ATNP WG1WP13-09
WG2WP479
WG3WP14-25

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL (ATNP)

WG1 – SYSTEMS PLANNING AND CONCEPT WORKING GROUP

5 - 6 October 1998
Bordeaux, France

Agenda Item 7 – Sub Group Reports

Sub Group 2 Chairman Report

Presented by M. Bigelow

SUMMARY
This paper outlines the progress made by SG2 since the 12th meeting of WG1.

1. Introduction

The purpose of this working paper is to report to WG1 on the activities and results of the Security Subgroup (SG2) since the WG1/12 meeting held in Utrecht.

2. Work Plan

2.1 The subgroup has held one meeting during this time. A changes was made in the sequence of WG1, and WG2/WG3 meetings to allow the SG(s) to provide input to WG1 in advance of the actual meeting rather than in the meeting itself. This report is still a bit late but as we get 'settled' into the new sequence we will endeavor to improve.

2.2 The work plan proposed to WG1 at Langen consists of investigation of a number of issues associated with utilization of security services, conduct of several activities related to investigation of operational requirements and development of a number of specific products.

2.3 Progress has been made on all parts of the work plan. The tables in Section 3 reflect the changes and a summary follows.

2.3.1 Issues worked on cryptographic algorithm selection including signature length and key length. Submitted flimsy to WG1 and call for input based on specified criteria.

2.3.2 Revised Version 0.8 of guidance considerable revision based on comments from and produced Version 0.9 proposed to WG1 as Version 1.0.

2.3.3 Updates have been made to the draft SV-1 SARPs. While some of these updates were editorial there were additions made to include the basic ATN security policy and requirements related to confidentiality.

3. Work progress

3.1 WG1 SG2 Issues

Specific issues being investigated and accounted for by SG2 include:

#	Issue	Comments	Status
1	The relationship between the Certification Authority (CAs) hierarchies and the ATN addressing and ATN router hierarchies.	Current thinking is that there is no relationship necessary between the Certification Authority (CAs) hierarchies and the ATN addressing and ATN router hierarchies	Closed
2	The institutional issues related to CAs and the nature of bilateral agreements that would be needed among the highest tier of CAs.	Material is planned for: 1. Core and SV-1 SARPs 2. Concept of Operations 3. Global ATN Security Policy	Ongoing
3	The institutional issues that are related to the use of cryptography as these may impact the specific cryptographic algorithm selected for use by the ATN.	Maintain approach as use of cryptography only for authentication. Masoud transmitted request to all administrations to provide information on government restrictions on import/export of cryptography and indicated that earliest likely return would be December 1997. Responses received from five states ICAO legal opinion also provided indicating that if the states accept the SARPs without taking exception then they are bound.	Ongoing
4	Transition issues (e.g., where some users support Package-1 with no support for security provisions while others support Package-2 of the ATN SARPs that includes security provisions)	Included in SARPs as requirement to maintain backward compatibility.	Closed
5	The interrelationship needed between the certificate authorities of the States and those of airlines, airspace users and service providers.	Proposed as set of CA certified to a common specification	Closed
6	Application of Security to ATSMHS	Input from WG3 needed	Ongoing
7	Airman vs. Airframe	Current position of WG2 is that certificates for ATS should be on airframe basis. Included in SARPs as assignment to airframe. Remaining investigation on whether this should be at 24-bit id or application.	Resolved – with some ongoing
8	Initial load of certificate/key into avionics	Action to P. Hennig and M. Bigelow to work with AEEC	Ongoing

3.2 WG1 SG2 Products

SG2 is developing the following products.

Item	WG1/SG2 Products	Due Date(s)	Status
1	Overall work plan of the subgroup	Oct. 1997	Unchanged (other than version numbering) from WG1/9
2	Ver. 0.*x* draft ATN system level security SARPs for Core/SV-1 at a level sufficiently complete for WG2 & WG3 to use as a basis to proceed with the development of the associated detailed SARPs (Proposed to WG1 as Ver 1.0)	WG1 Oct. 1997	Supplied to WG1/10 as WP10-18 and WP10-19
3	Ver. 0.*x* draft GM	WG1 Oct 1997	Supplied as WG1SG2WP3-7
4	Ver. 1.*x* draft ATN security SARPs for Core and SV1	WG1 March 1998	Supplied as attachments to this report
5	Ver. 2.*x* Proposed ATN security SARPs text for Core & SV1	WG1 June 1998	Supplied as WP12-10
6	Ver. 0.*y* draft GM	WG1 June 1998	Provided working draft version 0.1 for comment.
7	Ver. 1.0 Proposed ATN security GM	WG1 Sept 1998	Future September 1998 - Working draft 0.9 proposed as baseline 1.0.
8	Concept of Operations	WG1 March 1998	Not complete new due date June 1998. June 23, 1998 – Working as section 4 of guidance. Working draft 0.1 provided for comment.
9	Updates to Annex 17 and Doc 8973	WG1 June 1999	Annex 17 updates proposed, Doc 8973 under development. Flimsy to WG1 for Secretary to apprise other ICAO groups of ATNP activities related to security.

3.3 WG1 SG2 Activities

Activities related to the products assigned to SG2 are defined in the following table.

Item	Activity	Due Date(s)	Status
1	Coordinate with the ATNP WG2 and WG3 subgroups to solicit their comments on the WG1 documentation, from the WG1 July 1997 meeting, on the high-level ATN security strategy	July - Oct. 1997	Closed
2	Hold subgroup meetings to prepare Ver 0.1	Aug – Sep 1997	
3	Coordinate with WG2 and WG3 to insure consistency between the security provisions defined across the SARPs sub- volumes	on-going (each SG meeting)	Coordination has not been good and to correct the SG request time be given to this in the JWG. June 23, 1998 – Much better now. Generated a working document (included in section 3.3 and coordinated with each of the subgroups).
4	Provide subgroup status reports to WG1	each WG1 meeting	Ongoing
5	Investigate Operational Requirements	Sept 1997	Submitted flimsy from Langen to ADSP requesting confirmation of proposed Security Strategy. Response from Chris Dalton indicates earliest feed back will likely be after June 1998. Have received copies of IFALPA Position Statement; following up with Patrick Bourdier for additional input. June 23, 1998 – Partial response indicates that minimum required is masquerade, modification, replay, and denial of service, as proposed by ATNP. More promised

3.4 Co-ordination Activities

Working Group Activities related to Incorporation of Security

Item	WG	SubWG	Sub-Volume	Responsible	Activities	Due Date
1	WG1	SG2	SV-1	M. Bigelow	Track SV work	June 1999
2	WG3		SV-6	T. Kerr	Coordination only	
3	WG3	SG3	SV-4	S. Van Trees (P) & Gerard Mittaux-Biron	WG3/SG3 is developing the Secure Dialogue Service (SDS). The DS currently offer a security requirements parameter, which maps to the authentication requirements field in ACSE. The SDS offers authentication of the dialogue and digital signature of the data of the dialogue. The SDS is based on GULS and X.509.	January 1999
4	WG2	None	SV-5	Jim Moulton	WG2 is currently investigating the addition of Type 2 (strong) authentication for IDRP routing exchanges. For ground-ground exchanges, standard use of X.509 certificates is possible. For air-ground exchanges, a method of certificate use that does not require additional air-ground messages is anticipated. IDRP authentication first draft should be available by the Utrecht meeting.	June 1998
5	WG3		SV-7	S. Van Trees & J. Moulton	ASN.1, X.509 Certificate, Cryptography Algorithm(s)	January 1999
6	WG3	SG1	SV-3	J.M. Vacher	Selection of MHS Security Elements of Service (through a Security Class of the SEC Optional Functional Group defined in ISO MHS ISPs). This selection needs to offer a suitable protection against identified threats to the AMHS. Possible use of X.509 in this context will be investigated.	September 1998
7	WG1	SG2	SV-6	M. Bigelow	Definition of requirements of Security Management	September 1998
8	WG1	SG2	??	M. Bigelow	Definition of security algorithm	January 1999

4. Recommendations

1. The Working Group is invited to note WP1310 as Version 3.1 draft SV-1 material for Doc 9705. The Working Group is requested to accept this as Version 4.0.

2. The Working Group is invited to note WP1311 as Version 0.9 of draft guidance material. This draft is substantially different in structure (and some content) than the version 0.1 (and 0.2) submitted to WG1 at Utrecht. This is the result of considerable comments by a WG1 member and input from participants during the SG meeting. The Working Group is requested to accept this as Version 1.0.

3. The Working Group is invited to note the recommendation in WP1307 And is requested to concur with the recommendation that WG1SG2 assume the work of selection of the appropriate security algorithm for the ATN.