ATNP WG1WP14-
WG2WP499
WG3WP15-33

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL (ATNP)

WG1 – SYSTEMS PLANNING AND CONCEPT WORKING GROUP

25 - 27 January 1999
Honolulu, Hawaii, USA

Agenda Item – Sub Group Reports

Sub Group 2 Chairman's Report

Presented by M. Bigelow

SUMMARY

This paper outlines the progress made by SG2 since the 13th 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 WG1/13 meeting held in Bordeaux.

2. Work Plan

2.1 The subgroup has held two meetings during this time. The first was held subsequent to the WG1 meeting in Bordeaux and the second in early December in Phoenix AZ.

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 Major issue on cryptographic algorithm selection. Concerns have been raised on whether an algorithm that meets the defined criteria can be found. The SG has not received any responses to the call for input on this issue. Within the SG the participants from NASA Ames are leading the selection process. Investigation of possible additional participation has included US government (NIST, NSA), academic and industry. The current target is papers, review and discussion during the next two SG meetings and selection by the May WG1 meeting.
>
> 2.3.2 Updates have been made to the draft Core and SV-1 SARPs and based on WG1 direction a new SV-8 for Doc. 9705 has been prepared using the detailed material from the earlier draft of SV-1. Current versions of these are Core Version 2.2 proposed for acceptance by the WG as Version 3.0, SV-1 Version 4.2 proposed for acceptance as Version 5.0 and SV-8 Version 0.2 proposed for acceptance as Version 1.0.
>
> 2.3.3 Coordination with the other Working Groups continues and has been facilitated by participation in multiple groups by some of the group members.
>
> 2.3.4 Work continues on the Guidance Material but focus has been on SARPs and SARPs related issues and no new version is proposed.

3. Work progress

WG1SG2 Deliverable and Action List

#		Description	Assigned To	Due Date	Status
1		Draft Core SARPs	R. Jones		Complete
2		SV1 SARPs updates and additions for Certificate Authorities	M. Bigelow		Open
3		Draft Certification Practices Statement	M. Bigelow		Open
4		Questions and Issues for WG2 and WG3 (Flimsies 2-3 and 2-4)			Complete
5		Produce Concept of Operations	M. Bigelow	June 1998 (0.1)	Outline accepted. Additional work to be tracked under 19, 17, and 18
6		Annex 17 and Doc. 8973 recommendations	P. Bourdier & D Stewart		Tabled to follow AI 9 Work in progress under 20
7		Digital Signature Managed Object fault attempts and failure			Expanded to A and B below
	A	Addition of high level requirements to SARPs	R. Jones	September 1998	Included - Closed
	B	Addition of high level requirements to guidance	M. Bigelow	September 1998	
8		Recommendations to RTCA 189/EUROCAE 53 on security in the initial ATN implementation	P. Hennig	June 1998	Deleted as not applicable.
9		Draft ATN Security Policy	P. Bourdier		
10		Track SV work	M. Bigelow	Ongoing	Being tracked through ACTIVITIES file
11		Overall work plan of the subgroup	M. Bigelow	Oct. 1997	Complete
12		Version 0.1 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	SG2	WG1 Oct. 1997	Complete – accepted as Version 1.0
13		Version 0.1 draft GM	SG2	WG1 Oct. 1997	Complete – remained 0.1
14		Version 1.*x* draft ATN security SARPs for Core and SV1	SG2	WG1 Feb. 1998	Complete – Proposed as Version 1.2 in March meeting

WG1SG2 Deliverable and Action List

#		Description	Assigned To	Due Date	Status
15		Version 2.0 Proposed ATN security SARPs text for Core & SV1	WG1	March 1998	Complete – Version 1.2 accepted and increments to 2.0
16		Version 2.*x* Proposed ATN security SARPs text for Core & SV1	SG2	WG1 June 1998	Complete – Version 2.1 submitted and accepted.
17		Version 0.*y* draft GM	SG2	WG1 June 1998	Complete – Proposed and accepted.
18		Version 1.*x* Proposed ATN security GM		WG1 Sep. 1998	Complete – Proposed and accepted.
19		Concept of Operations		WG1 March 1998	Complete – Now part of the overall Guidance Material and will be tracked with it
20		Updates to Annex 17 and Doc 8973	P. Bourdier	WG1 June 1999	Working – Annex 17 updates proposed Doc. 8973 under development. Flimsy to WG1 for Secretary to apprise other ICAO groups of ATNP activities related to security.
21		Copies of Doc 8973 to SG	M. Bigelow	March 31	Complete – Not distributed due to limitations in the document. Made available for review at each meeting. Separate copies available on request.

WG1SG2 Deliverable and Action List

#		Description	Assigned To	Due Date	Status
22		Copies of responses to state letter on cryptography import/export limitations	M. Bigelow	March 31	Complete – Distributed at BOD as WP911.
23		Work with AEEC on definition of how the initial installation and subsequent update of certificates (actually the private key) into the avionics will be done.	P Hennig M. Bigelow	January 18, 1999	
24		Develop flimsy on need (or not) to conduct risk/threat analysis on individual application basis.	M. Bigelow	June 21	Submitted to WG3 as WP13-14.
25		Outline of CAMAL	M. Paydar	August 15 January 99	Partial – response came in too late for meeting 8 coordinated at meeting 9 with distribution as w1s2w908. Masoud agreed to provide outline of the other two parts (III and IV).
26		Addition of stricture against the use of encryption across administration boundaries	R. Jones	September 1998	Complete - BOD
27		Pose question to WG1 on consolidation of security guidance into single section or distributed throughout CAMAL	M. Bigelow	June 23, 1998	Answer at Utrecht was this likely will need to be handled with a mix of the two approaches. There is a section planned for Security but material will need to be in each of the other SV as well
28		Check with JSG on CONOP for input to W1S2 Meeting 10	M. Bigelow	December 1998	

Working Group Activities related to Incorporation of Security							
Item	**WG**	**SWG**	**Sub-Volume**	**Responsible**	**Activities**	**Due Date**	**Status**
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 & 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	W3WP1424 (w1s2w912) input to Bordeaux. The SG will review the paper in detail and comments will be covered at meeting 10 in Phoenix.
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	Target draft SARPs January 1999 Question raised – will any A/G router NOT support logon unless there is GG connectivity available
5	WG3	SG3	SV-7	S. Van Trees & J. Moulton	ASN.1, X.509 Certificate, Cryptography Algorithm(s)	January 1999	Algorithm investigation and selection moved to WG1SG2 X.509 profile in progress

Working Group Activities related to Incorporation of Security

Item	WG	SWG	Sub-Volume	Responsible	Activities	Due Date	Status
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	w1s2w910 – AMHS Security operation using Security Class 0. Based on paper presented to WG3 (WP225) Presented by Jean-Marc Vacher SG will review the paper in detail and prepare comments for Meeting 10
7	WG1	SG2	SV-6	M. Bigelow	Definition of requirements of Security Management	September 1998	
8	WG1	SG2	SV-8	M. Bigelow	Definition of security algorithm	January 1999	

WG1 SG2 – Security Issues List

#	Issue	Comments	Status
1	The relationship between the Certification Authority (CA) 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 CA and the nature of bilateral agreements that would be needed among the highest tier of CA.	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	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; This item is being worked under ACTIVITIES #6	Ongoing
7	Certificate assignment to Airman or 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 – ACTION #23	Ongoing
9	Need for risk/threat analysis to determine exact nature of changes to application SARPs	Action to M. Bigelow to respond to WG3 (SG2).	WP1314 submitted to WG3. Awaiting response.

WG1 SG2 – Security Issues List

#	Issue	Comments	Status
10	Rule(s) for operation in case of revoked or expired certificate.	Corollaries to this rule are operation during system failure. A possible approach to coverage of this issue was proposed in the form of consideration of a backup certificate	
11	B-directional AG authentication	Papers are solicited. WG1SG2 will determine if this is a requirement and if so will refer to WG2 for specifics on an appropriate mechanism.	
12	TEMPEST Risk Analysis	WG1SG2 must determine if this is needed. Papers are solicited.	

4. Recommendations

1. The Working Group is invited to note WP1406 as Version 2.2 draft Core SARPs. The Working Group is requested to accept this as Version 3.0.

2. The Working Group is invited to note WP1407 as Version 4.2 draft SV-1 material for Doc 9705. The Working Group is requested to accept this as Version 5.0.

3. The Working Group is invited to note WP1408 as Version 0.2 draft of a new SV-8 for Doc 9705. The Working Group is requested to accept this as Version 1.0.