threat where the origin of the threat does not involve any malicious intent.

ñ An administrative threat where the threat arises from a lack of administration of security.

ñ Intentional threats where the threat involves a malicious entity which may attack either the communication itself or network resources.

Within this standardization work, accidental and administrative threats may be taken into account as long as their consequences are the same as intentional threats.

The following intentional threats should be considered in a threat analysis of an ATM network:

- **Masquerade (“spoofing”):**
  The pretense by an entity to be a different entity.
- **Eavesdropping:**
  A breach of confidentiality by monitoring communication.
- **Unauthorized access:**
  An entity attempts to access data in violation to the security policy in force.
- **Loss or corruption of information:**
  The integrity of data transferred is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay.
- **Repudiation:**
  An entity involved in a communication exchange subsequently denies the fact.
- **Forgery:**
  An entity fabricates information and claims that such information was received from another entity or sent to another entity.
- **Denial of Service:**
  This occurs when an entity fails to perform its function or prevents other entities from performing their functions. This threat may include denial of access to ATM services and denial of communication by flooding the ATM network/component. In a shared network, this threat can be recognized as a fabrication of extra traffic that floods the network, preventing others from using the network or delaying the traffic of others.

Table 2 maps the generic threats to the security objectives. A cross in a field of this table denotes that the threat (e.g. “masquerade”) endangers the respective security objective (e.g. “confidentiality”).The concrete assessment of these threats, i.e. their probability and their potential impact is outside the scope of ATM Forum Standardization, as it depends on the concrete network instance and is therefore highly network (provider) specific.

Main Security Objectives	Generic Threats						
	Masque-rade	Eaves-dropping	Un-authorized Access	Loss or Corruption of (transferred) Information	Repudia-tion	Forgery	Denial of Service
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x

Table 2: Mapping of objectives and threats

4. Functional Security Requirements and Security Services

A set of principal functional security requirements can be identified to deal with the generic threats in the previous chapter. The functional requirements stated in this specification are not prioritized since priorities are derived from the individual assessments of the security threats and depend on the respective network scenario.

As a rule of thumb, it can be stated that open network environments require the application of more stringent technical security mechanisms than required in closed network environments. In closed environments, a sufficient level of security may be achieved by organizational means.

Table 3 gives an overview of the principal functional security requirements to counteract the generic security threats. A cross in a field of this table denotes that a specific threat (e.g. “masquerade”) leads to this functional security requirement (e.g. “verification of identities”). Note, that a single threat may lead to more than one principal functional security requirement.

. Generic Threats	Principal Functional Security Requirements								
	Verification of Identities	Controlled Access and Authorization	Protection of confidentiality	Protection of Data Integrity	Strong Accountability	Activity Logging	Alarm Reporting	Audit	Security Recovery / Management of Security 1)
Masquerade	x					x	x	x	x
Eavesdropping		x	x						x
Unauthorized Access	x	x	x			x	x	x	x
Corruption or Loss of (transferred) Information				x			x		x
Repudiation					x	x		x	x
Forgery					x	x		x	x
Denial of Service		x				x	x	x	x

Table 3: Mapping of generic threats and functional security requirements

1) “Security Recovery / Management of Security” is a conditional requirement in the following sense: as long as there appears a cross in the remaining columns of the respective row, “Security Recovery / Management of Security” is a prerequisite to guarantee the (other) principal functional security requirements.

Table 4 gives an overview of the mapping between security requirements and the security services, which guarantee the fulfilling of these requirements. For each security requirement the relevant generic security services are named.
This section only defines a basic list of security services, possible other services (e.g. "detection of denial of service") may be derived from this list.

Functional Security Requirement		Security Service
Verification of Identities		User Authentication Peer Entity Authentication Data Origin Authentication
Controlled Access and Authorization		Access Control
Protection of Confidentiality	Stored Data	Access Control
	Transferred Data	Confidentiality
Protection of Data Integrity	Stored data	Access Control
	Transferred Data	Integrity
Strong Accountability		Non-repudiation
Activity Logging		Security Alarm, Audit Trail and Recovery
Alarm Reporting		Security Alarm, Audit Trail and Recovery
Audit		Security Alarm, Audit Trail and Recovery
Security Recovery / Management of Security		-

Table 4: Mapping of functional security requirements and security services

The following subsections describe the functional security requirements and the corresponding security services in ATM terminology (AF SEC-1 to AF SEC-10). However, for a specific ATM network, the risk assessment for that network will determine which of these functional requirements must be fulfilled, and which corresponding security services must be provided.

The proposed generic security services are derived from [6].

4.1. Verification of Identities

AF SEC-1 The ATM network shall support capabilities to establish and verify the claimed identity of any actor in an ATM network.

Verification of identities is a fundamental security requirement for ATM networks.
Its main purpose is to support other security services and to provide accountability for actions taken.

The following security services should be made available (if necessary) to fulfill this requirement:

- **User Authentication:**
  User authentication delivers corroboration of the identity of the (human) user.
- **Peer Entity Authentication**
  Establishing proof of the identity of the peer entity at one particular moment in time during a communication relationship.
- **Data Origin Authentication**
  Establishing proof of identity of the peer entity responsible for a specific data unit.

Usage of an authentication service establishes the proof at that particular instant of time. To ensure continued proof of authentication, the authentication service has to be repeated or it has to be linked to another security service.

4.2. Controlled Access and Authorization

AF SEC-2 The ATM network shall support capabilities to ensure that actors are prevented from gaining access to information or resources they are not authorized to access.

The security service to meet this requirement is:

- **Access Control:**
  The access control service provides a means to ensure that (stored) objects are accessed by subjects only in an authorized manner. Objects concerned may be the physical system, the system software, applications and data. The limitations of access to these objects are laid out in access control information, which specifies:
  - the means to determine which entities are authorized to have access to an object,
  - what kind of access is allowed (reading, writing, modifying, creating, deleting).

Granting access to objects requires verification of the identity of the entity trying to gain access. This means that usage of access control is always linked to the usage of an authentication service.

4.3. Protection of Confidentiality

AF SEC-3 The ATM network shall support the capability to keep stored and communicated data confidential.

Protection of confidentiality is needed to protect:

- user related ATM network information, and
- information used by other security services, e.g. cryptographic keys.

The security services that support this requirement are:

- **Access Control (stored data)**
  See AF SEC-2.
- **Confidentiality (communicated data)**
  The confidentiality service provides protection against unauthorized disclosure of exchanged data. The following kinds of confidentiality services can be distinguished:
  - data confidentiality, and
  - connection confidentiality.

4.4. Protection of Data Integrity

AF SEC-4 The ATM network shall support granting the integrity of stored and communicated data.

Protection of data integrity is needed to protect:

- ATM network user related information, and
- information used by other security services.

Security services to support this requirement can be divided in services for the integrity of stored data and services for the integrity of communicated data:

- **Access Control (stored data):**
  See AF SEC-2.
- **Data Integrity (communicated data):**
  The integrity service provides means to ensure the correctness of exchanged data, protecting against modification, deletion, creation (insertion) and replay of exchanged data. The following kinds of integrity services are distinguished:
  - selective field integrity,
  - connection integrity without recovery, and
  - connection integrity with recovery.

4.5. Strong Accountability

AF SEC-5 The ATM network shall support the capability that an entity can not deny the responsibility for any of its performed actions as well as their effects.

Strong accountability requires that any individual actor in an ATM network must hold full responsibility for any of his/her/its actions. In other words, the actor may not repudiate its actions in the ATM network.

The security service to support this requirement is:

- **Non-repudiation:**
  The non-repudiation services provide means to prove that exchange of data actually took place. It comes in two forms:
  - non-repudiation - proof of origin, and
  - non-repudiation - proof of delivery.

4.6. Activity Logging

AF SEC-6 The ATM network shall support the capability to retrieve information about security activities stored in the Network Elements with the possibility of tracing this information to individuals or entities.

This requirement is supported by the following security service:

- **Security Logging**
  For controlling security policies it is necessary to be able to log information about security relevant events that have occurred or security relevant operations that have been performed or attempted,

When such information is retrieved from a log the security administrator must be able to determine whether any records were lost or whether the characteristics of the records stored in the log were modified at any time.

4.7. Alarm Reporting

AF SEC-7 The ATM network shall support the capability to generate alarm notifications about certain adjustable and selective security related events.

This requirement is supported by the following security services:

- **Security Alarm**
  The security alarm notification provides information regarding operational condition and quality of service, pertaining to security.

4.8. Audit

AF SEC-8 The ATM network shall support the capability to analyze and exploit logged data on security relevant events in order to check them on violations of system and network security.

This requirement is supported by the following security services:

- **Security Audit Trail**
  An audit is to be seen as an independent review and examination of system information and activities in order to test for adequacy of system controls, to ensure compliance with the established security policy and operational procedures, to detect breaches in security and to recommend changes in control, policy and procedures.

4.9. Security Recovery, Management of Security

AF SEC-9 The ATM network shall support recovery from successful and attempted breaches on security.

Whenever an attempt to breach security occurs it shall be possible to handle this attempt in a controlled manner, meaning that the attempt shall not result in a severe degradation of ATM network availability.

AF SEC-10 The ATM network shall support capabilities to manage the security services derived from the security requirements listed above.

Security management comprises all activities to establish, maintain and terminate the security aspects of a system. For example, security management includes:

- management of security services
- installation of security mechanisms
- key management (management part)
- establishment of identities, keys, access control information, etc.

The last two requirements (SEC-9 and SEC-10) do not lead to security services but are requirements on the specification of the security services and the necessary infrastructure (e.g., they act on key management or on management of security mechanisms and algorithms). However, these requirements must be fulfilled to guarantee the maintenance of security services. SEC-9 and SEC-10 must be supported by ATM network management (see also [2], [3], and [1]).

5. Plane Specific Interpretation of Functional Security Requirements

The purpose of this chapter is to interpret the functional security requirements of chapter 4 as requirements for plane specific security services. For each security service, requirements for implementing the service within the plane are specified. These implementation requirements include general requirements such as flexibility and quality/strength, as well as plane specific requirements such as supported architectures and service aspects.

5.1. User Plane

5.1.1. Interpretation of AF SEC-1

The ATM user plane shall support capabilities to establish and verify the claimed identity of ATM user plane entities.

Before exchanging data, the initiator may require authentication of the peer entity. The same requirement may come from the recipient of the data.

To deal with identification and authentication, the following security services should be made available within the user plane:

- **Peer Entity Authentication,**
- **Data Origin Authentication.**

Note, that peer entity authentication is a pre-requisite for many other security services such as access control or key distribution.

Human user authentication is not applicable for the user plane since no human entities are visible at the user plane.

Requirements for the peer entity authentication service are:

Flexibility (general requirements)

- The ATM entity authentication infrastructure shall provide an option for unilateral authentication [8].
- The ATM entity authentication infrastructure shall provide an option for mutual authentication [8].
- The ATM authentication infrastructure shall not restrict the number of authentication passes.
- The ATM entity authentication infrastructure shall allow the usage of symmetric as well as asymmetric key techniques.
- The peer entity authentication service shall be defined independently of specific (crypto-) algorithms.

- The ATM entity authentication infrastructure shall provide for the negotiation of algorithms [8] and mechanisms.

Quality/strength (general requirements)

- The ATM entity authentication infrastructure shall provide cryptographic strength (i.e. be based on cryptographic keys) and protocol features which resist attacks, e.g., replay.

Supported architectures (user plane specific requirements)

- The ATM entity authentication infrastructure shall support authentication of any network element.

Entity authentication as a support service

- The ATM entity authentication infrastructure shall allow for inclusion of (authentic and/or confidential) service specific parameters in the protocol flows [8] (e.g., as foreseen within ISO/IEC-9798 [9]).

Requirements for data origin authentication are presented together with integrity requirements in chapter 5.1.4.

5.1.2. Interpretation of AF SEC-2

The ATM user plane shall support capabilities to ensure that entities are prevented from gaining access to information and resources that they are not authorized to access.

The security service to meet this requirement is:

- **Access Control.**

Granting access to information or resources requires checking the identity of the entity trying to gain access. Hence, the access control service may require the usage of the peer entity authentication service (see 5.1.1).

Note, that access control is implementation specific, and details of implementation are outside the scope of this document. However, an access control infrastructure must support necessary communication between implementations.

Requirements for the access control service are:

Flexibility (general requirements)

- The access control service infrastructure shall support rule-based as well as label-based access control mechanisms.
- ATM access control mechanisms shall provide an option for user-specified access control during connection establishment [8].
- ATM access control mechanisms shall provide an option for enterprise-specified access control during connection establishment [8].

- ATM access control mechanisms shall provide an option for user defined access control attributes to be used with user defined access control rules [8].
- ATM access control mechanisms shall have the option of transporting user defined access control attributes with integrity [8].
- The access control information element shall allow multiple access control algorithms to be used concurrently [8].
- The access control infrastructure shall allow the possibility of mechanism and algorithm discovery.

5.1.3. Interpretation of AF SEC-3

The ATM user plane shall support the capability to keep communicated data confidential.

For the user plane, only confidentiality of communicated data is applicable.

The security service to meet this requirement is:

- **Confidentiality.**

Requirements for the confidentiality service are:

Service Aspects

- The ATM confidentiality infrastructure shall support data confidentiality.
- The ATM confidentiality infrastructure shall support mechanisms for key update and synchronization [8].
- The ATM data confidentiality infrastructure shall support key agile and single key scenarios [8].

Flexibility (general requirements)

- The confidentiality service shall be defined independently of specific (crypto-) algorithms.
- The ATM data confidentiality infrastructure shall support mechanisms for the basic negotiation of options [8].

Quality/strength (general requirements)

- The confidentiality service shall use cryptographically supported mechanisms.

Supported architectures (user plane specific requirements)

- The ATM data confidentiality infrastructure shall support any network element.

5.1.4. Interpretation of AF SEC-4

The ATM user plane shall support granting the integrity of communicated data.

For the user plane, only integrity of communicated data is applicable. The protection of data integrity also provides authentication of the data's origin since the cryptographic mechanisms used to provide data integrity implies knowledge of the data originator's identity.

The security service to meet this requirement is:

- **Data Integrity / Data Origin Authentication.**

Requirements for the data origin authentication and integrity service are:

Service aspects

- The data origin authentication / integrity service shall support options for
  - selective field integrity,
  - connection integrity without recovery,
  - connection integrity with recovery.
- The ATM data integrity infrastructure shall support key agile and single key scenarios [8].
- The ATM data integrity infrastructure shall support mechanisms for key update and synchronization [8].

Quality/strength (general requirements)

- The data origin authentication / integrity service shall detect deletion, insertion and modification of any part of the user data.
- The integrity service shall detect insertion and deletion of ATM cells as well as reordering and replay.
- The integrity service shall use cryptographically supported mechanisms.

Flexibility

- The integrity service shall be defined independently of the used key techniques (symmetric or asymmetric).
- The integrity service shall be defined independently of specific (crypto-) algorithms.
- The ATM data integrity infrastructure shall support mechanisms for the negotiation of options [8].

Supported architectures (user plane specific requirements)

- The ATM data integrity infrastructure shall support any network element.

5.1.5. Interpretation of AF SEC-5

The ATM user plane shall support the capability that an entity can not deny the responsibility for any of its performed actions as well as their effects.

For the content of transmitted data, non-repudiation is application specific. However, for billing aspects, the following service may become relevant in the future:

- **Non-repudiation of Delivery.**

5.1.6. Interpretation of AF SEC-6 to AF SEC-10

The requirements AF SEC-6 to AF SEC-10 refer to management aspects and are plane independent.

The following requirement holds:

All security services shall inform about all security relevant events (e.g., failed authentication attempts, recognized integrity violations, ...).

5.2. Control Plane

5.2.1. Interpretation of AF SEC-1

The ATM control plane shall support capabilities to establish and verify the claimed identity of ATM control plane entities.

To deal with identification and authentication the following security services should be made available within the control plane:

- **Peer Entity Authentication, and**
- **Data Origin Authentication.**

Note, that peer entity authentication is a pre-requisite for many other security services such as access control or key distribution.

Human user authentication is not applicable for the control plane since no human entities are visible at the control plane.

Requirements for the **control plane** peer entity authentication service are:

Flexibility

- The ATM control plane entity authentication infrastructure shall provide an option for unilateral authentication [8].
- The ATM control plane entity authentication infrastructure shall provide an option for mutual authentication [8].
- The ATM control plane authentication infrastructure shall not restrict the number of authentication passes.
- The ATM control plane authentication infrastructure shall support multiple authentication algorithms [8].

Quality/strength

- The ATM control plane entity authentication infrastructure shall provide cryptographic strength.

Supported architectures

- The ATM control plane entity authentication infrastructure shall support authentication of any network element, i.e.:
    - User-Network signaling:
        - Mutual authentication of user and network entities,
        - Unilateral authentication of user entity by network.
    - Network-Network signaling:
        - Mutual or unilateral authentication.
    - Network-Network routing messages:
        - Mutual or unilateral authentication.

Entity authentication as a support service

- The ATM entity authentication infrastructure shall allow for inclusion of (authentic and/or confidential) service specific parameters in the protocol flows [8] (e.g., as foreseen within ISO/IEC-9798 [9]).

Requirements for control plane data origin authentication are presented with integrity requirements in section 5.2.4.

5.2.2. Interpretation of AF SEC-2

- TBD. in phase 2

5.2.3. Interpretation of AF SEC-3

- TBD. in phase 2

5.2.4. Interpretation of AF SEC-4

The ATM control plane shall support granting the integrity of communicated control data.

The security service to meet this requirement is:

- **Data Integrity.**

The protection of data integrity also provides authentication of the data's origin since the cryptographic mechanisms used to provide data integrity implies knowledge of the data originator's identity.

Requirements for the **control plane** data origin authentication and integrity service:

Service aspects

- The control data origin authentication / integrity service shall support options for selective field integrity.
- The ATM control plane data origin authentication / integrity infrastructure shall support key agile and single key scenarios.

Quality/strength

- The control data origin authentication / integrity service shall detect unauthorized deletion, insertion and modification of any part of the control data.
- The control plane integrity service shall detect insertion and deletion of ATM cells as well as reordering and replay.
- The control plane data origin authentication / integrity service shall use cryptographically supported mechanisms.

Flexibility

- The control plane data origin authentication / integrity service shall be defined independently of the used key techniques (symmetric or asymmetric).
- The data origin authentication / integrity service shall be defined independently of specific (crypto-) algorithms.

Supported architectures

- The ATM control data data origin authentication / integrity infrastructure shall support any network element, i.e.:

- User-Network signaling:
    - Integrity of signaling messages.
- Network-Network signaling:
    - Integrity of signaling messages.
- Network-Network routing messages:
    - Integrity of routing messages.

5.2.5. Interpretation of AF SEC-5

The ATM control plane shall support the capability that an entity can not deny the responsibility for performed actions as well as their effects.

The service

- **Non-repudiation of Delivery**

may become relevant in the future if, e.g., billing requires use of signaling information.

5.2.6. Interpretation of AF SEC-6 to AF SEC-10

The requirements AF SEC-6 to AF SEC-10 refer to management aspects and are plane independent.

The following requirement holds:

All (control plane) security services shall report all security relevant events (e.g. failed authentication attempts, recognized integrity violations, ...).

6. Requirements for Support Services

Support services are required to assist plane specific security services. The following support services are addressed in phase 1:

- security message exchange protocols and basic negotiation,
- security messaging in the control plane,
- security messaging in the user plane,
- key exchange,
- session key update, and
- certificates.

Requirements on quality, strength, and flexibility of a specific support service result from the requirements of the plane specific security service which use this support service. Therefore, in principle all requirements of the supported service apply as well to the support services. Especially the quality and strength of the supported service must not be weakened by the applied support service.

Since most of the ATM Forum security services are optional, many combinations of security services and mechanisms may occur according to a distinct security policy. The defined support services have to be flexible enough in order to support a wide range of scenarios and possible architectures; applicable and non applicable scenarios for the use of a security support service have to be identified.

7. References

[1] ATM Forum Technical Committee, str-sec-01.00 ATM Security Specification 1.0; December, 1997.

[2] ATM Forum/96-1689; “Input for baseline material on security management (M4 NE view)”; December, 1996.

[3] ATM Forum/97-0067; “Proposed work on management capabilities for ATM security”; February, 1997.

[4] ETSI DTR/NA-61202; IN Interconnect Business Requirements; 1996.

[5] ETSI DTR/NA-043208; Telecommunication Management Network (TMN); Introduction to Standardizing Security for TMN; Sept. 1996.

[6] ISO 7498/2; Information Processing Systems – Open System Interconnection Reference Model – Part 2: Security Architecture; 1988.

[7] ITU-T Draft Recommendation M.3sec; "TMN Security Overview or Framework" (to be decided); Nov. 1996.

[8] ATM Forum Technical Committee, ATM Forum RTD-SECURITY-01.00; “Requirements for phase I Security Specification”; December, 1996.

[9] ISO/IEC 9798-1; Information Technology−Security techniques−Entity authentication-Part 1: General model; 1996.