CEC TEN-T ATM Task UK/96/94

ACCESS

ATN Compliant Communications

European Strategy Study

Security Mechanisms in the European ATN Network

Document Reference : ACCESS/STNA/222/WPR/036

Author : C.PETIT

Revision Number : Issue 1.0

Date : 23 October 1998

Filename : S036i1-0.doc

DOCUMENT CONTROL LOG

Revision Number	Date	Description of Change
Draft 0.1	28 July 1998	Initial revision proposing a structure for the document
Draft 0.2	1st September 1998	Current draft revision incorporating DFS input (DFSIN222.doc)
Issue 1.0	23 October 1998	Proposed final version (updating Draft 0.2 with comments received before 23 October 1998; executive summary, appendices B and C are added)

COPYRIGHT STATEMENT

EXECUTIVE SUMMARY

This document outlines general security precautions for the target ATN European network. The proposed precautions aim at protecting the network from the threats whose occurrence and/or potential damages are thought to justify specific countermeasures.

The retained threats induce general security requirements falling into the system security area (e.g., protection of the ATN resources themselves) or the telecommunication area (e.g., protection of the information exchanged on the network). Similarly the consequent precautions range from purely physical protection measures to procedural provisions or technical mechanisms implemented in ATN systems.

As most technical measures use cryptographic techniques (mainly based on a public key cryptosystem) which are not fully standardized in current draft ATNP material, the protection of the communications will not be achieved in the initial European ATN with CNS/ATM 1 implementations: once the relevant ATNP recommendations are finalized and the consequent implementations are available, it will be possible to operate the complete set of precautions.

The first part of the document makes of review of existing ATNP material and existing practices in the area of network security. It presents the threats and the high-level security requirements to be consequently taken into consideration for the security policy applicable to the European ATN and derives a set of general precautions deemed appropriate to that policy.

A second part of the document develops the various precautions to be applied to the target European ATN. It particularly highlights the necessity to develop an ATN public key infrastructure (PKI). That infrastructure is required for the correct operation of the ATN security mechanisms that are essentially aimed at ensuring the integrity and the authentication of the messages exchanged on the network. The implementation of an ATN PKI raises important technical and institutional issues which have not been clearly addressed by the ATN community so far (e.g., availability of an ATN X.500 repository, establishment of ATN Certification Authorities, etc.).

TABLE OF CONTENTS

FIGURES

1. Introduction

1.1 Scope

The 'ATN Compliant Communications European Strategy Study' (ACCESS) project that is being run under the European Commission's programme for financial aid in the field of Trans-European Transport Network (TEN-T), ATM Task UK/96/94, aims at defining the initial architecture of the ATN in EUROPE (i.e. selection of the initial applications, definitions of the initial network topology, definition of the routing organisations and of the addressing plan, etc.), and will propose initial solutions as regards to the security, safety/certification, network management, institutional, and other issues as well as a transition plan.

Part 1 of the ACCESS project focuses on ATN Implementation with the objectives of proposing a network architecture, solutions for network implementation issues and a plan for transition from the existing network infrastructure to the proposed ATN infrastructure.

Part 2 of the ACCESS project covers the ATSMHS Interoperability/Validation testing.

ACCESS Part 1 has been divided into three sequential sub-parts:

- the first sub-phase (April 1997 - April 1998) has defined the proposed **Network Architecture**, i.e. the main elements of the target ACCESS ATN. It has resulted in the production of Interim Deliverable 1,

- the second sub-phase (March 1998 - October 1998) proposes solutions for **Network Implementation Issues** related to the target ACCESS ATN but not studied or not completed during the first sub-phase (e.g., security, certification, etc.). It will result in Interim Deliverable 2,

- the final sub-phase (August 1998 - October 1998) will propose a **Transition Plan** from the existing network infrastructures to the target ACCESS ATN infrastructure and will define the initial ACCESS ATN. It will result in Interim Deliverable 3.

This report presents the outcomes of the **Work Package 222** (entitled " Security Mechanisms in the European ATN network ") and represents one part of ACCESS Interim Deliverable 2.

1.2 Geographical Area and Timeframe considered by the ACCESS Project

The geographical area considered in ACCESS consists of the following countries: UK, Ireland, Benelux, Germany, France, Italy, Spain and Portugal. These States were chosen for the following reasons:

- **They have a direct connection to the CFMU and/or are involved in the control of North Atlantic traffic.** States connected directly to the CFMU - in 1997 - were selected because this enables the major ground/ground data flows in Europe to be included in the study. North Atlantic Region States were selected, as this Region is likely to provide the first operational implementation of ATN services.

- **The study is representative of both Oceanic and Continental ATC**. Including the NAT Region and European States allows routing and architecture issues between boundary Regions to be studied.

With respect to the considered timeframe, it is assumed that an initial European ATN will be deployed and be operationally used during the period 2000-2005. This initial European ATN is considered in the time as the first brick to a global and mature target European ATN that would answer the most of ground-ground and air/ground ATN communication requirements currently identified. This target

European ATN is assumed to be deployed in years 2005-2010 where new data link services and new communication networks will be set in operation and additional ground facilities will be equipped.

The initial ATN of year 2005 must consist of the first elements of an expandable ATN infrastructure that will actually allow, in some further implementation steps, the building of the target European ATN of the year 2010. The initial European ATN is therefore viewed as a transition step toward the target infrastructure.

As a practical approach for the definition of the initial European ATN, it is considered that ACCESS must first focus on the definition of the target European ATN and that the initial implementation will be derived in the scope of the ACCESS transition planning Work Package (WP240).

Following this approach, the scope of this document has not been limited to the initial period of the ATN deployment and proposes security mechanisms for the target European ATN.

The ACCESS Work Package 240 will later on in the ACCESS project define more precisely what the initial European ATN could be and how security issues could be dealt with in the initial and in the transition phases.

1.3 Purpose of the Document

As per definition the purpose of this work package is to document the security precautions to be considered in the European ATN and to propose the security mechanisms that will be deemed appropriate in this context.

This task is mainly based on the WP208 results (Interim Deliverable 1), which proposes a network architecture for the European ATN. It is also related to WP224 (Institutional Issues), since the use of some security mechanisms may be constrained by the national legislation constraints of the various countries of the ACCESS geographic area, and to WP227 (Systems Management), as security mechanisms may raise specific requirements in terms of systems management.

1.4 Document Structure

This document is structured as follows:

- Chapter 1 presents the scope, structure and purpose of the document,
- Chapter 2 presents background information on security issues, both general and ATN-related. It particularly presents the various areas covered by security issues, the definition of different security concepts and terms and provides with a overview of existing material with regards to security, either general, ATSO- or ATN-related. As an informational material it also gives an overview of the approach of security problems and the solutions used in the Internet community,
- Chapter 3 proposes the security requirements to be taken into account for the ACCESS ATN European network (the security mechanisms proposed in the following sections of the document will be based on those requirements) and it consequently presents the general precautions retained to that purpose. It then proposes a two-step approach, mainly based on feasability constraints, which tends to identify two different sets of precautions: an initial one, applicable to the implementation of the initial ATN European network and a full one, applicable to the target network,
- Chapter 4 proposes security provisions to be applied to the target European ATN network. It particularly highlights the constraints and requirements, both technical and non-technical, raised by the proposed mechanisms,

- Chapter 5 gives an overview of non-technical issues required by the implementation of a security policy throughout the European ATN network (e.g., organisational, institutional and co-ordination aspects),

- Chapter 6 is the conclusion of the document.

1.5 References

ACCESS Reference	Title
[A208]	ACCESS Interim Deliverable 1 - Proposed Network Architecture of the European ATN
[A203]	ACCESS - Definition of the European Routing Architecture
[A206]	ACCESS - Definition of Addressing Plan
[A224]	ACCESS – ATN Institutional Issues
[A227]	ACCESS – Systems Management in the European ATN Network
[SARP-C]	WG1/WP11-15A - ATN Security Provisions - Core ATN SARPs Version 2.0 Draft Text
[SARP-SV1]	WG1/WP11-14A - ATN Security Provisions - SV-1 Version 2.0 Draft Text
[GUID]	Proposed Version 0.2 Draft ATN Security Guidance Material
[WG1/6-10]	WG1/WP6-10 - Summary of the Security Issues, Status and Recommendations for ATN SARPs
[WG1/6-11]	WG1/WP6-11 - Overall Security Concept
[WG1/9-5]	WG1/WP9-5 - Security Strategy for the ATN
[WG2/450]	WG2/WP450 - IDRP Security
[WG2/447]	WG2/WP447 - Alternatives for BIS Access to X.509 Certificates
[WG3/UPP]	WG3/WP?? - ATN Upper Layers Security
[WG1/FR]	WG1/SG2/WP?? - Impact of French Legislation on ATN Security
[WG1/2-4]	WG1/SG2/WP2-4 - Digital Signature Certification Authorities for ATN
[WG1/2-5]	WG1/SG2/WP2-5 - US Encryption Export and Key Recovery Policy and their Impact on Security Strategy for the ATN
[WG1/2-6]	WG1/SG2/WP2-6 - Additional Requirements for Security for the ATN
[WG1/2-7]	WG1/SG2/WP2-7 - Comments on Security Strategy for the ATN
[NSM-TF]	EATCHIP NSM-TF Security Policy Version 0.5

2. Background

2.1 Introduction

The objective of this paper is two-fold:

- to identify the security requirements to be considered for the ACCESS ATN European network,
- to propose security mechanisms aimed at fulfilling the identified requirements.

Prior to any security requirement identification for the ACCESS ATN European network, it is necessary to define what security is and how security issues are generally dealt with in somehow similar networking environments.

The first part of this chapter aims therefore at presenting security issues and global approaches usually retained to handle them. It will thus provide with some concepts and definitions that will be used in the following sections of the document.

The second part of this chapter presents an overview of existing material on security, including normative references including ATN specifications and guidance material as well as documents produced on security by European ATSOs or other ATM-related working groups.

Security requirements to be taken into consideration for the ATN European network will be derived in Chapter 3 from that material when applicable and from the application of the previously described approach to the European ATN.

2.2 General

2.2.1 Security concepts

This section proposes a general presentation of the security concept by presenting the main issues usually raised when security is applied to networking environments. There are also normative definitions of security issues, especially in the telecommunications community. However this section is intended to give an overview of security issues rather than an exhaustive presentation of the generic normative models and definitions with respect to security, which can be found in the previously referenced documents.

When applied to information systems in general, security may be regarded with respect to three high-level objectives:

- confidentiality: security is often reduced to confidentiality (e.g., protection of critical information from non-authorized users), which may be important in certain contexts but not necessarily the most important aspect (as it is effectively for the ATN community - see further). Confidentiality ensures that protected information is not revealed to unauthorized entities.
- integrity: integrity ensures that information are not modified or manipulated by unauthorized entities. Integrity usually encompasses authentication, which ensures the identity of entities modifying and/or exchanging information.
- availability: information must be made available to its authorized users. It is an important aspect of security which is often disregarded (a secure system must above all remain available to its users. As an example, denial of service attacks specifically targets service availability.

Security measures that are applicable to information systems in their whole can be specifically developed along the various components of the information systems. They fall into the following categories:

- system security: security measures should be applied to the individual systems making up the information systems (e.g., the end systems themselves). They mainly aim at protecting the specific functions run by the considered systems and the stored information, by setting up access control and system administration procedures and mechanisms (which do include physical protection measures),

- telecommunication security: telecommunications between the systems should be protected from different threats. Security measures in the communication area are focused on the protection of the information carried in the network, e.g. ensuring the authentication, the integrity and the confidentiality of the messages exchanged between the communicating parties.

Security requirements to be taken into account in the implementation of the European ATN network will be developed in the following sections of the document. However, even if communication security is the most straightforward area to be considered for the European ATN network due to its very nature, system security considerations cannot be left aside since the very function of the network could be impaired by system security violations. More generally, it will be necessary to define the object of the security issues in order to identify the applicable threats.

The identification of security requirements uses some generic terms, which are presented hereunder:

- attacker: any event or individual able to impair the protected system. An attacker can be characterized by its ability to harm the system and the associated probability of its attacks. Attackers can be either humans or natural phenomena. Human attackers may be individuals or groups of people characterized by additional characteristics, e.g. their motivation,

- vulnerability: a vulnerability is a potential breach or flaw in the protected system, which may be used by attackers to harm the system. Security measures aim at reducing the vulnerabilities of the protected system or the probability they could be used to violate the system rather than completely eliminating these vulnerabilities, which is not really possible. There are different types of vulnerabilities :

    - physical vulnerabilities (e.g., rooms homing the protected systems can be violated by non-authorized people),

    - natural vulnerabilities (e.g., fire, earthquakes, electric supply shortages, etc.),

    - hardware and software vulnerabilities (e.g., software bugs),

    - telecommunication vulnerabilities (e.g., message interception),

    - human vulnerabilities (e.g., system or network administrators).

- threat: a threat is a potential security violation. It can be turned into an actual security violation (or attack) when an attacker effectively uses vulnerability of the system incidentally (e.g., electric supply failure) or to achieve purposefully its objectives (e.g., human intruder attacking the system). A threat cannot result in an attack without an attacker. The probability a threat turns out to be a real attack and the potential damages that could be consequently caused to the system can be measured with a risk analysis. Threats can be classified into three general categories :

    - natural or physical threats,

    - non intentional (human) threats (e.g., misuse of a procedure by an authorized user which turns into an end system system crash),

    - intentional (human) threats that may come from either internal or external people (security violation audits show that a high percentage of security violations are realized by authorized people).

- countermeasures: security countermeasures (often abbreviated as security measures) are procedures and mechanisms used to protect the system. They are usually built according to the identified vulnerabilities and threats. They are aimed at reducing the vulnerabilities, the probability a vulnerability be used by an attack and the potential damages induced by the attacks. The total and complete protection of a system is generally not retained as a realistic objective, either technically or economically (see next section).

A security policy can be defined as a set of agreed high-level security objectives and principles. A security program can be defined as an implementation of the security policy by the operation of security measures encompassing technical and non-technical means (security mechanisms, procedures, organizational aspects, etc.). A security architecture can be viewed as a set of specific security mechanisms and components used by the security program.

Any component or service of the protected system can be characterized by a security level which is based on the consequences of possible threats affecting it (misuse, malfunction, alteration, etc.).

2.2.2 Global approach to security

Security considerations encompass many areas and cannot be limited to technical considerations: a comprehensive investigation of the need for security is usually retained as a necessary task to ensure the appropriateness of the security measures selected to protect a given system.

The first task is the definition of the subject of the study, i.e. the precise definition of the system to be protected, by answering the question: "what must be protected ?"

This question usually requires the prior identification of the strategic functions or services of the system and the resulting critical informations and data flows, thus allowing to define the limits of the system with respect to security.

Once the system has been characterized, the second step is generally the identification of the system vulnerabilities and the related threats, which then should be prioritized according to the associated risks (threat occurrence and potential induced damages). This step includes the identification of the possible attackers. It should also lead to the definition of objectives with respect to the identified risks (each considered threat is measured as a risk, a level of acceptability can be defined for each of these risks).

The third step consists in defining security countermeasures aimed at reducing the identified vulnerabilities and threats. Though completion of this step should have reduced the risks induced by the previously identified threats, it may be necessary to make iterations to step two so as to finally meet the target security objectives (i.e., reducing the associated risks to an acceptable level).

It does not appear to be realistic to set objectives of complete and total protection of the system for various reasons:

- attackers, vulnerabilities, threats, as well as the systems themselves continuously evolve, so that it is rather unrealistic to ensure the system will stay completely protected at any given time,

- security measures are based on assumptions which are sometimes difficult to ensure : it is for example very difficult to ensure any assumption based on human factors,

- security measures have a cost and often induce constraints which may be deemed inappropriate for various reasons, so that any proposed security mechanism or procedure has to be measured against its induced costs and constraints before being effectively retained for the protection of the system,

- etc.

That is why any realistic security policy will rather focus on a predefined set of objectives (i.e., the protection of the identified critical elements) and provide the means for continuously measuring its ability to fulfil its mission (security audit trail).

2.3 Existing material

2.3.1 ISO Standards

The main ISO standards specifically addressing security issues, which are relevant for most referenced ATNP documents, are listed hereunder:

- ISO/IEC 7498-2 : Basic Reference Model – Part 2: Security Architecture
- ISO/IEC 9594-8 / ITU-T Rec. X.509 : The Directory: Authentication Framework
- ISO/IEC 10745 : Upper layers security model
- ISO/IEC 11586-1 : Generic upper layers security: Overview, models and notation
- ISO/IEC 11586-2 : Generic upper layers security: Security Exchange Service Element service definition
- ISO/IEC 11586-3 : Generic upper layers security: Security Exchange Service Element protocol definition
- ISO/IEC 11586-4 : Generic upper layers security: Protecting transfer syntax specification
- ISO/IEC 10181-7 : Security Framework for Open Systems: Security Audit Framework
- ISO/IEC 10164-7 : System Management: Security alarm reporting function

2.3.2 ATN Material

2.3.2.1 ATNP Activities on Security

The ATNP is currently working on the specification of security provisions for the ATN. ATNP security provisions are not part of CNS/ATM 1 specifications: they are currently draft materials that should be fully standardized with CNS/ATM 2 specifications.

Ongoing ATNP activities on security are carried out by the various ATNP workgroups as summarized below:

- WG1/SG2 (Security Subgroup of WG1) is responsible for developing the system level requirements for security within the ATN and ensuring the co-ordination between the security provisions defined across the SARPS sub-volumes by the various ATNP workgroups. Security provisions for the Core and Sub-Volume 1 of the ATN SARPs as well as Guidance Material including the concept of operations for ATN security should be provided by WG1/SG2,
- WG2 is responsible for developing security provisions for the internet communication service consistent with WG1 material, which should lead to appropriate enhancements of Sub-Volume 5 of the SARPs. In particular WG2 is currently investigating the addition of Type 2 (strong) authentication for IDRP routing exchanges (IDRP authentication),
- the various subgroups of WG3 are responsible for the incorporation of security provisions in their respective specification areas. The main activities of the various WG3 subgroups are described hereafter:

- WG3/SG1 is developing the security provisions to be incorporated in the (selection of MHS security elements of service to offer a suitable protection against identified threats to the AMHS),

- WG3/SG3 is developing the security provisions to be incorporated in the ATN Upper Layers (ATN Upper Layers Security based on the use of a Secure Dialogue Service).

2.3.2.2 ATNP Specifications and Guidance Material

The main relevant ATNP documents regarding security are listed in the following table. The list reflects the collected documents taken into consideration and includes draft SARPs, Guidance Material as well as various WG working papers.

Type	ACCESS Reference	Title
Draft SARPs	[SARP-C]	ATN Security Provisions - Core ATN SARPs Version 2.0 Draft Text
Draft SARPs	[SARP-SV1]	ATN Security Provisions - SV-1 Version 2.0 Draft Text
Draft Guidance	[GUID]	Proposed Version 0.2 Draft ATN Security Guidance Material
Working Paper	[WG1/6-10]	Summary of the Security Issues, Status and Recommendations for ATN SARPs
Working Paper	[WG1/6-11]	Overall Security Concept
Working Paper	[WG1/9-5] 30 June-3 July 1997	Security Strategy for the ATN
Working Paper	[WG2/450] June 8, 1998	IDRP Security
Working Paper	[WG2/447] March 16, 1998	Alternatives for BIS Access to X.509 Certificates
Working Paper	[WG3/UPP] June 29 - July 3 1998	ATN Upper Layers Security
Working Paper	[WG1/FR]	Impact of French Legislation on ATN Security
Working Paper	[WG1/2-4]	Digital Signature Certification Authorities for ATN
Working Paper	[WG1/2-5]	U.S. Encryption Export and Key Recovery Policy and their Impact on Security Strategy for the ATN
Working Paper	[WG1/2-6]	Additional Requirements for Security for the ATN
Working Paper	[WG1/2-7]	Comments on Security Strategy for the ATN

Table 1 : ATNP material

2.3.2.3 Overview of WG1 Draft SARPs

This section only aims at giving a brief overview of the security provisions proposed for the Core and SV-1 SARPs.

The draft text of [SARP-C] recommends that security provisions shall be based on a combination of technical provisions as well as physical and/or procedural provisions that are implemented on a local/regional basis:

- physical provisions should be used to protect ATN ES, IS, network managers and subnetworks (restricted physical access, restricted user access to the resources, etc.),
- technical provisions shall be based on the use of strong authentication services:
  - the security architecture shall be based on ISO 7498-2 and shall use Public Key Cryptography[1] for authentication based on ISO 9594-8. This architecture sets a scalable algorithm-independent authentication framework allowing a wide range of security services (authentication, message encryption, etc.) through the use of security keys and digital signatures,
  - secured dialogues using authentication services for ATS communication exchanges shall be provided by the ATN upper layer communications services based on ISO 11586,
  - secured exchanges of routing information shall be ensured using authentication services at the ATN internetwork layer.

The draft text of [SARP-SV1] describes the ATN Security Strategy whose main objective is to satisfy operational requirements for secured communication services while ensuring backward compatibility with prior ATN implementations. It consequently specifies the ATN Security Architecture by defining:

- the security framework based on public key cryptosystems, thus allowing the ATN upper layer communication services to provide secured information exchanges,
- recommendations for key management and distribution, including certificate and Certification Authority[2] issues (e.g., by defining what entities could act as CAs in the ATN environment),
- the role of CM and CPDLC within the ATN Security Architecture (e.g., if CM supports security mechanisms, it can provide the mechanisms for supporting the distribution of security-related

---

[1]In conventional cryptographic systems the secret key used to encipher information by the originator of a secret message (using a given enciphering algorithm) is the same as that used to decipher the message by the legitimate recipient. In public key cryptosystems however, keys come in pairs: one is used for enciphering data, the other is used for deciphering the previously enciphered data. One of the keys is publicly known (the public key); conversely the complementary key (the private key) is only known by the party whose identity is associated to the key pair. The effectiveness of public key cryptosystems relies on the secrecy (non-disclosure) of the private keys.

[2]The key pair, made of the public key and the corresponding private key, must be generated by either the key holder (i.e., the user itself) or by a "trusted" authority, which must ensure by strict procedures and controls that the private key is only known to the key holder and potentially to the trusted authority if it issued the key pair. A certificate is a publicly available information associating the public key and the user it describes (i.e., the key holder), generated by a "trusted" authority (i.e., the Certificate Authority) which guarantees the validity of the certificate information to the potential users of the certificate (i.e., the communicating parties). A CA may also be a trusted authority responsible for the generation of key pairs.

information during the logon phase between airborne and ground-based ATS air-ground applications),

- the security provisions within ATN systems:

  - ISs: authentication of routing information exchanges shall be based on digital signatures. Exchanges between air-ground and ground BISs and from airborne BISs to air-ground BISs shall be authenticated; conversely there is no requirement for authentication from air-ground BISs to airborne BISs,

  - ESs: ATN ESs providing secured services shall support the security provisions of the upper layer communication services (Secured Dialogue Element) and of the hosted air-ground or ground applications. The secured services provided by the dialogue function of the ATN upper layers support five different security levels, which shall be accordingly specified by the user application at the dialogue establishment,

  - system managers supporting secured services shall use the ATN security mechanisms for authenticating system management information exchanges,

  - the distribution of certificates makes use of X.500 directory services, which must support the ATN security framework to limit access to ATN users only.

2.3.2.4 Overview of WG1 Draft Guidance

The draft text of [GUID] describes the general security architecture for the ATN and also includes a CONOPS for security within the ATN.

The objectives taken into account by the ATN security policy are reminded in the initial part of the document:

- communication monitoring (data interception) and third party traffic analysis do not constitute threats for the ATN operation[3],

- data link messages as well as network management and routing messages shall conversely be protected against modification, masquerade and replay and consequently require adequate authentication and integrity mechanisms,

- services supporting messages to and from aircrafts shall be protected against denial of service attacks to some level of probability,

- ATN systems (ESs and ISs) shall be protected from unauthorized physical access.

The ATN security architecture overview presented in [GUID] consequently describes the basic security services and mechanisms retained to meet the ATN security policy objectives, i.e. the mechanisms ensuring the integrity of the information exchanges, the authentication of the communicating parties and a discretionary access control to the ATN resources (those mechanisms are based on the X.509-based strong authentication framework, which additionally provides non-repudiation services and allows for the use of confidentiality services though those two services are not part of the current ATN security objectives). The ATN security architecture will then be based on an ATN Public Key Infrastructure, which is the specific underlying structure ATN users need to access in order to make use of public key based security services. The ATN PKI will provide for the creation,

[3] This objective is expressed for ATSC traffic; it is possible that AOC requirements exist whereby communication monitoring and third party traffic analysis constitute threats.

distribution and revocation of certificates[4] (and associated keys) and will supply the mechanisms by which the certificates will be used to provide the security services (certificates are retrieved in order to get the public keys of communicating parties while verifying the contained information can be "trusted").

The ATN security services will provide protection at the application layer and at the network layer (using IDRP authentication), essentially making use of the ATN PKI digital signature mechanism: this mechanism basically ensuring integrity and authentication (and even non repudiation) additionally protect against replay thanks to the inclusion of timestamps in the digitally signed messages.

The ATN PKI is based on the use of certificates, which will require the use of Certificate Authorities for the ATN community and the definition of the responsibilities and the relations between the various ATN CAs (chains of "trust" and consequent cross certification must be built between the various ATN PKI CAs in order to provide the ATN users with usable certificates).

The ATN security CONOPS presented in [GUID] aims at describing how the security features of the ATN may be used to provide an operational capability for authentication of exchanges:

- between peer applications,
- between BISs (routing information exchange),
- network management entities (network management information).

Key architectural assumptions are made in the CONOPS such as a distributed PKI with a hierarchical structure and delegation of authority, distributed key generation functions placed as low as practical in the PKI hierarchy, transaction logging and audit trail functions present in systems at all hierarchy levels and the use of an ATN-wide X.500 directory used for the storage and distribution of security-related information (e.g., certificates and Certificate Revocation Lists).

Several example scenarios are then described: one of these scenarios assumes all interacting ATN applications support security services and an integrated X.500-CM application provides the distribution of security key information between airborne and ground-based applications during the logon phase: the aircraft CM application initially has the public keys of ground CM applications, it then issues a logon request containing the aircraft's digital signature, the ground CM application homes an X.500 DUA able to query the global ATN X.500 directory for retrieving the aircraft's required security information (certificate), the aircraft retrieves the security information of the ground applications of interest from the logon response sent by the ground CM application containing the appropriate security information, ground ATS applications (e.g., CPDLC) desiring to communicate to the aircraft first access the ground CM application to retrieve the aircraft's address and security information (X.509 certificate) and then include their digital signatures to messages sent to the aircraft.

2.3.2.5 Overview of Security-Related ATNP Working Papers

2.3.2.5.1 WG1 Overall Security Concept

[WG1/6-11] is one of the main initial materials that were used for the definition of an ATN security policy and framework.

It essentially provides an initial threat analysis, vulnerability assessment and countermeasures identification for the ATN. The initial identification of 25 threats has been checked against a

[4] A user of a public key must be confident that the public key belongs to the correct remote entity with which the digital signature mechanism will be used. This confidence is obtained through the use of the certificates distributed by the CAs of the ATN PKI, which digitally sign the certificates, thus allowing any user having the public key of a CA to check the validity of the information carried in the retrieved certificate, i.e. the binding between the public key and the associated remote entity.

vulnerability assessment, which has consequently identified the relevant threats to the ATN that need specific countermeasures as part of SARPs or deployment or implementation plans. Those applicable threats are summarized hereunder:

- all CNS/ATM applications are vulnerable to denial of service attacks and require specific countermeasures in the ATN Internet (IDRP Type 2 authentication),
- ATC messages are at risk from modification, replay and masquerade attacks : countermeasures based on authentication (digital signatures) combined with unique sequence numbers as part of each message header (protection against replay),
- MHS messages are at risk from modification and masquerade attacks : specific X.400-based countermeasures are required,
- system management is at risk from modification, replay and masquerade attacks.

The document finally describes possible countermeasures:

- at the ATN internet level (IDRP authentication, alternative routing and routing control),
- at the application level (message authentication, replay protection, X.400-based digital signatures and message sequence numbers),
- for system management messages (3 possible approaches are considered).

2.3.2.5.2 WG1 Security Strategy for the ATN

[WG1/9-5] is one of the main initial documents proposing a high level security framework for the ATN as well as an approach for further developments of the ATN security architecture.

The content of this document is in line with the previously described SARPs and Guidance Material:

- the security policy to be considered is consistent with the one proposed in [GUID],
- the proposed security framework is based on the combination of X.500, X.509 (strong authentication) and the related ITU-T standards,
- the integration of mobile users is provided by an integrated CM/X.500 entity allowing certificate/key exchanges during the logon phase.

2.3.2.5.3 Overview of Relevant WG1/SG2 Working Papers

The document referenced [WG1/6-10] summarizes the issues, status and recommendations relating to security in the ATN: it particularly states that it is not technically feasible to mandate the use of cryptographic checksums (e.g., digital signatures) for protecting data or routing messages in CNS/ATM 1 packages and that it is not practicable to give guidance on institutional issues with CNS/ATM 1 implementations.

The threats to be considered and the security policy are then summarized (they are also described in the related Draft Guidance), the applicable countermeasures falling into one of those two categories: physical security or technical security (by means of cryptographic checksums such as digital signatures). The use of a public key cryptosystem requires a trusted organizational infrastructure for key generation, distribution and management functions, all those issues being usually referred to as institutional issues.

Other relevant WG1/SG2 working papers outline further requirements or specific developments needed for the operation of the ATN security architecture based on a public key cryptosystem:

- the document referenced [WG1/2-4] describes requirements and issues for Certification Authorities for the ATN (e.g., certificates trustworthiness, multiplicity and hierarchy of CAs, etc.) : recommendations are made to develop a standard ATN Certification Practices Statement for ATN CAs and to establish minimum proofing requirements for ATN certificates,

- the document referenced [WG1/2-5] describes U.S. current regulations or laws regarding the export and use of encryption products and their impact on the ATN security strategy : in conclusion use of cryptographic means for digitally signing a message should be legally acceptable,

- the document referenced [WG1/2-6] proposes additional requirements for the ATN security (e.g., the certificate holder may be the aircraft or the aircrew, need for recovery of compromised private keys and thus need for real time access to CAs by signing entities, accommodation of various algorithms and key lengths for planned upgrades, etc.) : in conclusion recommendations are made regarding the need to investigate the certificate holder issues and to conduct additional analysis to determine the minimum amount of data that could be transmitted within an ATN certificate (bandwidth conservation purposes),

- the document referenced [WG1/2-7] proposes an alternative solution for ATN security requirements with respect to the requirements described in [WG1/9-5]: it essentially presents a scenario providing real time validation of digital signature certificates/keys without any requirement for encrypting data (which is subject to usage restrictions) and without any use of X.500 lookups, the use of X.500 being seen by the authors as a potential major vulnerability. The proposed solution is based on both airborne and ground entities already having their private keys and the certificates of the appropriate CAs, the communicating entities' certificates being dynamically retrieved as needed by real time interactions with the appropriate CAs.

The document referenced [WG1/FR] provides a description of French legislation on data communication security and establishes the link between this legislation and applicable European recommendations. It also proposes authentication mechanisms that can be consequently defined in implementing ATN security.

Import, export and use of cryptographic means or services are strictly controlled by French government services. However if those cryptographic means are not used for confidentiality purposes (such as authentication of data origin, data integrity, digital signature, etc.), their usage is free.

As confidentiality is not an ATN requirement, the need for confidential exchanges of information is limited to the communication of private keys to user entities by key generators (usually trusted third parties), since an asymmetric-based cryptosystem is used in the ATN authentication framework. The initial phase of private key exchange could then be minimised (by avoiding key renewing during flight phase) and limited to off-line activity. With respect to governmental concerns, use of confidentiality mechanisms for private key exchanges could be envisaged if the private keys used during the encryption provide protection against most threats while still allowing encrypted messages to be decrypted using more powerful means and if the keys used during the encryption have been provided by an agreed key generator under governmental control.

2.3.2.5.4 WG2 IDRP Security

The proposed solution for IDRP security has been outlined in WG2 Flimsy 4 at the Rio de Janeiro meeting:

- use of digital signatures for all IDRP messages (including IDRP updates),

- authentication of downlink IDRP exchanges only, in the case of airborne BISs,

- airborne BISs will have a pre-loaded private key and certificate (aircraft-based at a minimum),

- air-ground BISs will authenticate airborne BISs based on the corresponding public key retrieved either by X.500 look-up or local caching,

- ground BISs will use authentication based on a pre-loaded private key and on the retrieval of public keys by different possible means (X.500 look-up, local caching, etc.) as a local matter.

The working paper referenced [WG2/450] discusses the implications of the proposed IDRP security solution on the use of ISO10747 provisions (use of Type 2 authentication), the Sub-Volume 5 of the SARPs (e.g., addition of an ATN specific feature for handling the asymmetric authentication used between airborne BISs and air-ground BISs, coexistence between CNS/ATM 1 and CNS/ATM 2 implementations with regards to IDRP authentication, etc.).

In order to get the required security information, ground BISs and air-ground BISs need to retrieve peer BISs's certificates. The working paper referenced [WG2/447] proposes different alternatives for retrieving certificates based on the considered BIS types. The proposed retrieval mechanisms use X.500 look-ups to X.500 servers, system management queries, IDRP-based message passing at the initiation of the BIS-BIS connection or ATN specific CM access protocol (CM making X.500 look-ups to X.500 servers).

2.3.2.5.5 WG3 Upper Layers Security

The document referenced [WG3/UPP] proposes security mechanisms applicable the ATN upper layers while limiting the impact of those mechanisms on the ATN ASEs (most mechanisms will take place under the ASEs).

The objective of those security mechanisms is to ensure the authentication of the communicating entities, the authentication of the data origin (each received message can be associated to the authenticated originating remote entity and has not been modified during its transfer) and finally the non replay of previously exchanged messages (by the provision of timestamping mechanisms).

The proposed mechanisms assume that the involved ATN ASEs rely on the Dialogue service for all security considerations. Though mainly implemented under the ASE level, the proposed mechanisms have potential impacts on the ASEs, e.g. because ASEs using security services shall be at a minimum aware of the requested service level and manage the various possible security-related indications in response to the initial request.

The services provided for secure exchanges between ASEs are optional and can be used by activating Dialogue services using no additional parameters (i.e., using the existing Dialogue service security parameter not used in CNS/ATM 1 implementations). Five kinds of services are provided:

1. Unsecured service: no protection will be envisaged on the dialogue either for its establishment or during the exchanges.

2. Secured dialogue service: authentication will be used for the dialogue establishment and maintenance but not during the exchanges.

3. Forward path secured application dialogue: authentication will be used for the dialogue establishment and maintenance and for all exchanges issued by the dialogue initiator.

4. Return path secured application dialogue: authentication will be used for the dialogue establishment and maintenance and for all exchanges issued by the dialogue acceptor.

5. Secured application dialogue: authentication will be used for the dialogue establishment and maintenance and for all exchanges issued by the entities involved in the dialogue.

The overall architecture makes use of the Security Exchange Service Element (SESE) as defined in ISO 11586-2 and 11586-3 and a System Security Function (SSF), which is a capability of a system to perform security related specific processing. Depending on the service level required, the security mechanisms thus implemented are based on digital signatures applied to association establishment,

association release or data transfer information items originated by application ASEs with a unique identifier (protection against replay).

There are important preliminary actions out of the scope of upper layers' security mechanisms. Depending on the service level required, part or all of the following actions must be completed for those security mechanisms to properly work:

- the sender must have the public key of the receiver together with the return certification path[5] from the receiver to the initiator and must have checked the validity of all the certificates in the certification path,

- the receiver must have the public key of the sender together with the forward certification path from the sender to the receiver and must have checked the validity of all the certificates in the certification path,

- sender and receiver clocks are synchronized by bilateral agreement (use of timestamps in signed messages).

[WG3/UPP] also includes an annex describing the need for security management mechanisms allowing appropriate security audit functions, thus permitting the necessary evaluation of the adequacy and the efficiency of the security policy. Those functions essentially concentrate on the detection of abnormal events with respect to security considerations, the recording of those events and the analysis of the collected events (the detection of a security event may generate a security alarm which can be used either for immediate recovery action or for further off-line analysis). The implementation of security management mechanisms will involve mechanisms pertaining to the ATN network management (logging of events, event forwarding).

2.3.3 European ATSO Material

2.3.3.1 EATCHIP NSM-TF Security Policy

The document referenced [NSM-TF] and produced under the leadership of AENA defines a security policy for the integration of the private ATSO aeronautical data networks. Though this document still has a draft form, its content is summarized below.

The document rather focuses on the assessment of general principles regarding the security of the internetwork made of the European ATSO networks (abbreviated as EAN) and the related organizational aspects. The document particularly aims at ensuring the coherence of a global security policy with the various local security policies. Specific security procedures or mechanisms to be used are not within the scope of the document.

It has to be noted that the outlined security organization calls for the creation of a specific organization (i.e. the EAN Security Forum) carrying out overall security tasks. Its relationship with local security organizations (at ATSO level) shall be defined by establishing the respective roles and responsibilities with regard to security tasks.

The document then proposes areas for the progressive development of the security policy (system security, security audit, contingencies and disaster management, corrective actions, security administration) and assesses general principles pertaining to the effective implementation of a security program (e.g., security life cycle issues, standardization issues regarding the procedures, the measures, the documentation, etc., required for a correct implementation of the security program).

[5] Appendix C illustrates the certification path concept as exposed in ITU-T Rec. X.509.

Annexes of [NSM-TF] contain more dynamic parts of the security policy, as they may need to be modified due to changes in the conditions under which the policy is to be applied. The security policy is thus declined for each above-mentioned area:

- system security: this is the central issue for the EAN security as its goal is to define, operate and maintain efficient security measures protecting general EAN resources (hardware, software, information, EAN-based network service, etc.), based on a corresponding risk analysis and according to security levels. This area encompasses the definition of :
    - an authorization policy (supervision of the access to the EAN resources, restrictions to the use of those resources), which particularly makes use of the general rule " deny all by default ",
    - security models regarding the strategy of authorization (either identity-based or rule-based, the latter making use of security levels associated to each EAN resource in general),
    - a security architecture, which must particularly take into account the very nature of the EAN made of different local security architectures with specific aspects arising from the interconnection of those local architectures,
    - a risk analysis for the EAN, allowing to identify the threats and vulnerabilities,
    - the EAN security requirements, derived from the security policy, the risk analysis and a cost/benefit evaluation (e.g., physical protection of EAN resources, access to the resources by internal staff, EAN user authentication mechanisms, access control based on security levels, automated record procedures, etc),
    - security levels, characterizing how critical a resource is with respect to security purposes (a guideline is proposed for that characterization).
- security audit : this area defines the means, resources and procedures required for ensuring the effectiveness of the security program,
- contingencies and disaster management : this area defines the means, resources and procedures required for ensuring a continuity of the EAN service in case of events affecting the normal operation of the network,
- corrective action : this area relates to the actions required by the detection of failures or limitations in the usual operation of the security system,
- security administration: this area deals with the roles and responsibilities of individuals and organizations involved in the EAN security program, e.g. defining the overall organization and the delegation of authority procedures for network security issues : for example, the proposed organization requires one Local Security Officer per ATSO to deal with EAN specific security issues.

2.3.3.2 DGAC Network Security

2.3.3.2.1 Security in the RENAR Network

RENAR by default allows any-to-any communications between internal users. Conversely external accesses to and from RENAR users are denied by default: specific access control functions based on X.121 address validation and/or translation are implemented at the boundaries of RENAR for controlling those external exchanges, including the exchanges with peer ATSO network users.

RENAR resources are located in protected environments (physical protection, physical access control allowing authorized personnel only, etc.) and access control measures are applied to RENAR

resources (password-based). RENAR critical resources are also duplicated so as to guarantee the continuity of its service in case of failure of any single internal component.

Ongoing activities pertaining to security include the use of closed user groups and the definition of a future access control and user identity authentication system relying on a dedicated central server working in relation with boundary RENAR switches

2.3.3.2.2 Security in Ground Environments (CAUTRA)

End systems, network components (e.g., LAN concentrators, routers, etc.) and network management systems are located in protected environments (physical protection, physical access control allowing authorized personnel only, etc.) and are generally protected by password-based access control. Those resources are duplicated for redundancy purposes whenever required.

Conversely current ground ATC applications generally do not impose any access control on end users (e.g., no password is required for the login of controllers to ODS workstations). However the communicating software entities can optionally exchange logical identifiers at connection set-up (ISO TP4 connections) for peer entity identification and use that information for application-level controls.

Several studies have been completed in the recent years regarding security in the context of the French ATC. Most of those studies have resulted in documents containing threat or risk analysis and consequent general recommendations or action plans, although no directly applicable security program with detailed measures has been produced:

- one study dealt with the security of the CAUTRA system, focusing on the overall CAUTRA system integrity (confidentiality was not retained as a requirement, availability was already handled within the system) and giving precedence to the consideration of external attacks (internal attacks resulting from non intentional actions were nevertheless also considered). The approach of the study was based the definition of " probable " attack scenarios built from the knowledge of the overall architecture, so as to measure the induced effects and consequently define appropriate countermeasures. The general conclusion for what concerns the future CAUTRA systems, based on open systems and internetworks and on standardized protocols and products, is the reinforced need for a global approach of security problems and for the definition of a coherent security policy along with actions to improve security concerns among all involved parties. General recommendations were finally proposed such as the implementation of access control measures for critical systems or functions,

- another study dealt with the security of the en route French ATC system. This study started with the identification of the critical functions of the system and of the potential attackers to be considered. The proposed next step of the study was the characterization of the existing architecture with regard to security considerations, the following identification of the vulnerabilities and a risk analysis so as to allow the definition of objectives for an appropriate security policy.

2.4 Internet Security

2.4.1 Motivation of this Section

This section contains a brief overview of security aspects of the Internet which might be relevant to the European ATN.

When compared with the Internet, the ATN, especially the European ATN, is only ever likely to be minute in terms of scale, i.e. number of users, nodes, amount of traffic and applications etc. Apart from that, the history of the Internet is at least two decades in advance.

Many similarities exist between the two internets (Note: "internet is used here in a generic sense, applying to the Internet internet as well as the ATN internet), amongst others:

- the fixed part of the logical architecture of the two internets is identical,
- there is an extensive correspondence in the protocol stacks (internetworking level, transport level, routing protocols),
- there are correspondences in the organisational structure concerning the freedom to interconnect and the independence of routing domains.

Of course, the Internet lacks the mobile components of the ATN.

Because of the *similarity* of the Internet with the ATN in many internet aspects and the vast *differences* in scale, it makes sense to look at the Internet in order to anticipate problems which might face the ATN in the long-term and to observe the solutions which have been or are being developed to solve them.

2.4.2 Current Security Practices

2.4.2.1 Threats

The term ”threat” in this section is taken to mean malicious attempts by persons to disturb the proper functioning of a system, whether for the gain of the perpetrator or not. Other dangers such as natural catastrophes and situations such as unusual traffic patterns etc. which were not engineered for are not considered in this context. In spite of protests from some quarters, the term ”hacker” has become the accepted name for those persons from whom threats originate.

Because of the enormous and ever increasing importance of the Internet in the areas of industry, government, education and entertainment, and their dependence on it, threats to its integrity and availability are of the utmost concern. Its most important characteristic, its openness, makes it extremely vulnerable because it cannot be the object of surveillance and control in a closed environment. In addition, many Internet *application environments* are also open (usually Unix-based, but increasingly Windows NT), meaning that any user with appropriate access rights, normally only the possession of a user name and the correct password, can establish user sessions, e.g. Telnet sessions, with systems connected to the Internet. Even worse: by compromising or impersonating a host, a hacker can sometimes gain access to resources such as access to other systems to which that host has access. Functions available via the World Wide Web are approaching those more primitive functions native to Unix.

It is with respect to such application environments that most concern and security work has been associated in the past several years. It is here that the hacker is feared the most. Threats to the availability of connectivity and bandwidth across the Internet and to the integrity and confidentiality of data flowing across it appear to be only of secondary concern. The recent history of security relevant events in the Internet would appear to bear out this assessment of the situation. A consideration of the volume of traffic being processed by a typical Internet node makes it obvious that a hacker has a difficult time making a focussed attack from within the Internet against a single user or a group of users. In any case, TCP together with IP already provides a good deal of resilience against the manipulation of IP packets since they are based on the assumption that the data transmission is unreliable.

For these reasons discussion in the following concentrates on *network access* to systems connected to the Internet. Questions of encryption techniques and digital signatures etc., although relevant to applications using the Internet, are not considered in this section because they are not *specific to* the Internet. Other Internet protocols such as routing protocols and SNMP are also subject to attack but are also not considered because of their highly specialised nature and because they have not been involved in many of the recorded Internet security events.

2.4.2.2 Means of Protection

Security protection in the Internet is currently concentrated on the implementation and operation of means to prevent non-allowed access to Internet hosts, cf. End Systems in the ATN.

2.4.2.2.1 Why are Internet Hosts vulnerable?

The success of hackers has in the past been due to a number of simple features of general purpose host systems:

- they normally run a wide range of complex software which interacts, e.g. via file systems, in an unpredictable way,
- this software often contains faults, which are known to hackers,
- security measures in the host are difficult to implement because of its complex, dynamic, fast changing environment.

The conventions used in operating Unix installations, e.g. naming conventions, are normally highly constant among different types of installations so that it is not normally difficult for a hacker to guess names, passwords, addresses, file locations etc. If, in addition, he is in possession of inside knowledge, e.g. through being a former employee, this makes his task even easier.

This situation makes it obvious that implementing security measures in Internet host computers themselves is likely to be futile.

2.4.2.2.2 The Firewall as a Gateway

The solution to the dilemma described in the previous section is to implement a gateway between a host computer (or a network to be protected) and the Internet. Its properties should be:

- all traffic passing between the host (or network to be protected) and the Internet must pass through the gateway,
- the gateway allows only traffic to pass which satisfies a well-defined security policy,
- the gateway, due to its structure, simple software, operation procedures and stability is immune to penetration.

Such a gateway has become to be known as a firewall and is a common feature of Internet connected hosts and networks. There are three basic types described in the following sections depending on the protocol level on which the filtering is performed.

2.4.2.2.3 Packet Filtering Gateway

Packet Filters are implemented in the Internet router software and work by dropping IP packets based on their source or destination addresses or ports. In general no context is maintained and decisions are made only on the header contents of the current packet. The administrator must create and maintain lists of IP addresses of hosts from which access is explicitly allowed and / or explicitly not allowed. Note that the sending IP address is not necessarily reliable and could have been manipulated.

At the IP level the applications and services being addressed are not known. For this reason, allowing access or not simply on the basis of IP addresses is usually too coarse. It may also be possible for a hacker to masquerade as a host with one of the allowed IP addresses.

Because of the predominance of TCP, the structure of data within packets is rather constant. Packet filtering can also use data in the TCP packet header such as the logical port number in order to make the filtering more specific. This is not true in the case of other Internet transport protocols such as UDP.

2.4.2.2.4 Circuit Gateways

Circuit gateways relay TCP connections. The caller connects to a TCP port on the gateway which connects to some destination on the other side of the gateway. Different techniques are necessary for incoming and outgoing calls. For the duration of the connection the gateway software copies data transparently between the two (half) connections.

Usually the gateway must be told the remote destination to which the second half connection needs to be set up. For this case there is a simple protocol between the caller and the gateway in which the remote host name or the numeric IP address is given. After the two half connections have been set up, the protocol is put out of operation. For incoming calls this process can be made automatic.

Several TCP circuit gateway packages are commercially available.

2.4.2.2.5 Application Gateway

An application gateway is a piece of software in the firewall written specifically to protect a given application or service. The remote user does not communicate directly with the application on the host computer but rather with the application gateway which then relays messages to and from the application. Protection measures such as special log on procedures, information filtering, logging etc. can be implemented as required. Application gateway can be a good means of implementing services accessed from outside such as electronic mail and ftp.

2.4.2.2.6 Other Techniques

Techniques other than the implementation of firewalls are fast changing, depending on the current methods being used by hackers. The techniques include:

- logging of network connections and the use of intelligent procedures to detect suspicious interactions,
- monitoring of attempts to reach certain address spaces which can reveal the presence of hackers and
- random tracing of connections.

It appears, however, that a long-term trend towards reliable user or host authentication (not just identification) by means of one-time passwords and cryptographic techniques etc. will make itself more evident in the near future.

2.4.2.3 Ongoing IETF Activities on Security

Most on-going IETF activities in the area of security aim at standardizing services and protocols for user authentication, message encryption or message integrity, using password-based or more sophisticated cryptographic techniques (e.g., public-key cryptosystems). The following subjects are particularly addressed by IETF workgroups in the security area:

- IP security (ipsec), which aims at providing cryptographic security services between hosts at the network layer,
- transport layer security, which provides security services at the transport layer (e.g., like SSL),
- S/MIME (in the messaging area), which defines MIME encapsulation of digitally signed and encrypted objects,
- one-time password authentication, which aims at counter replay attacks against connections carrying login ids and passwords,
- web transaction security, which develops requirements and specifications for secured web transactions (using HTTP),
- public key infrastructure: the works in that area are aimed at developing standards to support an Internet X.509-based public key infrastructure. This infrastructure should provide a framework which will support a range of trust/hierarchy environments and a range of usage environments (e.g., Privacy Enhanced Mail using RFC1422, ipsec protocols, secured www protocols, etc.).

2.4.3 Relevance to the European ATN

There are a number of significant differences between the security situation described above for the Internet and for the ATN:

- the ATN is not ”open” to the same extent as the Internet,
- only specific ATN applications are likely to be accessible in ATN End Systems: there should not be general-purpose applications such as remote login, file transfer, etc., thereby reducing the vulnerability of ATN End Systems,
- physical access to ATN End Systems is much more tightly controlled than in the case of the Internet.

The ATN with its safety critical applications demands much stricter security measures than the general-purpose Internet since the potential for sabotage and blackmail is much greater. Techniques along the lines of those currently implemented in Internet firewalls might be appropriate for the ATN. As in the case of the Internet, security measures can only be implemented satisfactorily provided that the periphery of the internet (i.e., the End Systems themselves) is also protected.

Additionally, the experience of the implementation, the deployment and the management of Internet mechanisms making use of cryptographic techniques such as Internet public key cryptosystems can provide a relevant input to the ATN, even if the ATN and the Internet environments present significant differences and the Internet experience is not truly available as applications requiring those mechanisms (e.g., e-commerce) only start to be widely used.

3. Security Requirements and Strategy

3.1 Security Requirements

3.1.1 Object of the Security Precautions

The object of the security precautions proposed in that document must be defined in the first place.

The subject of the security precautions in the ACCESS context is the European ATN network as described in [A208], including:

- the individual resources of the network : ground and air-ground subnetworks, intermediate systems (BISs and intra-domain ISs), ATN end systems and ATN network management systems,

- the end-to-end communication services provided by the ATN network to ATN user entities[6] (i.e., provided to ATN user applications by all ATN communication entities up to the ATN Application Entity level). Figure 1 shows the " upper boundary " of the ACCESS security considerations with respect to the ATN communication model : consequently if authentication of an ATN application-level communicating party is required, that party will be identified as an ATN Application Entity instance (e.g., the airborne CPDLC of a given aircraft) and not as a user application or its possible human end users,

- the ATN administration and network management communication services (e.g., communications between ATN managed resources and network management systems, configuration of ATN resources, etc.).

[6] The protection of ATN user applications and their possible end users (e.g., controllers, pilots, etc.) is therefore considered out of the scope of ACCESS: the proposed precautions will not aim at ensuring the identity of controllers, pilots, etc., which is a larger issue, particularly regarding the specific user applications rather than the ATN infrastructure.

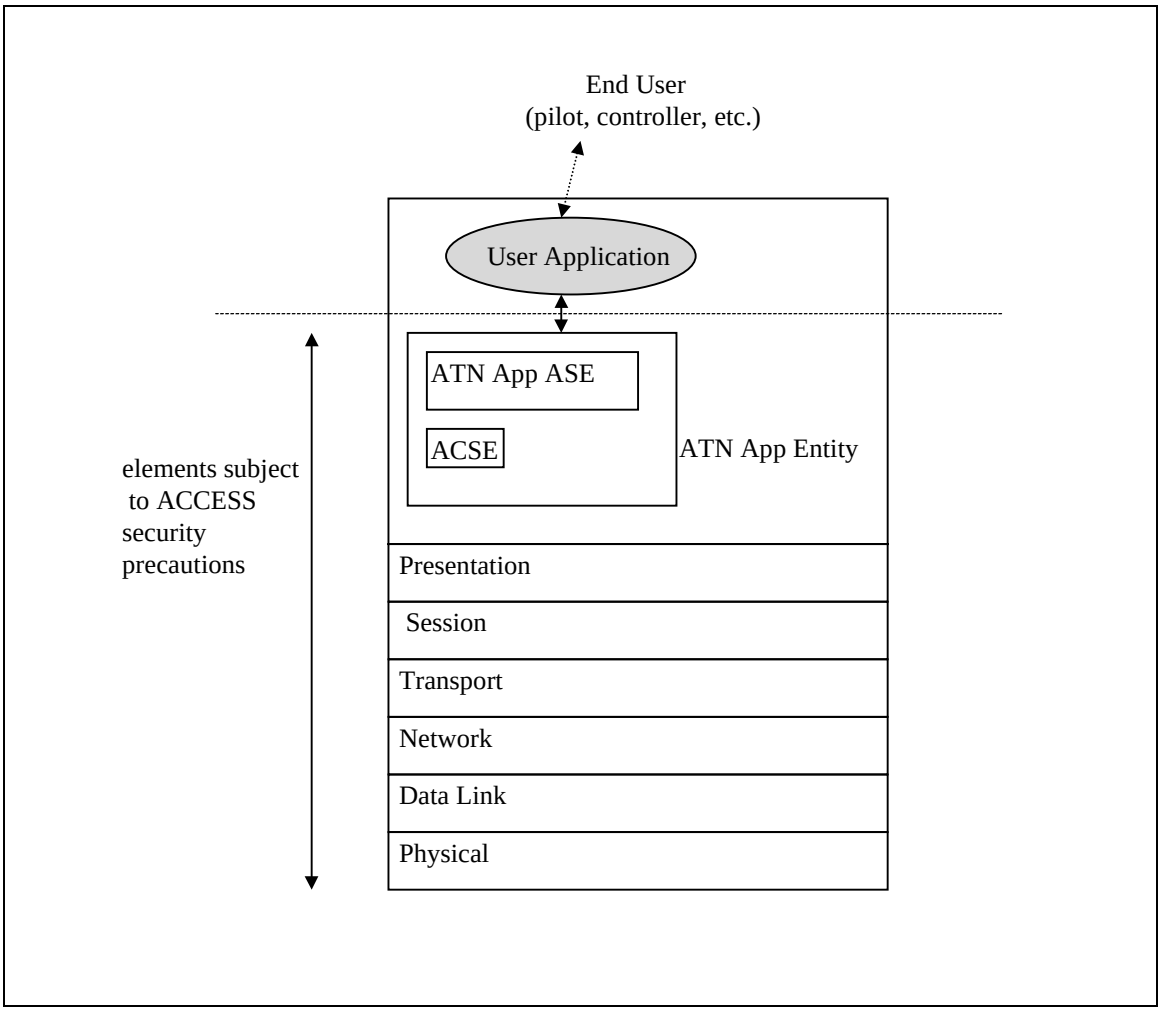

Figure 1: upper boundary of ACCESS security considerations

For what concerns the geographical limits of the ACCESS area and the specific institutional issues raised by the use of security means across different countries, although the ACCESS area is located within the EC, theoretically making fully applicable all relevant EC regulations or recommendations concerning the use of cryptographic means for data telecommunications, the integration of aircrafts originating from non EC countries makes inappropriate any limitation of the institutional concerns to strictly European considerations.

3.1.2 High-Level Security Requirements

The security objectives retained for the ACCESS ATN network are fully derived from the current expression of the ATN security policy objectives:

- communication monitoring and traffic analysis do not constitute threats for the ACCESS ATN network operation (no general need for confidentiality),

- data link messages as well as network management and routing messages shall be protected against modification, masquerade and replay : technical means ensuring authentication and integrity of the messages are therefore required,

- services supporting messages to and from aircrafts shall be protected against denial of service attacks,

- ATN systems shall be protected from unauthorized physical access.

The analysis of existing requirements and ongoing activities pertaining to security in the ATC area in general suggests that some of the above-mentioned objectives, essentially dealing with telecommunication security and more specifically with authentication considerations, can be further refined or completed with the following propositions:

- the availability of the European ATN services shall be ensured by appropriate architectural design choices and appropriate mechanisms (e.g., multiple alternative routes), so that single points of failure are minimized: this objective regards both system and telecommunication security,

- the objective of ATN system physical protection is the only previously described high-level objective pertaining to system security, the others being rather related to telecommunication security. In the area of system security, this initial objective can be broadened to the protection of ATN systems (and potentially all ATN resources) against misuse or misconfiguration, either intentional or not, by appropriate means (e.g., restriction of user access through access control with the definition of associated security levels, adapted training and system administration procedures for technical staff, etc.).

The general precautions to be applied in response to the formerly described threats will be made of technical provisions which can bring additional threats and consequently raise new security requirements: those requirements related to the implementation of specific countermeasures will be reminded as required in the next sections (e.g., the use of X.500 servers holding ATN security-related information can create additional security requirements for the access to the ATN X.500 directory).

Table 2 summarizes the proposed high level requirements for the security of the European ATN.

Ref.	Description	Type	Area
HL1	Data link messages shall be protected against masquerade, replay and modification	Integrity	Communication
HL2	Routing messages shall be protected against masquerade, replay and modification	Integrity	Communication
HL3	Network management messages shall be protected against masquerade, replay and modification	Integrity	Communication
HL4	Services supporting messages to and from aircraft shall be protected against denial of service attacks	Availability	Communication
HL5	Physical protection of ATN resources	Availability Integrity	System
HL6	Protection of ATN resources against misuse or misconfiguration (restricted user access, system administration procedures, IDRP authentication, etc.)	Availability Integrity	System Communication
HL7	Continuity of the European ATN communication services (redundancy, alternative routes, system administration procedures, etc.)	Availability	System Communication

Table 2: high-level security requirements

3.2 General Security Precautions Proposed for the European ATN

The general security precautions proposed for the implementation of the European ATN network are essentially derived from the current ATNP recommendations in the security area. They are made of both technical and physical or procedural provisions, thus providing adapted countermeasures for the retained security objectives.

3.2.1 Physical and Procedural Provisions

The general physical or procedural provisions proposed for the security of the European ATN are summarized hereunder:

- physical protection of ATN resources: ATN systems (i.e., end systems, intermediate systems and network management workstations) as well as ATN physical subnetworks' components (e.g., LAN hubs and switches, WAN switches, VDL GRS, etc.) shall be placed in locations with appropriate environmental protections (fire, flooding, etc.) and with specific physical access control protections restricting the physical access to only authorized personnel (e.g., using individual identification means, digital codes, etc.),

- user access control to ATN resources: ATN systems and more generally all systems participating to the ATN infrastructure (e.g., VDL GRS) should be protected by restricting user access according to security levels to be defined (use of appropriate passwords). For example, only maintenance personnel with an appropriate privilege level should be authorized to access and modify BIS or ATN ES configuration data. This type of precaution mandates the prior definition of a coherent organization for the operation and administration of the European ATN, thus allowing to define privileges based on the roles and responsibilities of the various involved parties,

- appropriate ATN system administration procedures: those procedural provisions, which aim at ensuring the correct behaviour of ATN components, are closely related to the administration requirements of each individual system and thus cannot be expressed in general terms. However they all aim at ensuring the overall availability of the network,

- appropriate ATN training procedures : those procedural procedures aim at minimizing misuses or misconfigurations of the ATN resources by authorized personnel and thus participate to the overall availability of the network,

- physical provisions minimizing network single points of failure: this set of provisions includes the replication of ATN critical components so as to minimize single points of failure wherever deemed appropriate. Use of alternative or redundant power supplies, implementation of replicated subnetworks, BISs, IDRP route servers, etc., are all examples of physical provisions participating to that objective.

The actual implementation of those provisions will highly depend on local issues, such as the location of the considered systems (ACC, airport, aircraft, etc.) and the existing security policy and security practices of the organizations responsible for the operation of the ATN equipments (ATSO, IACSP, Airport Operator, etc.), as the ATN security provisions will probably be integrated to the relevant organizations' overall security policy (e.g., physical access control procedures or means can be used for restricting access to ATN resources as well as other resources that may be located in the same operation center).

3.2.2 Technical Provisions

3.2.2.1 Core Provisions

The core technical provisions proposed for the security of the European ATN are derived from the current recommendations issued by the various ATNP workgroups in the security area and are summarized hereunder:

- technical provisions will be based on a security framework that uses security keys and digital signatures at the scope of ensuring the authentication and the integrity of the ATN messages. The European ATN security architecture will use the strong authentication mechanisms provided by a dedicated ATN public key cryptosystem based on ISO 7498-2 (ITU-T X.509 framework) while being algorithm-independent,

- secured exchanges of ATN application-level messages and ATN system management messages will be provided by the ATN upper layers' secured services based on ISO 11586 and using the services of the ATN public key cryptosystem. Those ATN upper layers' security mechanisms will provide five different security services to the communicating application entities,

- secured exchanges of ATN routing information will be provided by the authentication services of the ATN internetwork layer (IDRP authentication) using the ATN public key cryptosystem. The use of IDRP authentication will follow the applicable ATNP recommendations (i.e., uplink IDRP messages sent to airborne BISs will not be authenticated),

- alternative routing and routing control shall be set wherever possible to minimize the effects of denial of service attacks :

    - alternative routing offers alternative routes to avoid points of failure or attack : it can be facilitated by redundancy provisions (see previous section) and routing control,

    - forwarding control allows to restrict the forwarding of packets at specific network locations, based on the knowledge of whether the packets have been authorized to use a particular path (e.g., using access lists based on source and/or destination addresses) : even if forwarding control is certainly very difficult to implement in the core parts of the network, its use at specific locations within the network can be envisioned to reduce denial of service attacks,

- the built-in security logging capabilities of ATN systems will be used to detect and log any abnormal event in the frame of security. Those events (potential security violations) will be stored and/or forwarded to ATN network management systems for either on-line recovery actions or further off-line analysis,

- subnetwork-level provisions restricting the exchanges between authorized communicating devices (e.g., based on subnetwork-level addresses) can be envisioned for ATN subnetworks connecting a stable set of identified ATN systems, which makes those provisions better adapted to ground subnetworks.

3.2.2.2 Additional Provisions

Though those technical provisions will be described in a more detailed fashion in the chapter dealing with the target security precautions, their general presentation already allows to identify further requirements, essentially concerning the implementation of:

- a distributed Public Key Infrastructure (PKI) dedicated to the European ATN operation (and probably part of a world-wide ATN PKI), whose objective is to provide for the creation, distribution and revocation of the security information (security keys, certificates, etc.) required by the users of the ATN public key cryptosystem. This PKI requires the establishment of ATN Certification Authorities, an adequate ATN Certification Policy and trusted certification paths,

- an associated distributed European PKI repository (probably part of a world-wide ATN PKI repository) required by PKI users for the distribution of relevant security information (public keys, certificates, etc.). It is likely that this PKI repository will be a part of an ATN global X.500 directory, which can be used for achieving other objectives non related to security (e.g., the directory can contain ATN addressing and naming information),

- clock synchronization mechanisms[7], required by the two-way authentication scheme used by ATN upper layers' security mechanisms,

- an enhanced CM application providing the required security information distribution between airborne and ground ATN applications, probably via requests to the PKI repository (i.e., the ATN X.500 directory),

- upgraded ATN ASEs, able to manage the security services offered by the ATN upper layers.

Those technical requirements call for the definition of additional security objectives and the proposition of consequent additional provisions, either technical or procedural:

- ATN PKI nodes are critical resources for the operation of the ATN public key cryptosystem : appropriate measures must be taken to minimize the effects of ATN PKI nodes' malfunctioning or failures (e.g., PKI repository information shall be made available by different servers),

- the distributed security information (certificates / public keys) shall be made accessible only to authorized ATN users[8] : ATN authentication mechanisms can be used to that purpose (e.g., exchanges between the ATN X.500 servers and their ATN users or between ground CM applications and CM users),

- ATN databases holding security information (i.e., X.500 servers) must be protected : physical access protection and user access control countermeasures shall be implemented (only authorized personnel with appropriate credentials is allowed to modify or create X.500 entries),

- Certification Authorities trustworthiness: CAs shall ensure the validity and the availability of the information they certify and protect their private key, by using appropriate procedures and means (strict physical security measures, regular backup / disaster recovery procedures, use of secret sharing protocols to prevent any single individual from having the capability to know the CA private key, etc.),

- key / certificate management: specific procedures or mechanisms must be used to protect PKI management interactions. For example, concerning the key/certificate initialization process, the key pair used by signing entities can be generated either by a CA, a trusted third-party or event the key user itself. The communication of the public key to the CA (by the key pair generator, be it key user or trusted third party) and the communication of the private key to the corresponding key user (by the key pair generator, be it CA or trusted third party) must be achieved by appropriate on-line or off-line secured means ensuring the confidentiality and the integrity of the keys and the authentication of the parties exchanging the keys,

- private key protection: private keys used by signing entities (e.g., BISs, ATN Application Entities) and stored in ATN systems must be protected from local disclosure : appropriate user access

[7] It is not clear whether clock synchronization has already been addressed by relevant ATNP works. Moreover that issue should not be only developed in the context of security as clock synchronization may be required for other purposes.

[8] Though public keys and certificates are not confidential and are rather intended to be widely distributed, there is a recognized requirement within the ATNP that such "publicly" available informations be not advertised out of the ATC community.

control and/or local password-based encryption algorithms can be used to that purpose. Moreover, when generated by CAs or other third-parties, specific measures, including "secret-splitting" or "secret-sharing" protocols and encryption algorithms, must be used for ensuring the confidentiality of the private key storage in the CA premises.

3.2.3 Summary of General Provisions

Table 3 summarizes the general security provisions proposed for the implementation of the European ATN.

Ref.	Provision Description	Related Objectives
GP1	Physical protection of ATN resources (including ATN PKI resources)	HL5
GP2	User access control to ATN resources (including ATN PKI resources)	HL6
GP3	Appropriate ATN system administration procedures	HL6, HL7
GP4	Appropriate ATN training procedures	HL6, HL7
GP5	Provisions reducing ATN single points of failure (including ATN PKI single points of failure)	HL1, HL2, HL3, HL7
GP6	Use of ATN upper layers' security mechanisms by ATN Application Entities (including network management)	HL1, HL3
GP7	Use of IDRP authentication services by ATN BISs wherever applicable	HL2, HL6
GP8	Alternative routing	HL4, HL7
GP9	Forwarding control (where deemed appropriate)	HL4, HL6
GP10	Subnetwork-level provisions (ground subnetworks only)	HL1, HL2, HL3, HL6
GP11	Security management provisions for recording and analyzing security violations	all
GP12	Establishment and enforcement of ATN certification procedures and security means applicable to ATN Certification Authorities	HL1, HL2, HL3
GP13	Key/certificate management secured procedures and/or mechanisms	HL1, HL2, HL3
GP14	Private key protection measures	HL1, HL2, HL3

Table 3: general security provisions

3.3 Derived Implementation Strategy

Many general security provisions proposed for the implementation of the European ATN make use of technical mechanisms that will not be part of CNS/ATM 1 implementations. Moreover a number of issues related to the use of those mechanisms within the ATN are not yet completely defined, as activities are still in progress in the ATNP for the specification of appropriate recommendations and guidance material in the area of security.

It is assumed that CNS/ATM 2 packages fully integrate the capabilities already outlined in applicable draft versions of CNS/ATM 2 SARPs:

- ATN upper layers' security capabilities,
- IDRP authentication capability,
- built-in security audit trail functions (e.g., detection, logging and forwarding of abnormal events in the frame of security),
- X.500 capabilities if required (e.g., DUA or DSA integrated to CM),
- etc.

Conversely it does not seem realistic to meet all the proposed ATN security objectives with CNS/ATM 1 implementations, as they do not include some core security capabilities. The only objectives that can be partially or fully met are those objectives not requiring the use of the recommended ATN public key cryptosystem, i.e. HL4, HL5, HL6 and HL7 objectives as referenced in Table 2.

It is therefore proposed a two-step implementation strategy for the European ATN be adopted in the ACCESS area:

1. Initial ACCESS ATN: implementation of an initial set of security precautions aiming at meeting the objectives deemed realistic with CNS/ATM 1 packages. These objectives should constitute a subset of the previously identified objectives and should not require the implementation of any public key cryptosystem,

2. Target ACCESS ATN: implementation of the full set of identified security provisions. Ideally this step should be completed when ATN systems and networks will all be based on CNS/ATM 2 packages; however the simultaneous operation of both CNS/ATM 1 and CNS/ATM 2 packages is probable and the security provisions shall be adapted to handle that coexistence (i.e., backward compatibility shall be ensured).

The remaining sections of the document will describe the security precautions to be adopted in the context of the target security architecture (step 2). The initial security precautions (step 1) will be presented in the ACCESS work package WP240 (Transition Issues).

4. Target Security Provisions

4.1 Introduction

4.1.1 Objective of the Chapter

This chapter proposes security provisions for the target European ATN network in the 2005-2010 timeframe.

Those provisions, which are based on the general requirements and propositions presented in Chapter 3, are detailed with respect to the ACCESS architecture as presented in [A208] and some basic assumptions essentially concerning the final shape of ATNP security recommendations and guidance material (which currently still have a draft status).

The chapter will therefore focus on architectural and implementation issues, many of them being left as local matters in the relevant ATN material or being related to the implementation of the ATN public key infrastructure (ATN PKI).

4.1.2 Basic Assumptions

The provisions proposed in Chapter 4 are based on the following basic assumptions:

- CNS/ATM 2 implementations are considered to be widely deployed in the 2005-2010 timeframe, so that it can be assumed that security mechanisms of CNS/ATM 2 implementations will be fully usable,

- however as the likely situation to be coped with will be made of coexisting CNS/ATM 1 and CNS/ATM 2 implementations, it is assumed that CNS/ATM 2 security mechanisms will be backward-compatible with CNS/ATM 1 implementations, possibly resulting in the negotiated non-use of any CNS/ATM 2 security function for a given communication (e.g., unsecured dialog between applications),

- the security solution for the authentication and integrity of routing messages between ATN BISs is the one described in Chapter 2.3.2.5.4,

- the basic scenario for the operation of upper layers' security mechanisms between airborne and ground ATN applications is based on Example 1 described in Chapter 4.2 of [GUID],

- all protocol elements of the security mechanisms used in CNS/ATM 2 implementations (certificate formats, security key length, digital signature algorithms, version negotiation, etc.) will be established so that interoperability between ATN entities using security mechanisms will be ensured,

- the ATN public key infrastructure (ATN PKI) will make use of a distributed X.500 directory for the distribution of security information (certificates, public keys) to key users,

- organizational as well as regulatory aspects are considered to be coherent with the proposed provisions (those aspects are covered by Chapter 5).

A number of issues regarding the ATN public key infrastructure (ATN PKI) have not yet been fully addressed by the various relevant ATNP workgroups. Examples of PKI issues not yet finalized are:

- key pair holder: basically each key pair is associated to a specific entity identified by a globally unique distinguished name. The identity of ATN key pair holders is not finally established, however the current assumptions are that key pairs will be generated on an aircraft basis for

airborne signing AEs and on an AE basis for ground signing entities[9] (e.g., a given ACC's CPDLC application),

- key generation and key lifecycle, defining key pair generators (CA, trusted third-party or key holder itself) and the lifetime of key pairs (key pairs for airborne users should be valid for the duration of the flight at a minimum),

- public key / certificate retrieval: the precise mechanisms used by a signing entity for retrieving the certificate of a communicating peer (e.g., as part of the process described in Example 1 of Chapter 4.2 of [GUID], reproduced in Appendix B) and for obtaining and verifying the possible certification path are not yet defined. This aspect is closely coupled with the ATN Certification Authority structure to be defined (hierarchical relations between CAs, cross-certifications, etc.),

- certificate management: this issue is related to the (on-line) protocols or (off-line) procedures used for supporting the interactions between the various PKI nodes (PKI user entities, CAs, PKI repository nodes, etc.). Examples of such interactions are the posting of certificates to the repository, the revocation of certificates, the initial registration/certification of an end user by its CA (including the initial communication of the "trusted" CA public key to its user) , key pair maintenance operations (e.g., key pair recovery/update), cross-certification establishment, etc. ,

- ATN CA structure: this issue is related to the way ATN Certification Authorities are organized for serving the community of PKI user entities. The ATN CA structure will highly impact the certificate verification process run by ATN user entities each time a new peer needs to be authenticated (e.g., potentially each time an airborne BIS will have to establish a " secured " adjacency with an air-ground BIS).

Appropriate assumptions or propositions regarding these various aspects of the ATN PKI will be made in the section proposing a PKI for the ACCESS area.

4.2 Classification of ATN Resources

ATN resources encompass all hardware or software components participating to the ATN network operation. They include:

- ATN systems, either ISs (intra-domain or BISs) or ESs (including network management stations),

- ATN-used subnetworks, either air-ground (VDL, AMSS, Mode-S) or ground-ground (packet-switched WAN, leased line, LAN),

- ATN PKI management nodes (X.500 servers, CA systems, etc.).

The security provisions to be applied to ATN resources can be interpreted following two possible approaches:

1. The first approach makes no distinction between the various resources : security provisions are valid for any ATN resource,

2. The second approach makes distinctions between the resources based on pre-defined criteria: a security level can thus be associated to each resource, e.g. according to its criticality for the ATN

[9]It is not clear whether an airborne BIS will use the single aircraft-based key pair used by all airborne AEs or whether it will use a different dedicated key pair that would be generated on an airborne BIS basis. Similarly for ground signing entities, if a single key pair is being used on a facility basis rather than on an AE basis, the same question arises for signing air-ground and ground BISs.

operation. This approach therefore requires that ATN resources be classified with respect to security considerations[10].

The second approach appears to be more realistic as it is thought to be better suited to the actual operation of a network. In the following sections of this chapter, it is therefore assumed that classifications of ATN resources exist and that the applicable security provisions will be appropriately derived for each resource type. Consequently it is likely that ATN resources will not be subject to the same precise security measures.

An **example** of a general security classification is given in the following table, based on 3 security levels (critical, essential and normal). This classification could be further refined by taking into consideration the precise ACCESS topology, e.g. making distinctions between resources according to the facility they are located in (ACC, airport, etc.).

ATN resource	Class
backbone BIS	essential
route server	critical
RD BIS (A/G or ground BIS)	normal
network management ES	essential
ground ES	normal
X.500 server	critical
CA system (e.g., realizing certificate and key generation, storage and recovery)	critical
ground European WAN	essential
a/g subnetwork (e.g., VDL station)	normal

Table 4: classification of ground ATN resources

Recommendation: it is necessary to define classification(s) of ATN resources with respect to security considerations. The classifications should be common to the ACCESS area for backbone resources at least. This task includes the prior definition of the criteria used for the classification(s) and the number of security classes to be managed.

[10]Several classifications can be envisioned based on the precise security provisions that are considered: availability, physical access control, user access control, etc.

4.3 Physical Provisions

4.3.1 General

The general related provision as expressed in Table 3 is reminded below.

GP1	Physical protection of ATN resources (including ATN PKI resources)

This section only proposes physical security provisions to be adopted for the ground sites of the ACCESS area: ACCs, airports, other ATS sites, etc.

The precise measures for ensuring the proposed physical security provisions can be chosen and implemented on a local basis in accordance with the local security policy and practices and with the topology constraints of the considered site (ACC, Airport, etc.), provided those provisions are effectively ensured.

It is likely that protected ATN resources will be located with other non-ATN resources (e.g., networking or telecomm equipments, ATS servers, etc.) in appropriate locations within the site premises, thus benefiting from the existing technical and procedural security protections of the local infrastructure.

4.3.2 Physical Access Control

ATN resources should be located in premises with physical access limited to authorized personnel only, possibly with specific access control systems. The type of access control system to be used is a local issue (digital code, electronic badge, etc.).

ATN PKI critical resources (CA systems in general and specifically CA systems holding the CA private key, user certificate/key pair generation or storage systems, X.500 repositories, etc.) shall be particularly protected by strong physical access procedures and/or systems.

4.3.3 Protection Against Environmental Threats

ATN resources shall be located in premises protected from natural threats (flooding, fire, earthquake, power supply shortage, etc.) by appropriate local installations. The type of installation protection is a local issue.

4.4 User Access Control Provisions

The general related provision as expressed in Table 3 is reminded below.

GP2	User access control to ATN resources (including ATN PKI resources)

User access control is intended to restrict the use and/or administration of ATN resources to authorized personnel only:

- user access shall be limited to local access only (remote dial-in to ATN resources should be allowed on an exception basis when fully required; access control mechanisms used for the login of remote users should provide the same level of service as for local users at a minimum),

- the mechanisms used to that purpose shall be password-based at a minimum and can call for the definition of different user/administrator profiles with associated privileges allowing them to

perform pre-defined operations on the protected resources. The specific mechanisms to be used are a local issue, except for the resources that are to be accessed by different actors.

User access control measures must be specifically implemented on the periphery of the ATN, i.e. on ATN end systems, which are the ATN resources most exposed to users and consequently to possible malicious attackers (especially if those end systems are not in protected premises, which may be required for certain applications destined to a "large" community of ATS users).

User access to ATN network management systems and to ATN PKI critical resources (CA systems, X.500 directories) shall be particularly protected by strong control mechanisms (e.g. using the X.509-based strong authentication services for access to the X.500 directories with write/modification privileges).

Recommendation: it is necessary to identify those resources which can be used/managed by different actors of the ACCESS area and define common user access control mechanisms and appropriate user/administrator profiles and associated privileges for the access to those resources, if required. This action is closely related to ACCESS organizational issues and network management aspects.

4.5 System Administration and Training Procedures

The general related provision as expressed in Table 3 is reminded below.

GP3	Appropriate ATN system administration procedures
GP4	Appropriate ATN training procedures

The main objective of the system administration procedures is to ensure the considered system is in conditions allowing it to provide its expected services, including in the security area. Those procedures are to be considered in the two following ways with respect to security:

- availability: the continuous operation of the system requires some specific administration tasks to be accomplished (e.g., file system maintenance, upload of local records, data backups, etc.),

- integrity: the correct operation of the system demands appropriate easy-to-use administration procedures aiming at reducing the non intentional threats raised by misuse or misconfiguration of the system.

Particularly strict procedures must be applied to ATN PKI critical resources, especially to CA systems holding essential security data (certificates, CRLs, key pairs, etc.), which should be administered with appropriate procedures ensuring the confidentiality and the availability of the stored information (using specific disaster recovery procedures or mechanisms).

The main objective of training procedures is to ensure the maintenance personnel has the appropriate knowledge and information to correctly manage the network resources. As for system administration procedures, training procedures target availability and integrity requirements. They include continuous training programs following the possible updates or evolutions of the managed networks and are closely related to network management aspects.

4.6 Availability Provisions

The general related provision as expressed in Table 3 is reminded below.

GP5	Provisions reducing ATN single points of failure (including ATN PKI)

Those provisions aim at ensuring the continuity of the ATN communication services, essentially at the lower layers' level (up to the internetwork layer).

In addition to the built-in quality provisions which should have been applied by the component suppliers to all product production phases, two types of provisions can be envisioned for the European ATN with respect to availability objectives:

1. Architectural provisions: the way the European ATN is designed (i.e., its logical topology and its physical implementation) can ensure by itself the continuity of its operation after a failure has occurred in the network. An example of such a provision is provided by the use of multiple connections and alternative routing and/or adaptative dynamic routing (see further), which provides with the capability of using multiple network paths at the internetwork level,

2. Redundancy provisions: some critical network components should be duplicated to overcome problems caused by their failure. Switchover between duplicated components may be manual or automatic, depending on the availability requirements of the component and the associated technical constraints.

Priority must be given to "core" resources in the application of availability provisions, as their failure would generally cause more damages to the ATN operation (e.g., ATN routers are supposed to be more critical than ATN end systems).

Examples of availability provisions are given hereafter:

- if option 1 is retained for the ATN architecture in Europe (see [A208] and [A203]), the route server of the European (sub)island(s) should be duplicated (IDRP should ensure the automatic recovery in case one of the route servers fails),

- any given national ATSO ATN RDC should be connected to two different backbone BISs at a minimum (possibly located in different sites), so as to provide different usable paths between the ATSO RDC and the backbone,

- duplicated systems (e.g., duplicated BISs within an ACC) should be connected to different WAN entry points and should be using separate power supply circuits (if locally available),

- the architecture of the ATN PKI repository (i.e., the global ATN X.500 directory) should be designed so as to continuously serve its users in case of any component failure : appropriate X.500 mechanisms (such as directory replication) and/or duplicated systems homing X.500 servers can be envisioned to that purpose,

- etc.

ATN PKI critical resources such as CA systems shall particularly be made available to their users by appropriate mechanisms and/or procedures.

Recommendation: a specific action should be completed to determine the availability provisions to be retained for the European ATN (based on the network and routing architectures as presented in [A208] and in [A203]) and for the associated European ATN PKI (to be defined).

4.7 Subnetwork-Level Provisions

The general related provision as expressed in Table 3 is reminded below.

GP10	Subnetwork-level provisions (ground subnetworks only)

Those provisions are intended to restrict the use of the ATN subnetworks to specified devices only, e.g. based on subnetwork-level addressing (X.121 address for X.25 WAN, MAC address for LAN, etc.). They should be applied to subnetworks connecting a stable set of ATN systems, which makes them suited to ground subnetworks only.

Those provisions aim at protecting the network resources from both intentional and non-intentional threats (the connection of any new ATN device to the subnetwork requires a specific validation action to be effective).

The precise technical provisions to be applied to the interconnections based on existing national PSNs should be locally selected and implemented in accordance with the national PSN security policies.

The precise technical provisions to be applied to the interconnections based on the future EAN should be selected and implemented in accordance with the EAN security policy based on the ongoing NSM-TF works.

Examples of such provisions are proposed below:

- the X.25 Closed User Group facility can be used in the EAN to restrict the X.25 connections within a given set of identified X.25 user equipments. For example, this X.25 facility or equivalent mechanisms could be used on the backbone for restricting X.25 exchanges within the identified set of backbone BISs and route servers (incoming/outgoing connections from/to other EAN-accessible devices will thus be prohibited),

- LAN equipment facilities can be used within ATN sites to restrict the communications between identified sets of LAN devices (e.g., using Virtual LANs).

4.8 Internetwork-Level Provisions

4.8.1 IDRP Security

The general related provision as expressed in Table 3 is reminded below.

GP7	Use of IDRP authentication services by ATN BISs wherever applicable

The European ATN BISs shall make use of IDRP security provisions as recommended by applicable ATNP WG2 documents (see [WG2/450]).

Current assumptions about IDRP security are summarized below:

- use of digital signatures for all IDRP messages (including IDRP updates),

- authentication of downlink IDRP exchanges only, in the case of airborne BISs,

- airborne BISs will have a pre-loaded private key and certificate (aircraft-based at a minimum),

- air-ground BISs will authenticate airborne BISs based on the corresponding public key retrieved either by X.500 look-up or local caching,

- ground BISs will use authentication based on a pre-loaded private key and on the retrieval of public keys by different possible means (X.500 look-up, local caching, etc.) as a local matter.

As different alternatives are still envisioned for retrieving the peer BIS's certificate at the IDRP connection set-up, it is difficult to make any assessment on the exact retrieval mechanisms that will be recommended and used:

- one proposed solution assumes that air/ground BISs will retrieve from the ATN PKI repository (i.e., X.500 DSAs) the certificates associated to airborne BISs, by either integrating an X.500 DUA or using a gateway (e.g., the ground CM) making the appropriate X.500 lookup on behalf of the BIS. This retrieval process may be accomplished by the air-ground BIS prior to the IDRP adjacency establishment, by using a priori knowledge of the corresponding flight plan information, which allows to uncouple the X.500 lookup and the certificate verification process from the actual IDRP authentication,

- another proposed solution is based on certificate passing at the IDRP adjacency establishment, which would result in the certificate verification process alone, prior to the achievement of the IDRP authentication,

- the retrieval by a ground or air-ground BIS of the public key (or certificate) associated to a peer ground or air-ground BIS can be made by bilateral procedures according to specific agreements (the adjacency is supposed to be relatively static). Anyway the solution based on X.500 lookups to the ATN directory remains valid.

Certificate retrieval interactions between DUAs and DSAs are not required to be particularly secured in the general case: however as their use shall be restricted to the ATC community, those interactions should be secured, e.g. using the appropriate X.509 strong authentication mechanisms. Similarly interactions between the BIS and the local CM application shall be authenticated using the ATN upper layers' secured services.

Security provisions applicable to initial key loading, key storage and key management in general will be described in further sections of this chapter.

4.8.2 Alternative Routing

The general related provision as expressed in Table 3 is reminded below.

GP8	Alternative routing

The European ATN shall be architectured to provide alternative routes between any pair of ERDs at a minimum.

The internal architectures of national RDCs and of their component RDs shall be designed so as to provide alternative routes between ESs when deemed appropriate.

This provision is intended to protect the European ATN against denial of service attacks or against non-intentional threats (e.g., failures) that could result in the loss of a route within the network. The implementation of this provision is closely related to the implementation of availability provisions as described in Section 4.6 because redundant connections and/or ISs allow alternative routing to be set up.

The re-routing along an alternative inter-domain route is automatically done by IDRP, provided one of the BIS in the route detects the failure of an adjacent component or possibly its decreasing

performance. Re-routing internal to a RD is also possible in case an element of the network path fails and is automatically provided by IS-IS.

4.8.3 Forwarding Control

The general related provision as expressed in Table 3 is reminded below.

GP9	Forwarding control (where deemed appropriate)

Forwarding control provisions can be implemented to restrict the forwarding of CLNP packets at specific network locations. Those provisions should be at a minimum based on source and/or destination NSAP address prefixes in conformance with the addressing plan of the network as proposed in [A206].

They should not be implemented in core parts of the European ATN (such as the backbone): their use should be restricted to peripheral parts of the network (e.g., at ERD boundaries) where their management is relatively simple and where their operation cannot affect alternative routing provisions.

Typical implementations of forwarding control provisions make use of access lists, filtering the packets based on their NSAP addresses (and possibly on criteria based on other fields) and taking an appropriate decision (packets are forwarded or dropped). Logging of dropped packets due to forwarding control mechanism can help identify the origin of the denial of service attacks or of the responsible misconfigurations.

Simple **examples** of forwarding control applicability are presented in Table 5.

Network location	Forwarding control measure
ACC A/G BIS	Only packets originated from airborne ESs (i.e., with the appropriate source NSAP prefix identifying airborne systems) must be forwarded to the ground ESs
(Europe Western Area SubIsland) Backbone BIS	Packets originated by ground ESs not located in the connected national ATSC RDC (i.e., having a source NSAP not matching the appropriate prefix identifying all ground systems of the national ATSC authority) shall not be forwarded from the national RDC onto the backbone

Table 5: forwarding control measures (examples)

4.9 Upper Layers Security Provisions

The general related provisions as expressed in Table 3 are reminded below.

GP6	Use of ATN upper layers' security mechanisms by ATN Application Entities (including network management)

ATN Application Entities will use the security mechanisms provided by ATN upper layers, thus allowing any ATN ASE to request at connection set-up one of the five secured dialogue levels.

The basic scenario for the use of those mechanisms by air-ground applications is presented in Chapter 4.2 of [GUID].

The interactions for the retrieval and verification of the certificate (including the public key) of the communicating peer entity required at the establishment of a secured dialogue is not yet fully specified in ATNP relevant recommendations: a likely solution makes use of an enhanced CM application

integrating a X.500 DUA capability for issuing appropriate requests to the X.500 servers of the ATN PKI (another solution uses an integrated CM/X.500 DSA application) and locally caching the required certificates for further distribution to local ground ATN applications using the CM services.

With that scheme, the certificate retrieving process may be accomplished by the ground CM prior to the logon phase issued by the airborne CM, by using an a priori knowledge of the corresponding flight plan information, which allows to uncouple the X.500 lookup and the certificate validation processes from the actual upper layers' authentication process.

In the general case, the induced X.500 interactions (between DUA and DSA) are not required to be particularly secured: however as the use of certificates shall be restricted to the ATC community, those interactions should be secured, e.g. using the appropriate X.509 strong authentication mechanisms. Similarly the interactions established for certificate distribution between the ground CM and CM-user ground applications shall be authenticated using the ATN upper layers' secured services.

Security provisions applicable to initial key loading, key storage and key management in general will be described in further sections of this chapter.

4.10 ATN PKI

This section aims at proposing a public key infrastructure for the European ATN and security provisions for its operation. The proposed infrastructure as well as the related provisions are based on assumptions that shall be verified against the future specifications or recommendations issued from the ongoing works of the ATNP workgroups in the security area.

4.10.1 PKI Model and Assumptions

4.10.1.1 Introduction

The ATN PKI is made of nodes that are PKI user entities[11] (e.g., ATN AEs, ATN BISs, etc.) or PKI management entities (e.g., ATN CA systems, PKI repository nodes, etc.). PKI user entities are essentially ATN security user entities (e.g., ATN AEs). PKI management entities can also be PKI user entities (e.g., a CA using ATN secured services for the exchange of a certificate).

The European ATN PKI is assumed to be distributed and, from an administrative perspective, hierarchically structured so that PKI management entities manage identified sub-communities of end users and possibly other lower-level management entities with appropriate delegation of authority.

ATN security user entities can be classified as follows:

- for a given aircraft, airborne ATN security end users can be identified as each signing entity from an operational point of view (i.e., the airborne BIS plus each supported airborne AE). From a PKI management perspective, airborne PKI user entities can be reduced to two entities at most :
    - the aircraft-based ATN "AE-level" entity, since it is assumed a single security key pair is used per aircraft for AEs (the way the aircraft-based key pair is made available to the various airborne signing AEs is assumed to be covered by local means),
    - the airborne BIS[12] if it uses its own key pair (for IDRP authentication).

[11] A PKI user entity can be defined as an entity subject of a certificate.

[12] There is also the possibility that the key pair used by the airborne BIS be the one used by the airborne AEs: in that case a single PKI user entity per aircraft should be considered from a PKI management perspective.

- ground-based ATN security end users can be air-ground BISs, ground BISs and ground ATN AEs. From a PKI management perspective, they are considered as different potential PKI user entities as they can use their own key pairs. Another possible solution is based on the use of a single key pair per facility[13].

ATN PKI management entities can be classified as follows:

- CAs: they perform certificate management tasks such as certificate/CRL generation and update, certificate/CRL posting to the ATN PKI repositories, etc. They may perform additional tasks related to the generation of key pairs (key pair generation, key pair recovery, etc.). Subsets of CA functions can optionally be carried out by specific PKI management entities called Registration Authorities (RAs) : the PKI proposed for ACCESS will not make appear RAs as this concept is not specifically identified in the current ATNP documents about security,

- repositories : they are assumed to be X.500-based and to hold security information required by ATN security end users (certificates, CRLs, cross-certificates, etc.) for the operation of the ATN security mechanisms,

- trusted third-parties, e.g. responsible for the generation of key pairs on behalf of ATN security end users.

The concept of operations of the ATN security (as drafted in [GUID]) should define the way ATN security user entities interact with the PKI infrastructure to get the ATN security mechanisms properly working.

4.10.1.2 Operational Model

An operational model for the ATN security can be extracted from Example 1 described in Chapter 4.2 of [GUID]: the only interactions between ATN security user entities and ATN PKI management entities are the lookups to the global PKI repository to obtain and validate the certificates of peer signing entities[14].

Figure 2 summarizes that operational model for signing AEs inducing air-ground communications (the figure assumes each ground AE uses its own key pair):

1. Logon request from aircraft's CM including its digital signature (the aircraft CM is supposed to hold a pre-stored database of the public keys of the ground CMs).

2. Request of the ground CM to the global ATN PKI repository (X.500 lookup) to obtain the aircraft's certificate and the corresponding public key (this step includes the verification process by which the ground CM obtains the certification path to the aircraft's signing entity). This lookup will probably be achieved prior to the flight (i.e., prior to the logon phase) based on the knowledge of the corresponding flight plan information by the ground CM.

3. Retrieval and local caching of the aircraft's certificate by the ground CM.

---

[13]In that case, as for airborne BISs, there are two possibilities: either all ground-based BISs of that facility use the unique facility-based key pair, either each of those BISs uses its own dedicated key pair.

[14] Another possible scenario is based on the certificate passing in the logon request (the certificate corresponding to the aircraft would be passed to the ground CMA that should then only verify the certificate).

4. Logon response sent to the aircraft's CM signed by the ground CM and including the public keys (and encryption algorithm version number) of the other ground ATS applications of interest (e.g., CPDLC public key).

5. Ground CPDLC looks for the public key of its peer airborne CPDLC (i.e., the aircraft public key) held by its ground CM (by using local means).

6. The public key of the aircraft is provided by the ground CM to the ground CPDLC (by using local means).

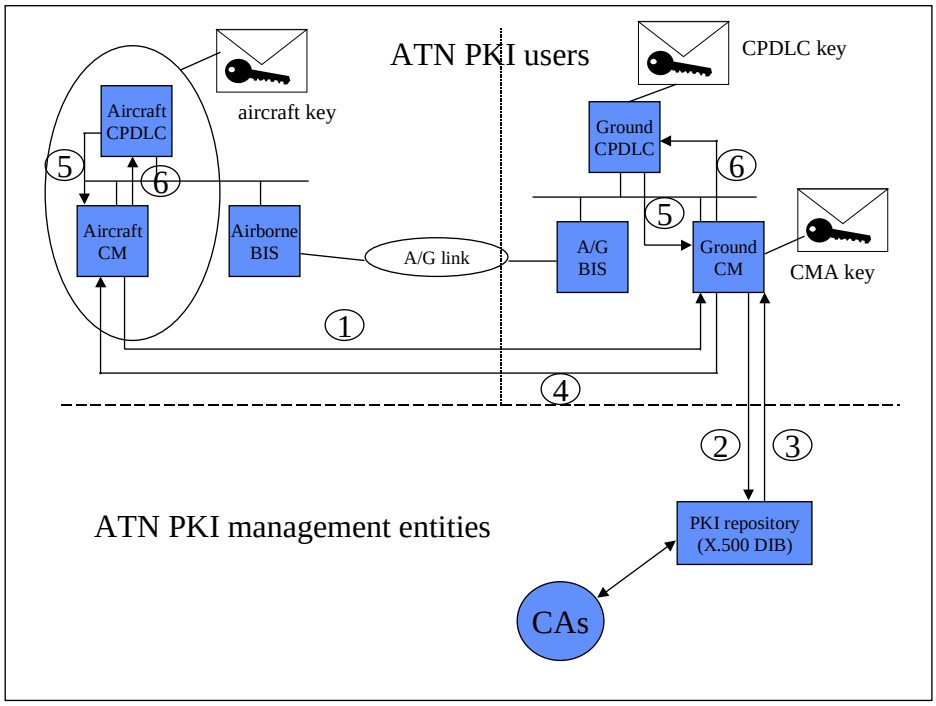

Figure 2: PKI operational model for signing AEs

The following description extends that model for a CPDLC dialogue:

7. The initiator of the CPDLC dialogue (i.e., either the ground or the airborne CPDLC AE) establishes the secured connection by specifying one of the four secured levels offered by the Dialogue. As peer authentication is required, this results in the sending of a connection establishment PDU (i.e., an ACSE AARQ PDU) whose authentication field holds user data signed by the initiator's private key.

8. Based on the received signed data, the receiver CPDLC authenticates the initiator using the initiator's public key that is already in the receiver's possession. It then responds by specifying an appropriate security level to the Dialogue service, that level being inferior or equal to the level specified by the initiator. This results in the sending of an response PDU (i.e., an ACSE AARE PDU) whose authentication field holds user data signed by the receiver's private key. The initiator is then able to authenticate the receiver by using the received signed data and the receiver's public key that is already in the initiator's possession.

9. If data origin authentication and data integrity are required for this dialogue (depending on the security level previously negotiated), data issued by the sending CPDLC (i.e., passed to the Presentation-Data Request primitive) can be signed using the sending CPDLC private key. The receiving CPDLC is then able to authenticate the origin and check the integrity of the received data by using the public key of the sending CPDLC.

The operational model for secured communications between ground AEs is assumed to be somehow similar: prior to the connection establishment, each signing AE would retrieve the certificate (and public key) of the remote communicating party by an appropriate lookup to the ATN PKI (the same lookup could be used for retrieving other informations such as the address of the remote entity).

The operational model for IDRP authentication is not ascertained since the way air-ground BISs retrieve the certificate of airborne BISs at the IDRP adjacency establishment is not yet defined. Several possibilities are envisioned: certificate passing at IDRP adjacency establishment, X.500 lookup made by the air-ground BIS or by CM on behalf of the BIS (via an appropriate BIS request to CM).

4.10.1.3 Management Model

The management model of the ATN PKI defines the operations between the various ATN PKI nodes for the management of the PKI infrastructure. This model is not yet fully described in the relevant ATNP documents since many issues regarding key management in general are still to be addressed.

The management operations can be realized using either on-line interactions (e.g., using the ATN communication services) or off-line procedures. Figure 3 illustrates the main entities and the essential interactions of the ATN PKI management model :

a) key pair generation/update: the key generator entity (which may be the user entity itself, its CA or a trusted third party) generates the key pair on behalf of the user and transmits the key pair to the user entity (a possibility exists whereby the public and possibly the private key when generated by a third party are securely communicated to the CA by the third party). The key pair is then confidentially stored by the key generator itself or by the end user's CA for a recovery purpose,

b) initial registration/certification or user-requested revocation :

- initial registration/certification is the process whereby a user entity makes itself known to its CA prior to the CA issuing a certificate for that user entity. This process should be completed after the user entity has been initialized (operation g) and after it has had its key pair generated unless this very process invokes the generation of the key pair by the CA in the case the CA is a key generator (operation a),

- revocation is the process whereby the user entity asks for its certificate to be revocated. Revocation can also be requested to the CA by other authorized entities (operation h),

c) certificate update: this operation is required whenever the key pair is updated, a new certificate being required from the responsible CA. For certificate updates, the CA must be communicated the new public key of the user entity either by the key generator (or the user entity provided with the new key) unless the CA itself is in charge of the key pair generation,

d) certificate/CRL posting: this is the process whereby a CA updates the PKI repository (i.e. the ATN X.500 DIT) by posting certificates or CRLs. This operation results from the initial certification (operation b), the public key update (operations a and c) or the revocation (operations b and h) of the user entity,

e) cross-certification : this operation results from the cross-certification agreements between different trusted CAs,

f) pre-flight loading of ground CM public keys[15] : this operation is required by aircraft-based user entities, potentially on a " per flight " basis, and results in the upload of the public keys of the ground CM entities contacted by the aircraft during its flight,

[15] This issue is similar to the one raised by the loading of the address of the initial CM.

g) PKI end user initialization : this is the process whereby a PKI user entity is securely initialized with appropriate ATN PKI data such as the identity of its CA, the CA's public key, etc.,

h) revocation : this operation results from an authorized entity asking for the revocation of the user entity and causes the appropriate update of the repository (operation d),

i) key pair recovery: this operation results from a user entity asking to recover its private key to the management entity in charge of key recovery functions which may be the key generator itself or the CA of the user entity.

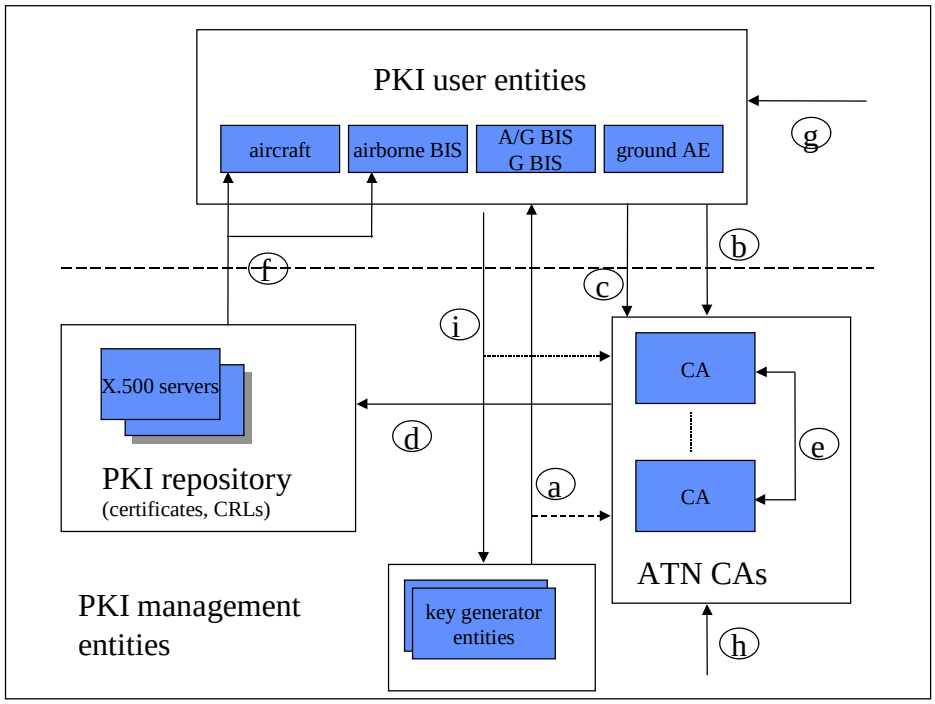

Figure 3: ATN PKI management model

The PKI management operations may be accomplished on-line (e.g., by using ATN communication services) or off-line (e.g., by non-electronic means).

4.10.2 PKI Architecture for the ACCESS area

4.10.2.1 Introduction

This section proposes a possible architecture for the European ATN PKI required in the ACCESS area. This architecture is to be intended as a proposition based on draft ATNP material and on assumptions that need to be further verified. Consequently this proposition is likely to be modified and refined in accordance with the expected developments or modifications of the ATN security recommendations.

4.10.2.2 PKI X.500 Repository

4.10.2.2.1 General

The PKI repository is used for storing and distributing certificates and CRLs to PKI user entities (BISs or ATN application entities).

The following assumptions are made with regard to the PKI repository:

- it will be implemented as a X.500 directory : the X.500 DIT will be structured so as to provide entries unambiguously identified by the distinguished names of the PKI user entities and of the management entities (CAs) :
    - X.509 certificates will be stored as attributes of the DIB entries identifying the corresponding PKI user entities,
    - CRLs will be stored as attributes of the DIB entries identifying the corresponding CAs,
- it will be based on a distributed architecture: the global ATN X.500 directory will be made of several directory domains, each domain being managed by a given organization and composed of one or more DSAs and of zero or more DUAs. The domains can be split into sub-domains composed of one of the domain DSAs at a minimum and of subgroups of the domain DUAs,
- it will be somewhat hierarchically organized, so that it is considered the ACCESS area can be served by a European ATN directory, part of the global ATN directory (this European ATN directory can be then split into several sub-domains),
- the X.500 directory used as the PKI repository could hold other data non related to security (e.g., addressing, naming) and thus will be part of a global ATN directory.

Although CAs must be unambiguously identified by a directory entry, it is not necessary that the CA structure as exposed in Section 4.10.2.3 are related to the DIT structure.

4.10.2.2.2 Proposed Architecture

The operational models previously described have the following consequences:

- X.500 lookups are only initiated by ground-based DUAs[16], which potentially are ground CMs, air/ground BISs, ground BISs or ground-only application entities,
- there is no need for airborne DUAs or DSAs,
- as the ATN directory is distributed, any DSA will hold a part of the overall ATN DIB and DSAs will interact with each other to carry out the DUA request in case the request cannot be answered by the initially accessed DSA (using chained requests or referrals).

There are several scenarios for the use of DUAs and DSAs in the X.500 architecture with respect to PKI requirements:

- DUAs :
    - one DUA per "requester", i.e. one DUA per ground CM and one DUA per air/ground or ground BIS,
    - one DUA serving several "requesters", e.g. one DUA per facility accessed by the requesters using specific protocols : a typical example of that scenario is the implementation of an X.500 DUA integrated to the ground CM and serving the local air/ground or ground BISs,

[16]According to the operational model, the public keys of ground-based AEs required by airborne AEs are retrieved from the logon response. Additionally as air-ground BISs are not authenticated by airborne BISs, airborne BISs do not need to retrieve certificates from the directory for IDRP authentication. Consequently there is no need for an airborne X.500 DUA or DSA: the only exception may arise if the pre-flight loading of certificates into the airborne CM is realized using X.500 lookups from an airborne DUA as the aircraft is parked and connected to the Gatelink subnetwork of an airport facility.

- one DUA per ground-based PKI end user (i.e., ground CM + A/G BIS + ground BIS + each ground-based AE) : this scenario is adapted to solutions based on the integrated ground CM-X.500 DSA (interactions between ground CMs and their user AEs are X.500 lookups in that case),

- DSAs :

  - integrated ground CM-X.500 DSA : in that case the database of certificates/public keys held by the ground CM can be a subset of the local DIB hold by the DSA and CM-user AEs can interact with CM using X.500 lookups,

  - X.500 DSA not integrated to ground CM (e.g., one DSA per facility directly accessed by local DUAs and remote DSAs).

In any case it is necessary to define the DIT, the number and the location of the DSAs, the part of the overall DIB hold by each DSA (the local DIB), the DUAs served by each DSA and the relationships between the DSAs for carrying out chained requests (hierarchical or meshed architectures): those definitions must not be bound to security considerations only, as the assumed scope of the ATN directory is not limited to the PKI repository.

The following propositions are made regarding a possible X.500 architecture for the ACCESS area:

- a global ATN X.500 DIT provides any PKI user or management entity with a specific entry identified by the X.500 distinguished name of the entity[17]and that appropriate mechanisms in the DUAs allow to build the X.500 distinguished name corresponding to :

  - the (remote) airborne user entity, based on the knowledge of previously acquired identification parameters related to flight plan information or on the aircraft or flight identification parameters present in the logon request (in that latter case the X.500 lookup would be chained to the logon request),

  - the (remote) BIS, based on the knowledge of previously acquired identification parameters related to flight plan information or on the NET of the airborne BIS, in the case of IDRP authentication requiring X.500 lookups (in the latter case the X.500 lookup would be chained to the IDRP adjacency establishment process),

- the X.500 DIT is structured in order to fit to organizational boundaries between the various actors of the ATN network :

  - X.500 object entries associated to ground signing entities of a given ATSO will all be placed "under" a common DIT node identifying that ATSO,

  - X.500 object entries associated to airborne signing entities will be placed "under" a common DIT node exclusively identifying airborne entities, whether ATSC or AOC (i.e., a “Airlines-level” top node with possible subordinate nodes identifying the various airline companies),

- the DSA architecture is basically based on the interconnection of :

[17]Currently available ATN SARPs do not specify any ATN X.500 DIT, whereas naming specifications are provided for ATN Application Entities. The ATN X.500 DIT will not necessarily coincide with the application-level naming tree (i.e., a given AE, identified by its AE Title as specified by the naming tree of the relevant SARPs, will be identified in the X.500 directory by an X.500 distinguished name which will not be its AE Title).

  - one DSA at least per ATSO (see [A203]) providing its national DUAs with an access to the global directory (this is required for organizational reasons as each organization is supposed to be responsible for the operation of the part of the global DIB containing its own objects),

  - one DSA at least per Airline, managed by or on behalf of that Airline, able to resolve the requests for airborne signing entities present in its aircrafts,

  - (optionally) “top level” regional ATC DSAs able to route X.500 lookups between ATSO-level directory domains within the region or between any ATSO directory domain and Airline domains or other regions’ domains,

  - (optionally) “top level” Airline DSAs, managed by or on behalf of groups of Airlines (e.g., by IACSPs), able to resolve the requests for airborne signing entities or route them to the appropriate Airline DSA,

- some ATSOs will probably require more than one DSA for both organizational and operational reasons (DIB decentralization allowing better scaling and management, performance related to the DSA use, etc.): one DSA per ACC is a likely solution for such national networks in Europe (e.g., France, Germany, Italy, etc.),

- DUAs access the directory by sending their requests to the DSA of the corresponding ATSO: performance optimizations are possible by having DUAs forwarding their requests directly to the upper level DSAs (such as a European ATC Region DSA or an global Airlines DSA if existing) when looking for entries related to airborne signing entities.

Figure 4 depicts a possible scenario for an ATN European X.500 directory, where “top level” regional DSAs are used:

- normal lines represent a possible set of chaining relations between DSAs : they make up the longest path used for routing an X.500 request in the context of a ground user entity retrieving a certificate associated to an airborne user entity,

- dotted lines show possible optimizations for the chaining of X.500 requests in the context previously described,

- double arrows represent possible "horizontal" optimizations that could be useful for ground user entities looking up for other ground user entities.

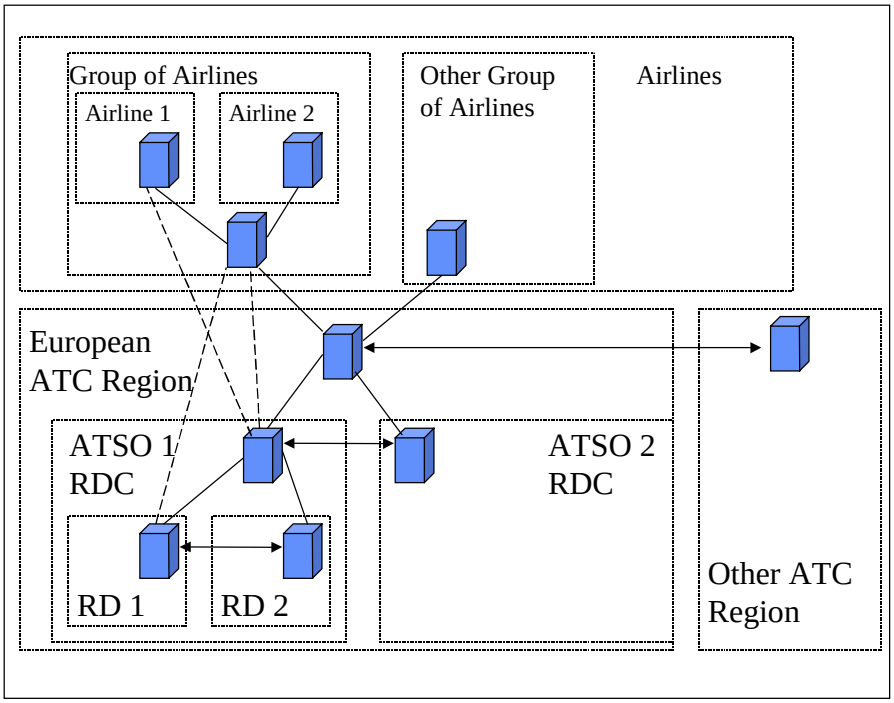

Figure 4: European PKI X.500 repository architecture (example)

As most of the X.500 lookups induced by the ATN security operation will be initiated by ground signing entities to get security information regarding airborne signing entities, most of the lookups will be resolved by chaining or referral operations between multiple DSAs across different administrative domains. Depending on the directory architecture, they may successively involve a local ACC DSA, a national ATSO DSA, a European-level ATC DSA and finally one or more Airlines DSAs. In any case the induced interactions between the requesting DUA and the various DSAs or between the DSAs themselves should be relatively limited so as to ensure acceptable performance.

In conclusion, performance considerations, taking into account DSA processing burden and X.500 chaining performance, must be balanced with the decentralized management and the scalability of a distributed architecture to get an acceptable X.500 architecture. This aspect is particularly important for the operation of the ATN security, as most resulting X.500 lookups will span different administrative domains.

4.10.2.3 Certificate Authorities

4.10.2.3.1 General

In order for a user entity to trust the authentication procedure achieved by the ATN security mechanisms, it shall obtain the other user's public key from a source that is trusts. Such a source is a Certification Authority (CA), which produces certificates ensuring the validity of the association between a user (identified by its distinguished name) and its corresponding public key. Certificates are digitally signed by the issuing CA (which make them unforgeable) and posted by the CA to a directory that users having the public key of the CA can access to retrieve and verify the certificates.

The basic role of CAs is therefore to ensure the binding between user entities and their corresponding public keys. A CA can be formally defined as an entity named in the issuer field of a certificate.

A user that needs the public key of a "remote" user must first obtain the certificate of that user (signed by the remote user's CA). If the remote user's CA is not known and/or trusted by the requesting user, it must then obtain the certificate of the remote user's CA to get the CA public key. This process may be

repeated several times, as chain of multiple certificates may be needed to prove the validity of a single public key association (i.e., the public key associated to the "remote" user). This chain of certificates is identified as a certification path. Somewhere in the path a trusted association must be initiated for each user: the user entity must be certified by "its" CA and be initialized by local means with the public key of "its" CA. Certification paths may be hierarchical or distributed. There is no need for a single top CA as bilateral agreements can be established between pairs of CAs: a CA would then certify its peer CA by issuing a certificate associated to it (cross-certification).

As presented in [GUID], an ATN CA is a trusted entity that:

- associates a unique name with an ATN entity,
- joins that name with the public key associated to that ATN entity in a certificate,
- verifies the association through digitally signing the information contained in that certificate,
- makes certificates available to its users,
- is responsible for the creation, modification and distribution of Certificate Revocation Lists (CRLs) which are used to disseminate information regarding entity/public key association that have become invalid (certificates are issued for a given lifetime).

It is therefore the responsibility of the CA to set up procedures to verify the truth of the associations they certify (e.g., using physical presence or "demonstration of identity" procedures), to strongly protect the private keys it uses, to make its own public keys widely available and to set agreements with other CAs.

It has to be noted that CAs may be in charge of additional tasks such as key generation for example.

4.10.2.3.2 ATN Certificate Policy

The policies used by a CA for issuing a certificate are indicated in the certificate. The certificate may optionally include a pointer to a Certification Practice Statement (CPS), which is a detailed statement by a CA as to its practices employed for issuing certificates.

A certificate policy refers to the way a certificate indicates to a user whether or not the certificate is suitable for use for a particular application purpose: it consists of a set of rules relating to the issuing and use of certificates and certified public keys by a given community of users for a particular application context.

The CPS published by a CA can conform to more than one Certificate Policy.

The applicable ATNP documents will define an ATN Certificate Policy: CAs used in the ATN PKI will be required to have their CPS conformant to the ATN Certificate Policy. Organizations or states participating to the ATN shall set audit procedures to verify the CA practices with respect to the ATN Certificate Policy.

4.10.2.3.3 Proposed Certification Authority Structure

Due to its distributed architecture and its international extent, different multiple CAs will be required for the operation of the overall ATN PKI.

ATN CAs will have to maintain relationships among themselves (e.g., cross-certifications) such that one CA will be able to obtain the certification path between itself and the CA responsible for a given user's certification: the set of those CAs and their relationships will make up the ATN CA structure.

It is agreed that this structure will not be based on a unique top level CA for the overall ATN but rather on a highest tier of CAs having peer relationships established through bilateral or multilateral agreements (CAs under that highest tier may be organized hierarchically).

ATN CAs may be operated by or on behalf of the various organizations or states participant to the ATN, provided they comply with the ATN Certification Policy.

Figure 5 proposes a likely CA structure for the operation of the European ATN: it is based on the assumption that the highest tier of CAs will be found at a state/organization level, particularly for administrative and/or institutional reasons. This gives a “flat” distributed structure (one CA per ATSO and one CA per Airline), which does not preclude an organization from using multiple CAs for its own users (see ATSO 2 in the figure).

The structure represented in the following figure is a functional view of the structure: it can be envisioned that a single entity act as the actual CA for different organizations.

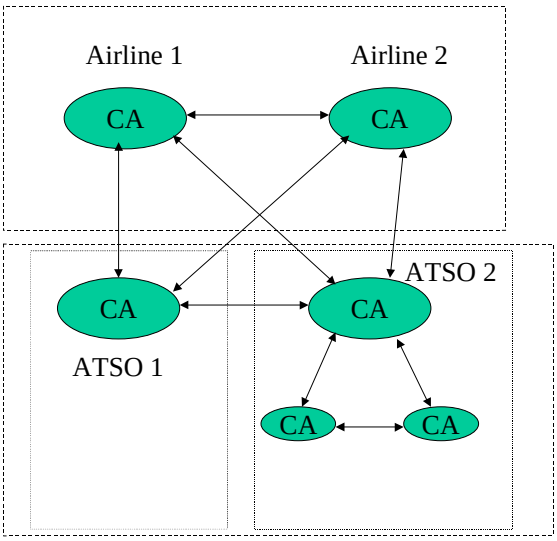

Figure 5: ATN CA structure (example)

4.10.2.4 Key generators

Current ATNP applicable documents do not make any recommendation about the identity of key pair generators. Moreover the lifetime of key pairs is not well established: the only recommendation states that key pairs for aircrafts shall be valid for the entire duration of a flight at a minimum.

One possible scenario is exposed hereunder:

- airborne entities: the key pair for a given aircraft could be generated by a specific on-board process, whose initiation remains to be defined,
- ground entities: key pairs could be generated by the respective national CAs.

4.10.3 PKI Security Provisions for the ACCESS area

4.10.3.1 Introduction

This chapter describes the main security provisions that are required for the operation of the PKI architecture as previously exposed.

The first subsection reminds the general security provisions that are applicable to all PKI management systems (CA systems, X.500 DSAs, etc.). The following subsections extend the general provisions or present specific provisions to be applied to identified PKI elements.

As PKI management operations are not fully addressed by the current applicable ATNP documents, both on-line and off-line alternatives should be considered for the actual implementation of the security provisions related to those operations.

4.10.3.2 PKI Systems

The general related provisions as expressed in Table 3 that are globally applicable to main PKI systems are reminded below.

GP1	Physical protection of ATN resources (including ATN PKI resources)
GP2	User access control to ATN resources (including ATN PKI resources)
GP3	Appropriate ATN system administration procedures
GP4	Appropriate training procedures
GP5	Provisions reducing single points of failure (including ATN PKI single points of failure)

4.10.3.3 PKI X.500 Directory

The general provision specifically applicable to the X.500 directory is reminded below.

GP13	Key/certificate management secured procedures and/or mechanisms

This general provision shall be applied to the X.500 directory as follows:

- access to the repository for certificate retrieval shall be limited to ATN user entities only. There are several technical possibilities ranging from simple password-based authentication to strong authentication mechanisms as described in ISO 9594-8 (consequently DUAs will have to be authenticated by the DSAs),

- posting of certificates or CRLs to the X.500 directory by CAs shall be authorized to ATN CAs only, e.g. by using X.509 strong authentication mechanisms if the posting of certificates is achieved on-line (CAs modify X.500 entries when posting a certificate to the directory).

The general provision about user access control shall be particularly applied to the individual X.500 DSAs by restricting the access of the databases to only authorized users, especially for creation or modification access rights.

4.10.3.4 Certification Authorities

The general provisions specifically applicable to the ATN CAs are reminded below.

GP12	Establishment and enforcement of ATN certification procedures and security means applicable to ATN CAs
GP13	Key/certificate management secured procedures and/or mechanisms
GP14	Private key protection measures

The first of these three general provisions means that:

- assuming an ATN Certification Policy has been defined, ATN organizations (i.e., Airlines, ATSOs) will have to ensure that their CAs do conform with that policy. This can be accomplished by making periodic audits of the CA certification practices or by any other means aiming at controlling the CA activity for the ATN community,

- as particularly strong security measures are required for protecting CA systems from identified threats (e.g., protection of the CA private key), it is the responsibility of the ATN organizations to check whether the security measures employed by the CA are deemed appropriate.

The second general provision (GP13) is potentially applicable to all management operations involving ATN CAs, whether made on-line or off-line: it is not actually possible to define precise mechanisms or procedures to that purpose because they will highly depend on the way those operations are achieved (i.e. on-line or off-line) and because they are not yet fully specified by ATNP recommendations. An example of such a precaution is related to the initial communication of its private key to the key holder, which shall be protected from interference and disclosure since this, is a very critical information (e.g., by using encryption techniques).

The third general provision (GP14) will be treated in the next section.

4.10.3.5 Private Key Protection

The general provision concerning this specific aspect induced by the use of a public key cryptosystem is reminded below.

GP14	Private key protection measures

This general provision is applicable to:

- ATN security user entities (if they locally store their private key),

- ATN PKI management nodes implied in the key pair generation process. In principle only the key pair holder is supposed to hold its private key : if the key pair has been generated by another entity (e.g., its CA), then the private key should be deleted from the records of the key generator (unless specific arrangements are set, e.g. for recovery purposes) once communicated to its intended holder : this should be ensured by appropriate measures,

- ATN CAs which must strongly protect their own private keys from disclosure.

The use of automated encryption tools (e.g., password-based encryption algorithms) can be used to protect the locally stored private keys.

The use of "secret-splitting" schemes can be additionally used to protect CA private keys (that type of scheme requires some combination of several private keys held by different persons to access the private key storage, thus preventing any single person to "steal" the CA private key).

4.11 Security Management

4.11.1 Scope

Security management encompasses all actions pertaining to the management of the security program, which is essentially made of the set of measures selected to meet the objectives, defined by the security policy.

Security management includes the following aspects:

- security audit, which permits to evaluate the adequacy of the security policy by aiding in the detection of the attacks, the identification of the attackers and the evaluation of the effectiveness of the security measures,
- actions aimed at preventing security violations,
- actions/procedures to be taken in response to security violations, which range from immediate recovery actions to off-line analysis actions and possible procedures for modifying the current security measures,
- organizational aspects, that must be defined to support the actions undertaken in the security area.

The security management provisions presented in that section will be focused on security audit as the other aspects are not specific to the ATN security framework.

4.11.2 Security Audit Provisions

The general related provision as expressed in Table 3 is reminded below.

GP11	Security management provisions for recording and analyzing security violations	All

As presented in Annex B of [WG3/UPP], security audit concentrates on:

- the detection of events which are considered as abnormal in the frame of security,
- the recording of such events,
- the analysis of the collected events.

Security audit mechanisms will provide objects and functions to support the access control policy (e.g., access to PKI repository), the monitoring of security threats affecting both the ATN and the ATN PKI and the reporting and/or storing of security violations.

This should be accomplished by:

- having ATN resources subject to security precautions (including ATN PKI nodes) able to locally detect security events and discriminate the events in order to generate an audit record or a security alarm (e.g., issued to a network management station),
- using alarm processing systems, that can initiate actions depending on the alarm criticality,

- using audit record processing systems, that have the capability to gather and consolidate audit record and produce reports for off-line analysis,

- using archiving systems.

The mechanisms used to that purpose will probably be based on ISO standards pertaining to network management, particularly to ISO 10164-4 (System Management: Alarm Reporting Function), ISO 10164-5 (System Management: Event Report Management Function, ISO 10164-6 (System Management: Log Control Function) and ISO 10164-7 (System Management: Security Alarm Reporting Function).

They shall therefore be included in the ACCESS network management framework defined in [A227].

5. Organizational and Institutional Aspects

This section of the document has not been developed.

However elements regarding those institutional aspects raised by the operation of the ACCESS ATN in general are provided in [A224].

6. Conclusion

The first step required for the definition of useful and effective security precautions applicable to the European ATN is the identification of the threats to be countered: one of the main difficulties in the ATN context arises from the fact that there is no current operational ATN, so there is no experience of attacks to the ATN from which that identification would be solidly established (the attacks affecting existing “public” networks such as the Internet usually give an effective and continuous input to the identification and prioritization of the threats that need to be countered).

Consequently the threats retained for the proposition of security precautions are rather extracted from ATNP analysis based on a priori assumptions rather than on effective experience of security violations, which makes harder any cost/benefit analysis and any following prioritization of the proposed precautions.

That is why it is difficult at that stage to focus on specific precautions amongst the ones presented in Chapter 4. As soon as the ATN will be effectively deployed, it will be particularly important to set procedures and appropriate resources for an effective security audit in order to evaluate the accuracy of the ATN security policy and the derived countermeasures.

Furthermore, as the proposed technical precautions are mainly based on draft ATNP recommendations which are either uncomplete or susceptible of modifications or enhancements, their application to the European ATN will have to be refined and detailed as the applicable ATNP recommendations will be finalized, especially those concerning the ATN public key infrastructure and the ATN directory.

The implementation of many precautions will require prior actions in diverse areas ranging from organizational aspects to technical frameworks necessary for the operation of the security mechanisms (e.g., the network management framework).

Those considerations together with the fact that some essential security mechanisms (i.e., those using the ATN public key cryptosystem) will not be available with CNS/ATM 1 packages call for a phased implementation strategy where only a subset of the proposed precautions will be implemented in the initial ATN (by the year 2005). That phased implementation should be addressed by the ACCESS work package WP240 (Transition Issues).

In any case many precautions are implementable in a first phase, such as physical protection, user access control, availability and some subnetwork-level provisions, etc., provided an adequate organization and common procedures will have been established among the different actors of the European ATN, especially for the operation of the “backbone” ATN resources.

Appendix A - Acronyms

AAC	Aeronautical Administrative Communications
ACARS	Aircraft Communications Addressing and Reporting System
ACC	Area Control Center
AFTN	Aeronautical Fixed Telecommunication Network
AIS	Aeronautical Information Service
AMHS	ATS Message Handling System
AOC	Aeronautical Operational Communications
APC	Aeronautical Passenger Communications
ATC	Air Traffic Control Center
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATS	Air Traffic Services
ATSC	Air Traffic Services Communications
ATSO	Air Traffic Services Organisation
BIS	Boundary Intermediate System
CA	Certification Authority
CAA	Civil Aviation Authority
CAO	Commercial Aircraft Operator
CFMU	Central Flow Management Unit
CLNP	Connection-Less Network Protocol
CPS	Certification Practices Statement
CRL	Certificate Revocation List
EATCHIP	European Air Traffic Control Harmonisation and Integration Programme
EATMS	European Air Traffic Management System
ECAC	European Civil Aviation Conference
ENOC	European Network Operating Concept
ES	End System
GDLP	Ground Data Link Processor
GES	Ground Earth Station
IACSP	International Aeronautical Communications Service Provider
ICAO	International Civil Aviation Organisation
IDRP	Inter Domain Routing Protocol
IS	Intermediate System
METAR	Meteorological Actual Report
NSAP	Network Service Access Point
OSI	Open System Interconnection
PKI	Public Key Infrastructure

PSN	Packet Switched Network
QoS	Quality of Service
RA	Registration Authority
RD	Routing Domain
RDC	Routing Domain Confederation
SARPs	Standard And Recommended Practices
SIGMET	Significant Meteorological Information
SM	System Management
TAF	Terminal Area Forecast
VDL	VHF Digital Link
WAN	Wide Area Network

Appendix B – Example scenarios for the ATN security concept of operations (extracted from [GUID])

Security Scenario 1 (aircraft, ground CM and ground CPLDC all support ATN security provisions)

1. Aircraft Context Management Application (CM) either has:

a. pre-stored a data base of ground CM addresses, corresponding public key and encryption algorithm version number; or

b. received an upload of current CM address, corresponding public key and encryption algorithm version number from a trusted airline/service provider ground host

2. Aircraft's CM requests a secure dialog then sends CM log-on to ground CM, message includes the aircraft's digital signature.

3. Ground CM accesses X.500 server (ground-ground) to obtain the security certificate (X.509) for the aircraft that has send the CM logon.

4. Ground CM enters the X.509 certificate along with the CM logon information into its data base (potentially the data base used by CM is actually the X.500 data base where CM is fully integrated with an X.500 server).

5. Ground CM generates CM logon response message that includes the ground CM's digital signature and includes the public key and encryption algorithm version number for the other ground ATS applications of interest (e.g., the information of the controlling ATS facility). This would be in addition to the other CM version 1 information (e.g., network address) for each ground application.

6. Ground ATS applications (e.g., CPDLC) desiring to communicate with an aircraft must first access the ground CM server (or potentially an X.500 server where the ground CM is integrated with an X.500 server) and retrieve the aircraft's address and X.509 certificate information. CM server access should be restricted to authorized users (i.e., authentication services between CM server and CM users.

7. A ground ATS application (e.g., CPDLC) would include its digital signature with messages sent to the aircraft.

8. Aircraft would include its digital signature with messages sent to ground ATS applications.

9. The CPDLC ground application would include security information (public key and encryption algorithm version number) for the next ATC facility's CPDLC application as part of the next data authority message sent to the aircraft before handoff to the next ATC facility.

Security Scenario 2 (aircraft supports ATN security services but ground CM does not)

1. Aircraft CM either has:

a. pre-stored a data base of ground CM addresses, corresponding public key and encryption algorithm version number (when applicable); or

b. received an upload of current CM address, corresponding public key and encryption algorithm version number (when applicable) from a trusted airline/service provider ground host

2. Aircraft, for this scenario, has ground CM address but no public key information. Aircraft CM requests an unsecured dialog service and then sends a logon request, without any security provisions (i.e., no digital signature).

3. An unsecured dialog will be established between the aircraft CM and the ground CM.

4. Ground ATS applications (e.g., CPDLC) desiring to communicate with an aircraft must first access the ground CM server and retrieve the aircraft's address information. Since in this scenario the ground CM does not support ATN security services, the ground ATS applications, relying on this CM server, would only be able to request or accept an unsecured dialog because they would not have access to the necessary key information to allow the use of digital signatures.

Security Scenario 3 (aircraft does not support ATN security services but ground CM and ATS applications do support ATN security services)

1. Aircraft CM either has:

a. pre-stored a database of ground CM addresses: or

b. received an upload of current CM address from a trusted airline/service provider ground host

2. Aircraft CM requests a dialog (unsecured) and then sends a logon request, without any security provisions (i.e., no digital signature in ACSE header).

3. Ground CM receives CM Logon request, looks at the aircraft's CM version number. If the aircraft and ground CM are at the same CM version number then the logon and exchange of address information proceeds as per the normal process specified by the Doc 9705.

4. If the Ground and aircraft's CM are at a difference version numbers then the later version reverts to a mode compatible with the earlier version of CM, as specified by the Doc 9705. In this case the ground CM would operate in a mode interoperable with the aircraft's earlier CM version.

5. Since the aircraft version of CM does not support ATN security services then the ground CM registers the aircraft within its database as not receiving secured services. Therefore there would be no attempt to retrieve the X.509 certificate for the aircraft nor security information (e.g., public key) included in the CM data base entry for this aircraft. Potentially the database used by the ground CM is actually the X.500 database where CM is fully integrated with an X.500 server.

6. Ground ATS applications (e.g., CPDLC) desiring to communicate with the aircraft must first access the ground CM server and retrieve the aircraft's address information. Since in this scenario the ground CM data base entry for the aircraft will indicate that ATN security services are not to be provided, the ground ATS applications would only be able to request or accept an unsecured dialog with this aircraft.

Security Scenario 4 (aircraft and ground CM support ATN security provisions, but one or more ground ATS applications do not)

1. Aircraft CM either has:

a. pre-stored a data base of ground CM addresses, corresponding public key and encryption algorithm version number; or

b. received an upload of current CM address, corresponding public key and encryption algorithm version number from a trusted airline/service provider ground host

2. Aircraft CM requests a secure dialog and then sends CM log-on to ground CM, message includes the aircraft's digital signature.

3. Ground CM accesses X.500 server (ground-ground) to obtain the security certificate (X.509) for the aircraft that has send the CM logon.

4. Ground CM enters the certificate along with the CM logon information into its data base (potentially the data base used by CM is actually the X.500 data base where CM is fully integrated with an X.500 server).

5. Ground CM generates CM logon response message that includes the ground CM's digital signature and includes public key and encryption algorithm version number for the other ground ATS applications (in addition to the other CM version 1 information for each ground application). Ground ATS applications not supporting ATN security services would so be indicated (i.e., no public key provided).

6. Ground ATS applications (e.g., CPDLC) desiring to communicate with an aircraft would first access the ground CM server and retrieve the aircraft's address and security certificate information. For ground ATS applications supporting security services the scenario is the same as scenario 1. For ground ATS applications not supporting ATN security services, the ground CM would need to provide the aircraft information in a format compatible with the ground ATS application.

7. Ground ATS applications (e.g., CPDLC) not supporting security services could only initiate or accept unsecured dialogs to/from the aircraft

Appendix C – Certification Path Examples

This appendix illustrates the certification path concept with appropriate examples which are extracted from ISO/IEC 9594-8 (ITU-T Rec.X09) 1993 Edition.

X.509/Figure 4 illustrates a hypothetical example of a DIT fragment, where the CAs form a hierarchy. Besides the information shown at the CAs, we assume that each user knows the public key of its certification authority, and its own public and private keys.

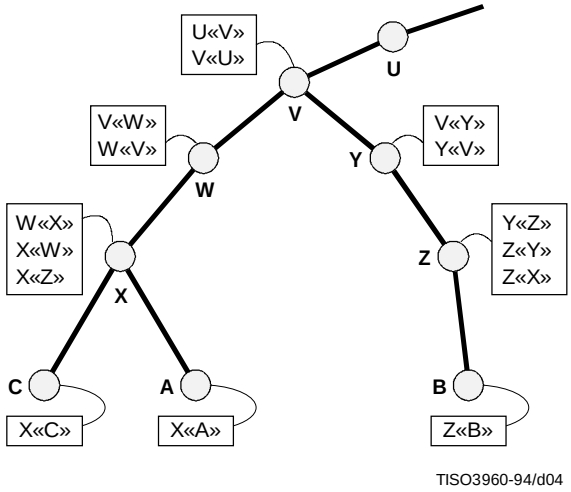

Figure 4 – CA hierarchy – A hypothetical example

If the CAs of the users are arranged in a hierarchy, A can acquire the following certificates from the Directory to establish a certification path to B:

X“W”, W“V”, V“Y”, Y“Z”, Z“B”

When A has obtained these certificates, it can unwrap the certification path in sequence to yield the contents of the certificate of B, including Bp:

Bp = Xp • X“W” W“V” V“Y” Y“Z” Z“B”

In general, A also has to acquire the following certificates from the Directory to establish the return certification path from B to A:

Z“Y”, Y“V”, V“W”, W“X”, X“A”.

When B receives these certificates from A, it can unwrap the return certification path in sequence to yield the contents of the certificate of A, including Ap:

Ap = Zp • Z“Y” Y“V” V“W” W“X” X“A”

Applying the optimizations of *[X509 Section 8.1]*:

a) taking A and C, for example: both know Xp, so that A simply has to directly acquire the certificate of C. Unwrapping the certification path reduces to:

Cp = Xp • X“C”

and unwrapping the return certification Path reduces to:

$$Ap = Xp \bullet X\text{“}A\text{”}$$

b) assuming that A would thus know W“X”, Wp, V“W”, Vp, U“V”, Up, etc. reduces the information which A has to obtain from the Directory to form the certification path to:

V“Y”, Y“Z”, Z“B”

and the information which A has to obtain from the Directory to form the return certification path to:

Z“Y”, Y“V”.

c) assuming that A frequently communicates with users certified by Z, it can learn (in addition to the public keys learned in b) above) V“Y”, Y“V”, Y“Z”, and Z“Y”. To communicate with B, it need therefore only obtain Z“B” from the Directory.

d) assuming that users certified by X and Z frequently communicate, then X“Z” would be held in the directory entry for X, and vice versa (this is shown in X.509/Figure 4). If A wants to authenticate to B, A need only obtain:

X“Z”, Z“B”

to form the certification path, and:

Z“X”

to form the return certification path.

e) assuming users A and C have communicated before and have learned one another’s certificates, they may use each other’s public key directly, i.e.

$$Cp = Xp \bullet X\text{“}C\text{”}$$

and

$$Ap = Xp \bullet X\text{“}A\text{”}$$

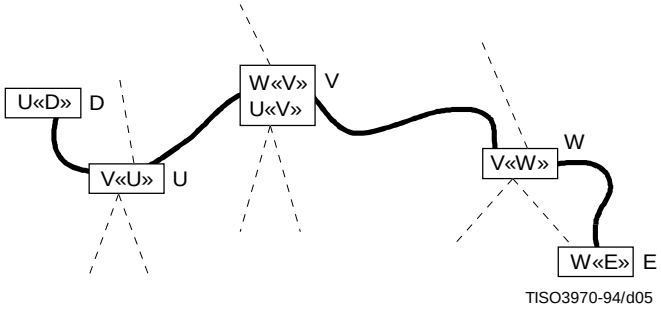

Figure 5 – Non-hierarchical certification path – An example

In the more general case the Certification Authorities do not relate in a hierarchical manner. Referring to the hypothetical example in X.509/Figure 5, suppose a user D, certified by U, wishes to authenticate to user E, certified by W. The Directory entry of user D shall hold the certificate U“D” and the entry of user E shall hold the certificate W“E”.

Let V be a CA with whom CAs U and W have at some previous time exchanged public keys in a trusted way. As a result, certificates U“V”, V“U”, W“V” and V“W” have been generated and stored in the Directory. Assume U“V” and W“V” are stored in the entry of V, V“U” is stored in U’s entry, and V“W” is stored in W’s entry.

User D must find a certification path to E. Various strategies could be used. One such strategy would be to regard the users and CAs as nodes, and the certificates as arcs in a directed graph. In these terms, D has to perform a search in the graph to find a path from U to E, one such being U“V”, V“W”, W“E”. When this path has been discovered, the reverse path W“V”, V“U”, U“D” can also be constructed.