ATNP/WG2
ATNP/WG3

FLIMSY __________________

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL(ATNP)

WG2/WG3

23 June – 26 June 1997
Langen, Germay

Presented by : Rapporteur WG1

INTRODUCTION

The attached WP's are to be presented to WG1 next week so they do not have official acceptance at this time. It is necessary, however, that they be seen by WG2/WG3 prior to the WG1 meeting so that they can be incorporated into your work planning. I do not anticipate any major changes to their content but if this occurs, you will be immediately notified prior to the end of the WG1 meeting next week.

RECOMMENDATION

WG2/WG3 are requested to review the papers and indicate to WG1, which areas of the SARPs will be impacted and whether or not your WG will be able to accomodate the workload to have the SARPs completed in time for ATNP/3

ATNP/WG1
WP 9-5

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL(ATNP)

WG1 – SYSTEMS PLANNING AND CONCEPT WORKING GROUP

30 June – 3 July 1997
Langen, Germay

Security Strategy for the ATN

Presented by Ron Jones

Summary

This working paper proposes a high level security framework for the ATN and proposes an approach by which the ATNP working groups can progress their work program in this area.

References:

1. WG1/WP6-10 Security Concept ATNP/2 (WG1 Standing Document)
2. WG1/WP6-11 Overall Security Concept
3. ITU-T Rec. X.500, Information Technology – Open Systems Interconnection – The Directory: Overview of Concepts, Models, and Services
4. ITU-T Rec. X.509, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
5. IETF RFC 1421 (Proposed Standard), Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authenication Procedures
6. IETF RFC 1422 (Proposed Standard), Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management
7. IETF RFC 1423 (Proposed Standard), Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers
8. IETF RFC 1423 (Proposed Standard), Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services
9. IETF RFC 2120 (Experimental Protocol), Managing the X.500 Root Naming Context

10. IETF RFC 2144 (Information Paper), The CAST-120 Encryption Algoritm

Attachment A: Sources for information on X.500/X.509

1. Introduction

Working Group 1 of ATNP was given a work item by ATNP/2 to "develop a security strategy for the ATN including a plan for the administration of the security features." This is a continuation of work started prior to ATNP/2 which lead the creation of a standing document for the ATN Security Concept (ref. 2). Reference 1 was a working paper prepared by WG1 at its meeting in Halifax and submitted to ATNP/2. This latter working paper provides an overview of the results of work documented in reference 2 and recommends the following work items:

1. *The safety and security implications of unauthorized interference with user messages and IDRP messages containing routing information should be further investigated in the context of the operation of the ATN.*

2. *Based on the above investigation, the use of a cryptographic check sum to protect user messages and IDRP messages containing routing information should be investigated, and appropriate SARPs and Guidance Material developed.*

3. *Guidance material to States and Organisations on how to address the administrative and organisational issues of key generation, distribution and management associated with any cryptographic security solution should be developed.*

2. Discussion

2.1 Background

Based on previous work of WG1 and its members, the following reference baseline security policies were proposed (reference 1):

1. *Communication monitoring and third party traffic analysis - neither of these constitute a safety hazard, so there is no need to guard against them.*

2. *Data link messages shall be protected from modification, masquerade and replay - that means that for data messages between aircraft and air traffic control centres there will be a high level of assurance that a message comes from where it claims, has not been tampered with, and is not a repeat of an obsolete message.*

3. *Messages for the purpose of network management, and the messages that carry routing information shall be protected from modification, masquerade and replay - that means that there will be a high level of assurance that no unauthorised entity can modify the routing characteristics of the ATN.*

4. *The services that support messages to and from the aircraft shall be protected against denial of service attacks to some (to be specified) level of probability - this means having alternative communications paths available in case one path gets jammed.*

5. *ATN Hosts and routers shall be protected from unauthorised physical access - this means that physical security measures will be provided to prevent unauthorised persons gaining access to the ATN hardware and/or software.*

If we accept these security policies as appropriate for the ATN the next step is to look at the implications of each.

For policy number 1 it is not necessary to apply any security mechanisms or procedures.

For policy 2 it would be appropriate to apply security mechanisms for authentication for aircraft to air traffic control center communications to provide assurance that a message comes from where it claims. Mechanisms need to also be defined to insure such messages have not been tampered with or are a repeat of an obsolete message.

For policy 3 it would be appropriate to apply security mechanisms for authentication for systems management and IDRP exchanges to provide assurance that a message comes from where it claims. Mechanisms need to also be defined to insure such messages have not been tampered with or are a repeat of an obsolete message.

For policy 4 no specific security mechanisms are needed, however the mobile subnetwork design, the ground subnetwork implementations and the aircraft equipage should support having alternative communication paths available in case one gets jammed. The role of the ATNP would be to coordinate with the other ICAO panels responsible for the development of air-ground subnetwork standards. Guidance for ground and airborne implementors should be provided to clearly indicate the benefit of having multiple subnetwork paths between routers.

For policy 5 guidance for ground implementators should be provided on the importance of providing physical security measures.

Thus it is in response to policy 2 and policy 3 that the ATNP will need to develop SARPs for security provisions. As indicated above, mechanisms are required to secure ground-ground and air-ground exchanges. Standard mechanisms exist to provide the appropriate security provisions in networks with only fixed service users. However, the inclusion of mobile users within the ATN has introduced a number of additional issues that must be resolved. As recognized in the tasking from ATNP/2 the administration of the ATN security features could be difficult where mobile users, and many international organizations are concern. Also the limited bandwidth of the air-ground subnetworks require that very bit-efficient security mechanisms must be defined.

2.2 Security Framework

ATNP WG3 was tasked by ATNP/2 to develop "provision of X.500 directory service integrated with other ATN applications including CM and ATSMHS." An initial review of the current (1993) ITU-T standards for X.500 (reference 3) as well as X.509 (reference 4) has shown a potential approach to overcome what heretofore have been seen as major obstacles to defining a security framework that can accommodate mobile as well as fixed users of the network. With this approach a combination of X.500, X.509 and associated ITU-T standards, and the integration of X.500 and CM would provide the essential tools around which ATN standards could be developed to provide authentication services, distribution of security keys, and the administration of security keys.

2.2.1 Overview of X.509 and it Potential Application to Support Security on the ATN

Public key cryptography is widely used to deliver secure data transmission. The generation and control of public keys require management, and for this purpose X.509 describes the notion of a 'trusted' authority referred to as the Certification Authority (CA). The CA is responsible for endorsing the identity of users whose details may be held in the X.500 Directory, and the CA issues a certificate to authenticate the user's name and public key. There are commercial tools available that enable an administrator to create and manage these certificates easily.

The ITU-T, through X.509, has recommend strong authentication based on public key cryptosystems as the basis for providing secure services. X.509 provides a flexible, scaleable and manageable algorithm-independent authentication infrastructure, which can be used as the basis for a wide range of security services such as message encryption and access control.

In order to support strong authentication X.509 defines a security framework where each user obtains its public and private key assignments from a CA. In the case of the ATN the CA could be the CAA or an organization contracted by the CAA to provide the CA services. An airline, or an organization contracted by one or many airlines, could serve as their CA. Each end user will then know its own public and private keys as well as the public key of its own certification authority. Each user is identified by its possession of its private key. A second user is able to determine if the communication partner is in possession of the private key, and can use this to corroborate that the communication partner is in fact the correct user (i.e., authenication). The validity of this corroboration depends on the private key remaining confidential to the user. For a user to determine that a communication partner is in possession of the correct private key, it shall itself be in possession of that user's public key.

In order for this authentication process to work, a user must obtain the other user's public key from a source that it trusts. Such as source (i.e., the CA) uses the public key algorithm to certify the public key and to produce a 'certificate'. The certificate includes a collection of information including the user's distinguished name and public key as well as other optional information. The X.500 directory entry for a user supporting strong authentication contains the certificate along with other directory information such as the user's network address. The public key of a given user can be discovered by any other user knowing the public key of their own CA.

In the general case, before users can mutually authenticate, the directory will supply the complete certification and return certification paths. Note that the certification path is defined by X.509 as:

> *An ordered sequence of certificates of objects in the Directory Information Tree (DIT) which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.*

The X.509 standard defines 5 generic cases on how the certification path can be obtained. These alternatives are:

> *a) if the two users that want to authenticate are served by the same CA, then the certification path becomes trivial, and the users unwarp each other's certificates directly;*
>
> *b) if the CAs of the users are arranged in a hierarchy, a user could store the public keys, certificates and reverse certificates of all certification authorities between the user and the root of the directory information tree (DIT). The user would then only require the certification paths from the common point of trust;*
>
> *c) if a user frequently communicates with users certified by a particular other CA, that user could learn the certification path to that CA and the return certification path from that CA, making it necessary only to obtain the certificate of the other user itself from the Directory;*
>
> *d) certification authorities can cross-certify one another by bilateral agreement. The result is to shorten the certification path;*
>
> *e) if two users have communicated before and have learned one another's certificates, they are able to authenticate without any recourse to the Directory.*

Having learned each other's certificates from the certification path, the users can check the validity of the received certificates.

Note that the X.509 framework supports having the CAs form themselves within a hierarchy. While a conventional form of such a hierarchy would imply there be a single CA at the top of the hierarchy it appears other alternatives are acceptable within the X.509 security framework.

Now let us consider how, within the context of an ATN environment, how a user could learn the certification and return certification paths. If we accept that the CAs will not be organized in a hierarchy with a single CA at the top, then alternative b) above is not directly applicable on a global basis. However, within the context of a State, Region and a global basis it may be desirable to arrange the CAs in a hierarchy to serve the ATN but there will not be a single CA at the top of the global hierarchy. Thus for the ATN the method for determining the certificate path should not assume a single root at the top of the hierarchy.

Alternatives a), c), d) and e) may each be applicable in certain contexts within the ATN. Of these four alternatives it appears that alternative d) is the general case that could be applied to the ATN on a global scale. If we assume for a moment that the States and organizations that operate the global ATN backbone (e.g., States, regional organizations, airline industry service providers, etc.) each have an associated CA. This would result in a modest number of CAs at the highest level of the hierarchy. These CAs could cross certify each other through bilateral agreements. Thus we could envision an hierarchy of CAs with several, rather than a single CAs at the top of the hierarchy. These top level CAs would would certify each other through bilateral agreements, thus enabling provision of a complete certification path between two users served by a CA under the heirarchy of different top-level CAs. This approach would allow any legitimate ATN user to learn the certification path and return certification path between themself and any other ATN user they desire to communicate with.

2.2.2 Industry Support for X.509 Based Security Framework

Both the ITU-T (OSI) and the Internet communities have widely accepted X.509 based security solutions. There already exists extensive industry and Government support of X.509 based systems. For example, within the internet community major companies such as Netscape, Microsoft, RSA Laboratories and many others are currently using X.509 to support security for data exchanges across the Internet (see the list of reference documents 5 through 10 and the Web sites in Attachment A to this working paper for more information). Note that the referenced RFCs provide useful information related to the use of X.500/X.509. However, the approach proposed by herein for the purposes of ATN SARPs is for the use of X.500/X.509 within the context of an OSI protocol stack.

Examples of Government use of X.509 includes the U.S. Department of Defense and the ICE-TEL Project funded by the European Commission involving 17 partners from 13 countries (see Attachment A to this working paper for more information).

Commercial products are readily available to support X.500 and X.509. Included are products for use by Certificate Authorities as well as by the users and providers of directory services.

2.2.3 ATN Security Framework

If it is accepted that X.509 defines a security framework that can be applied to the ATN ground infrastructure to provide for the assignment, management and distribution of security key information, then we next must consider how this can be extended to support mobile users. The ATNP WG3 work program includes the integration of X.500 with the air-ground context management (CM) application. The security approach proposed here is to upgrade the CM application for version 2 to include the necessary air-ground support for public key distribution. An example of a process that could be employed for an airborne user to receive secured ATN communication services is described below as a series of steps:

Step 1 - aircraft owner/operator obtains their public and private assignments from their designated certification authority (CA). With this they also are given the public key of the CA.

Step 2 - the aircraft owner/operator implements X.500 Director User Agent (DUA) in their ground automation system (e.g., automation system used for flight plan). For a general aviation user, they could work though a CAA operated or authorized organization which in turn has implemented a X.500 DUA.

Step 3 - the aircraft owner/operator provides the information for a X.500 entry that includes the aircraft's ATN network address(es) and the CA issued Certificate that contains the public key information.

Step 4 - once entered into the X.500 directory the ATN ground infrastructure provides authorized ATN ground users with global access to this information. Note that the X.509 authentication procedures would apply to all X.500 access thus providing the means to ensure that only authorized ground users can access the X.500 directory.

Step 5 - an aircraft using a version 2 of the Context Management (CM) application generates a CM logon request message that includes an indication that secured services are requested. One alternative would be for this logon request message itself not be secured and if the ground CM application were still at the version 1 level (i.e., as per package-1 ATN SARPs) then the air and ground CM applications would revert to a version 1 CM service, not supporting the security provisions.

Step 6 - if both air and ground CM applications are at version 2 level and the aircraft has requested secured services then goal would be for all subsequent ATS (or at least ATC) exchanges to employ digital signatures. One way of supporting this would be for the ground CM application to incorporate a X.500 directory user agent. Having received the initial aircraft CM logon requesting secured services, the ground CM application would use X.500/X.509 to obtain the certification path and ultimately the directory entry for the given aircraft. This directory entry would include the Certificate that in turn includes the public key for the aircraft. The directory entry would also include addressing information for that aircraft that could be compared against the information in the CM logon request.

Step 7 - having obtained the public key for the aircraft, the ground CM application has the information it needs to generate a secured message to the aircraft. Note than only an authorized ground X.500 user has access to this directory information. The ground CM application, having obtained the public key for the aircraft, can now respond to the CM logon request with a secured CM logon response message. However, up to this point the aircraft does not have the public key for the ground CM application. The ground CM application's logon response message could include the public key information for itself and the public keys of the ground ATS applications. Since this message would be secured, only the aircraft with the correct private key would be able to decrypt the received CM logon confirmation message.

Step 8 - ground applications (such as CPDLC) desiring to initiate a dialog with an aircraft would obtain the addressing and public key information from the ground CM application. The ground access to the CM application would also need to be secured to ensure that only authorized ground applications can access the public key information contained in the CM data base. Next data authority messages generated by the ground CPDLC application could include the public key as well as the address information for the next ATC authority.

The above is an example of how X.500, X.509 and an enhanced CM application could be used to support secured services on the ATN. At the detailed level, alternative approaches are certainly possible. However, such details go beyond the basic security framework and the further definition can be undertaken by the appropriate ATNP working group.

While the above example has not specifically addressed the use of authentication for IDRP exchanges, the use of the X.509 based security framework provides a straight forward approach to supporting authentication for ground-ground IDRP exchanges. However, further investigation will be required to validate the need for secured air-ground IDRP exchanges and if this capability is required, any required additions or extensions to the proposed ATN security framework would need to be defined to support this capability.

The proposed ATN security framework, based on X.500/X .509, would also support ATN systems management by providing the means for key management and distribution in support of secured systems manager-to-manager and manager-to-agent communications.

3. Proposal

a) It is proposed that WG1 accept the above described framework for ATN security based on the use of X.500, X.509 and enhanced CM services.

b) It is proposed that the working groups of ATNP develop the ATN security provisions based on commercially available products to the maximum extent practical. The goal should be to isolate the ATN specific security features to those areas which are already inherently unique to the ATN, such as the context management application.

c) WG1 endorse that the ATNP working groups undertake the following work items in order to progress the development of Package - 2 ATN SARPs enhancements for security:

3.1 Proposed WG1 tasking

a) Prepare a flimsy to WG2 and WG3 requesting they review the proposed high level framework proposed by this working paper and undertake the work program items described below.

b) Develop a Package - 2 Core and Sub-Volume 1 SARPs for the ATN security architecture based on the above proposal and as well as any feedback received from WG2 and WG3.

c) Investigate the relationship between the Certification Authority (CA) hierarchies and the ATN addressing and ATN router hierarchies.

d) Investigate the institutional issues related to CAs and develop guidance on the nature of bilateral agreements that would be needed among the highest tier of CAs.

e) Investigate the institutional issues related to the use of cryptography as this may impact the specific cryptographic algorithm selected for use by the ATN. Coordinate with WG3 on this topic.

f) Investigate transition issues (e.g., where some users are at version 1 while others are at Package - 2 of the ATN SARPs) and failure/recovery issues.

g) Investigate the interrelationship needed between the certificate authorities of the States and those of airlines and service providers.

h) Develop guidance material for Package - 2 ATN security provisions including the need for bilateral agreements between States/organization.

3.2 Proposed WG2 tasking

a) Review the proposed ATN security framework and provide comments to WG1 on the applicability of the proposed ATN security framework to support IDRP authentication services for ground-ground IDRP exchanges and/or air-ground IDRP exchanges.

b) Develop Package - 2 ATN ICS SARPs to support authentication for IDRP exchanges.

3.3 Proposed WG3 tasking

a) Review the proposed ATN security framework and provide comments to WG1 on the applicability of the proposed ATN security framework to support secured data communications between ATS applications.

b) Develop the SARPs for the X.500 service including the X.500 schema and the X.500 directory profile with support for X.509 authentication services.

e) Define the use of the ACSE option to support application authentication including the definition of the cryptographic algorithm to be used (references 7 and 10 define potential algorithms). Coordinated with WG1 in order to ensure the associated institutional issues are addressed and coordinate with WG2 to ensure the consistency with the security requirements for IDRP exchanges. Consider the use of different key lengths for aircraft/ground communications vs. ground/ground communications as a means of reducing overhead across the air-ground subnetworks and potentially avoiding institutional issues associated with the movement of cryptographic systems (i.e., on aircraft) across international borders.

f) Define Package - 2 of the context management application to support integration with X.500 and to support the security framework.

g) Define Package - 2 of the air-ground and ground-ground applications to support secured services.

Attachment A
Sources for information on X.500/X.509

1. Standards documents from the Internet Engineering Task Force (IETF) are available electronically over the Internet from the ftp site listed below. The standards, draft standards, proposed standards, etc. from the IETF are published as "Request for Comments" (RFCs) with a number appended. Key RFCs of interest related to X.500/X.509 and cryptographic algorithms are: is RFC 1421, RFC 1422, RFC 1423, RFC 1424. RFC 2120 and RFC 2144. The official ftp site for all RFCs is:

   ftp://ds.internic.net/rfc

   RFCs are also available from a number of other sites on the World Wide Web including:

   http://sunsite.auc.dk/RFC

2. The most widely used browser for users of the World Wide Web (WWW) is Netscape Navigator. Netscape uses X.509 for secured services over the WWW. Netscape offers a white paper on "Securing Communications on the Intranet and Over the Internet." This white paper is available off of the Netscape WWW site:

   http://www.go-digital.net/whitepapers/securecomm.html

3. The European Commission has funded the ICE-TEL Project. This funding covers the period of December 1995 through November 1997. The project, involving 17 partners from 13 countries, has as its purpose building and operating a Certification Authority (CA) infrastructure and secure applications (WWW, S/MIME and X.500). The model being used allows a hierarchy of CAs with no reliance on a top level registration authority. A briefing package is available electronically over the WWW at:

   http://fw4.iti.salford.ac.uk/ice-tel/dimacs.tsld001.htm

4. A document titled "Overview of Certification Systems: X.509, CA, PGP and SKIP" has been electronically published by a group promoting an alternative referred to "Meta-Certificates." The utility of this paper is in its description of the role Certification Authorities under the X.509 framework and potential concerns. While the paper identifies concerns with the use (or perhaps better termed the improper use) of X.509, that they claim to overcome these concerns with their alternative solution. The value of this paper to the ATNP is that it does appear to raise a number of points that need to be considered when defining the ATN security framework. This paper does not raise any concerns or issues that invalidate the recommendation that the ATNP adopt a X.509 based security framework for the ATN. This paper is available via the WWW at:

http://novaware.cps.softex.br/cert.htm

ATNP/WG1
WP/_____

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL(ATNP)
WG1 – Systems planning and concept working group

30 June – 3 July 1997
Langen, Germay

Systems Management Strategy for the ATN

Presented by Martin Adnams

Summary

This working paper proposes an approach by which the ATNP working groups can progress their work program for Systems Management based on existing work done in that area.

References:

1. WG1/WP6-08 Systems Management Concept ATNP/2 (WG1 Standing Document)
2. WG1/WP6-09 Overall Systems Management Concept

Introduction

Working Group 1 of ATNP was given work items by ATNP/2 to:
"develop a systems management strategy for the ATN including a plan for the administration of the systems management features", and
"develop system level SARPs and guidance material for ATN Systems Management".
This is a continuation of work started prior to ATNP/2 which lead to the creation of a standing document for the ATN Systems Management Concept (ref. 2). Ref. 1 was a working paper prepared by WG1 at its meeting in Halifax and submitted to ATNP/2. This working paper does not reproduce of the results of work documented in Ref. 2, the Overall Systems Management Concept which already defined a basic strategy, but identifies work items to be undertaken and decisions to be made using that strategy.

Discussion

Background

The previous work of WG1 on this subject is given in references 1 and 2. Included there as an Appendix to WG1/WP6-09 is Chapter 12 of the ATN Manual v2 (that was never published by ICAO) where the OSI model for Systems Management was taken as the basis for the development of SARPs and Guidance Material.
At Toulouse in March 95, participants of the meeting agreed that:
"Given the current lack of well identified operational requirements regarding Systems Management for the ATN internet , the definition and implementation of a global ATN Systems Management solution cannot be achieved within the timeframe foreseen for the package 1 SARP acceptance. Consequently , within this timeframe:

1. No exchange of Systems Management information will be required between routers of different administrative domains .
2. No exchange of System Management information will be required by means of a management protocol over the air/ground links. This does not preclude the exchange of routing information, by means of routing information exchange protocols.
3. The exchange of System Management information within an administrative domain is considered a local matter and can be achieved by any means deemed appropriate."

For CNS/ATM-2 Package this decision is being re-visited.

Why do we suddenly need SARPs ?

There can be no doubt that there is a great deal of work to be done when implementing the ATN in the area of Systems Management, the question is; how much needs to be standardised by ICAO ?
Previous statements made in The Systems Management Concept (Ref. 2) are given in the section immediately below, the section after that makes an analysis of these statements to identify what is needed for SARPs.

Previous Statements

The Systems Management Concept (Ref. 2) made the following statements (all statements were tagged for future reference in the original document).

General

[SM 1] The management of operational applications using the ATN is outside the scope of this document.

[SM 2] ATN SARPs shall only cover aspects that are necessary to the correct behaviour of ATM services using the ATN offered between organisations, across international boundaries and between the air and the ground.

[SM 3] Regional standards may need to be developed and applied internally within distinct geographical areas and organisations.

[SM 4] The structure of systems management and the associated interfaces within an organisation are not the subject of SARPs, although it may be desirable to provide guidance on these matters to accompany SARPs.

Institutions

[SM 20] No ICAO ATN SARPs are required unless institutions provide electronic repositories of information (e.g. an address registration and allocation database).

[SM 21] Institutional procedures must be defined to make and administer service contracts, policies and agreements.

Administrators looking at multiple networks

[SM 26] As a minimum regional standards are required for the communication of information between Administrators, Network Managers and Service Providers.

[SM 27] ICAO ATN SARPs will be needed if Administrators in different regions wish to exchange summary information at their disposal.

Networks

[SM 32] Regional standards will be needed for the distributed management of networks within organisations on the ground.

Airborne

[SM 33] ICAO ATN SARPs will be needed when management information is exchanged over the air ground link.

[SM 43] Aeronautical standards will be needed for the distributed management of networks within aircraft.

[SM 44] ICAO ATN SARPs will be needed when management information is exchanged over the air ground link for fault and event reporting.

Analysis

To summarise the above it appears that SARPs will only be required:

[SARPS 1] For Manager to Manager communication (i.e. between Administrators or Network Managers) in different regions or organisations when serious network problems in one region or organisation (or in subnetworks connecting them) may affect the ability of another to achieve the required quality of service.

[SARPS 2] For Manager to manager communication for statistical reporting (e.g. for cost sharing and performance assessment).

Note 1: In support of this it will be necessary that ATN systems in Regions and organisations accumulate and report the required information and present it in a standard format.

Note 2: It is assumed that the ATN Systems owned by a particular state, organisation, airline or service provider are not managed by another such entity. When this is the case then those entities bi-laterally agree on the standards to be applied and they appear again as just one entity where internally SARPs do not apply.

[SARPS 3] For Management Information and protocols exchanged over the air-ground link for event and fault reports of serious operational consequence to ATC authorities.

Note: Full Management of airborne systems from Airline ground facilities is a different case where Airlines may want full management of airborne systems on board. SARPs are not considered appropriate for that. The medium of communication may be shared with ATN application traffic, a functional system level requirement may be needed to dictate that this shall not hinder normal ATC operations. Guidance and examples may be appropriate but Aeronautical standards will be needed.

[SARPS 4] In support of SARPS1/2/3 where it will be necessary that ATN systems in Regions and organisations report the pertinent information (for Fault reporting, performance assessment and accounting) to Network Managers and Administrators.

Note: Functional system level SARPs are sufficient to define the information required from ATN systems. It is not necessary to have detailed SARPs for the Information, Protocols, Managers and Agents in ATN systems within organisations and regions. Guidance and examples may be more appropriate.

[SARPS 5] For performing measurement and reference testing of ATN systems in the context of approval and certification (ref. Eurocontrol RAF and ATNSI CTS projects). For this it will be necessary to standardise information relating to an implementation such that its characteristics can be assessed by an external tool. If this is agreed then standard management information and access mechanisms will be needed.

Question: Is the principle of enforced management implementation by SARPS to support approval, certification and testing agreed ?

ATN Systems Management Framework

The Rules

When SARPs, Guidance or Manual material is developed for Package 2 the following rules should be applied.

R1 The Material should identify a minimum base set that can be extended by regional implementations, airlines etc. for their own purposes. The objective is to standardise as little as possible whilst ensuring that sufficient management information and functionality is guaranteed in ATN systems and that this is available to Managers using SARPs compliant management protocols.

R2 The Material should not represent a “quantum leap” from Package 1 and should concentrate on practical aspects that can be “built in” to ATN systems and subnetworks (or are available in existing commercial products) in the short term (i.e. before 2000). The objective is to provide sufficient visibility on the internal operation of ATN systems in support of Performance assessment, Accounting and Fault detection. Automatic fault correction, performance enhancement and configuration management are “out of SARPs scope”, recovery procedures and manual intervention will be required.

R3 The SARPs Material should be based on the OSI model for Systems Management Information, Functions and Protocols (as previously specified in Appendix 12 of the ATN Manual V2). CORBA, JAVA and other esoteric proposals for management solutions are “out of scope”. Guidance material on the internal use of other mechanisms for management (e.g. SNMP) may be given.

R4 The Material should be formulated taking input from existing and planned ATN implementations (e.g. PROATN and ATN Systems Inc.) and their specifications.

R5 The Material should allow as far as possible for the use of COTS products for Manager implementations.

R6 The Material should allow as far as possible for the use of COTS products for Agent implementations in ground based and airborne ES/BIS.

R7 The Material for the Systems Management protocol stack for the Internet should be identical to the ICS SARPs and not introduce modifications to that specification.

R8 The applicability of the existing UL SARPs for the Systems Management protocol stack should be evaluated with the objective of reducing as far as possible the need for parallel upper layer stacks (i.e. for ATN application data, Systems Management data and Security key communication).

Note 1: The use of the UL SARPs for Systems Management is a subject for further study, the fastbyte upper layers are not available in any commercial management product.

Note 2: The extent to which the use of COTS is possible is dependent upon the overall assessment of system certification and approval. This is currently an unsolved problem and is outside the scope of ICAO, the level to which Systems Management needs to be certified/approved depends upon how it will be used.

Proposal

a) It is proposed that WG1 agree that the ATNP/2 mandate to "develop a systems management strategy for the ATN including a plan for the administration of the systems management features" was largely achieved by the Overall Systems Management Concept (ref. 2) and recommend further strategy work (e.g. the planning aspect) only on that basis.
b) WG1 discuss the above described framework for ATN systems management and decide on the open issues raised above with respect to what should be SARPs, Guidance or in a Manual.
c) WG1 endorse that the ATNP working groups undertake the following work items in order to progress the development of ATN systems management:

Proposed WG1 tasking

a) Develop a Package - 2 Core and Sub-Volume 1 SARPs for the ATN systems management architecture based the above proposal and feedback received from WG2 and WG3.
b) Based on the Operational Concept define the basic purpose and scope of Systems Management for each of FCAPS (Fault, Performance, Configuration, Accounting and Security (done by WG1 SG2)).
c) Investigate the institutional issues.
d) Investigate transition issues (e.g., where some users are at version 1 while others are at Package - 2 of the ATN SARPs)
e) Develop guidance material for Package - 2 ATN systems management provisions.

Proposed WG2 tasking

Despite the open questions for SARPs development WG2 can do significant work to prepare for systems management implementation. Suggested tasks are:

a) Review the proposed ATN systems management framework (ref1 and ref2 included) and provide comments to WG1 on the applicability of the proposed ATN systems management framework.
b) Develop guidance material for the implementation of distributed management of the ATN Internet within organisations on the ground (i.e. manager to agent communications) based on existing material (e.g. ISO standards, ATN Manual V2, industrial ATN system developments).
c) Develop SARPs for management exchanges over the air-ground during flight for real-time event and fault reports of serious operational consequence.
d) Identify how systems management information is to be transported by the ATN Internet.
e) Identify the minimum set of information ATN Internet systems need to support to provide Performance assessment, Accounting and Fault detection to managers, for ground-ground and air-ground communications.
f) Identify the Managed Objects and access mechanisms required for reference testing of the Internet using input from the Eurocontrol RAF and ATNSI CTS projects.
g) Provide SARPs, Guidance to aeronautical standards bodies for the distributed management of ATN systems within aircraft and for Airline ground access to manage those systems (TBD is this ICAO's job ?).
h) Identify Management information needed for enforcing Service Level Agreements with Service Providers.
i) Provide guidance to link system events to actions needed to enable the exchange of application data (i.e. between s/n connectivity JOIN/LEAVE, IDRP connection, TP4 connection, Context management exchange and Application associations).

Proposed WG3 tasking

Despite the open questions for SARPs development WG3 can do significant work to prepare for systems management implementation. Suggested tasks are:

a) Review the proposed ATN systems management framework (ref1 and ref2 included) and provide comments to WG1 on the applicability of the proposed ATN systems management framework.

b) Define Managed Object addressing and registration scheme.

c) Recommend systems management upper layer profiles and identify their impact (e.g. compatibility with existing ULA, support of filtering scoping etc.)

d) Define Upper Layer management information needed to provide Performance assessment, Accounting and Fault detection to managers, for ground-ground and air-ground communications.

e) Identify the systems management functions required (standard ISO 10164 or other) required to support Performance assessment, Accounting and Fault detection in ATN systems (Agents) and Managers.

f) Propose a peer to peer Manager to Manager communications architecture and associated functions using the ATN Internet based on the OSI Model and ISO standard profiles.