ATNP WG1WP1610
WG2WP537
WG3WP17-44

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL (ATNP)

WG1 – SYSTEMS PLANNING AND CONCEPT WORKING GROUP

4 - 7 October 1999
Gran Canaria, Spain

Agenda Item – 9a – Sub-Group Reports

Sub Group 2 Chairman's Report

Presented by M. Bigelow

SUMMARY
This paper outlines the progress made by WG1SG2 since the 15th 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 WG1/15 meeting held during May 1999 in Naples, Italy.

2. Work Plan

2.1 The subgroup has held three full subgroup meetings during this time. Meeting 13 was held immediately following the WG1 meeting in Naples, meeting 14 during July in Atlantic City, NJ, and meeting 15 August 23-26 in Columbia, MD. Coordination with the other Working Groups has been particularly productive in resolving a number of issues.

2.2 The work plan proposed by the SG to fulfill the WG1 tasking consists of investigation of a number of issues associated with utilization of security services, conduct of activities related to investigation of operational requirements and the 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 this progress and a summary follows.

Note: As with the previous report, new material in the tables is highlighted in ***bold.*** *In addition, the tables have been edited to place all completed items into a separate section.*

2.3.1 Recalling previous report of a breakthrough in resolution of the issue on cryptographic algorithm selection at the 11th and 12th meetings, progress by WG1SG2 has been significant since that time. The approach is holding true. It has been refined and work has taken place to define the necessary interfaces

2.3.2 Updates have been made to the draft Core SARPs and draft SV-1 and SV-8 of Doc 9705. These versions are proposed for acceptance as new baselines. The drafts of Core and SV-1 are essentially complete as regards the Security additions (although final updates will be needed for glossary and references). Major additions to SV-8 have been made in the area of the specifics of the domain parameters for the elliptic curve algorithm, definition of the primitives for the security service, and definition of the ATN Public Key Infrastructure. This draft of SV-8 has been reviewed in Gran Canaria by a subset of the SG and electronically by the whole SG. Although the draft contains material on Certificate Authorities and their interaction with ATN users, the placeholder for the ATN Certificate Authority Certificate Practices Statement remains just that. However, negotiations

are in progress to apply additional expert resources to this area.

2.3.3 Coordination with the other Working Groups continues. This has included participation in the WG1SG2 meetings by WG2 and JSG members, participation by a number of the WG1SG2 members in the WG3/SG3 meeting held in Toulouse in early September, and at the same time and venue, coordination with WG1JSG and representatives of WG3SG1 and WG3SG2. Electronic coordination among all the WG and SG has also been very helpful. Issues worked and resolved include:

2.3.3.1 Systems Management. Review of proposed Cross-Domain MIB and agreement that the Security requirements are limited to Security of System Management rather than Management of Security. This then is limited to Access Control. Remaining work is being done in the JSG.

2.3.3.2 Levels of Security. After a number of exchanges with WG3SG2 and reconsideration, WG1SG2 has reduced the originally proposed five 'levels' of security to three. These are none (for backward compatibility with Package 1), 'CM-security', and 'Application-security'.

2.3.3.3 Use of CM-forward and CM-update. During review of the WG1SG2 proposed application security solution, Frederic Picard noted that the description of CM exchanges did not include the CM-forward and CM-update. Consideration of his comments by WG1SG2 led the group to the conclusion (albeit, without precise quantitative evaluation) that the savings in A/G bandwidth associated with the CM-forward and CM-update could well be lost due to the additional data and exchanges necessary which are inherent in the CM-logon. This, along with suggestions that no known implementations were considering use of these features led the SG to recommend that these features not be used in Package 2 (Secure ATN). Further coordination with Fred and other WG3 members convinced WG1SG2 to reconsider this recommendation. WG1SG2 has accepted the requirement to include CM-forward and CM-update within the security solution and this work should be complete for WG1 meeting 16.

2.3.4 Validation planning is underway. A proposal for an overall approach has been tabled and discussed. A paper on validation objectives is expected at our SG meeting October 6 – 8. The draft validation report is on the agenda for the same meeting.

2.3.5 Papers prepared to define the public key infrastructure for the ATN and to describe the security solution as well as its operation will be incorporated into the Guidance Material. However as previously reported, focus has been on the specification of the solution and no new version is proposed.

3. Work progress

WG1SG2 Deliverable and Action List					
#		**Description**	**Assigned To**	**Due Date**	**Status**
2		SV1 SARPs updates and additions for Certificate Authorities	M. Bigelow	May 1999 **Final – December 1999**	**Inserted in SV-8 by T Mcparland based on WP; to be presented reviewed in preliminary at meeting 16**
3		Draft Certification Practices Statement	M. Bigelow	May 1999	Open
7		Digital Signature Managed Object fault attempts and failure			Expanded to A and B below
	B	Addition of high level requirements to guidance	M. Bigelow	**December** 1999	
9		Draft ATN Security Policy	P. Bourdier		
20		Updates to Annex 17 and Doc 8973	P. Bourdier	WG1 September 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. Papers submitted to M11 Preliminary updates to 8973, additional work on Annex 17 and first cut at organizational structure. Additional coordination is needed with Masoud and the ICAO Security office during the September – December time frame to make them aware of the proposed ATN SARPs relative to security
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	

WG1SG2 Deliverable and Action List					
#		**Description**	**Assigned To**	**Due Date**	**Status**
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.
29		Validation Plan	M. Bigelow	May 1999	**Paper "Proposed Validation Approach for ATN Security SARPs" presented to M12. Discussed and work continues. VOs proposed in M16; Draft Validation report to be provided to WGW**
30		Version *y.x* Proposed Final ATN Security SARPs text for Core, SV1, & SV8	SG2	September 1999	**September - Core and SV-1 essentially complete; SV-8 has most of material required. Final will be available December 1999**
31		Version *y.x* Proposed Final ATN Security GM	SG2	December 1999	**Draft will be available December 1999; Final in Spring 2000**
32		Validation Report	WG1SG2	November 1999	**Draft will be available December 1999; Final in Spring 2000**
33		Communiqué to WG3SG2 on the selection of security level.	MPB	July 1999	**Complete in M16 –** Email between GMB, MPB and FP. **Flimsy generated at M14 and sent to WG3SG2 Additional discussion at M15. Refined 'levels' to be selection of security type – either 'CM type' or 'Application type'. Conveyed to WG3SG2 and further discussed in TLS..**
Completed Actions					
1		Draft Core SARPs	R. Jones		Complete
4		Questions and Issues for WG2 and WG3 (Flimsies 2-3 and 2-4)			Complete

WG1SG2 Deliverable and Action List

#		Description	Assigned To	Due Date	Status
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	September 1999	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 **limited to access control** - Closed
8		Recommendations to RTCA 189/EUROCAE 53 on security in the initial ATN implementation	P. Hennig	June 1998	Complete - Deleted as not applicable.
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
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.

WG1SG2 Deliverable and Action List

#		Description	Assigned To	Due Date	Status
19		Concept of Operations		WG1 March 1998	Complete – Now part of the overall Guidance Material and will be tracked with it
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.
22		Copies of responses to state letter on cryptography import/export limitations	M. Bigelow	March 31	Complete – Distributed at BOD as WP911.
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). Complete – CAMAL delivered to SVT and available from same.
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	Complete – Placed on the server at HNL and will be updated on the CENA server

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 requirement parameter, which maps to the authentication requirement 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 **Directory Schema needs to come from WG1SG2**

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	K. Nguyen	Definition of requirements of Security Management	September 1998	Will produce for May 1999
8	WG1	SG2	SV-8	M. Bigelow	Definition of security algorithm	January 1999	Work in progress. SME have recommended a hybrid system. Investigation expanded to selection of algorithms for both asymmetric and symmetric. Considerable work done between M12 and M13. Hybrid system definition presented to M13.
9	WG3	SG**2**	SV-4	Editors **(JH, GS, FP)**	Selection of Security Level	December 1999	**Flimsy provided to WG3SG2 proposing**

WG1 SG2 – Security Issues List

#	Issue	Comments	Status
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
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.
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	**Resolution is if the certificate cannot be validated or if the certificate is revoked or expired then security services are not available.**

WG1 SG2 – Security Issues List

#	Issue	Comments	Status
11	Bi-directional AG IDRP 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.	Papers reviewed in M11. Resolution that a hard requirement exists for the ground to be able to authenticate the aircraft. The reverse direction will be worked as an option. Ongoing work defining overall mechanism will consider developing a mechanism to support bi-directional AG IDRP.
12	TEMPEST Risk Analysis	WG1SG2 must determine if this is needed. Papers are solicited.	**WP1405 presented. Agreement that something is needed. Evaluation needed of the applicability of FIPS 140-1 and possibility of establishment of ATN Common Criteria.**
13	Random number generation	Ensure (how?) that key generation methods that require random numbers produce real randomness rather than pseudo.	
14	Action on authentication failure	Sent flimsy to ADSP	Response received as WP15-21 (WG1) Only remaining issue is what organization establishes sunset dates. Refer back to WG1.
15	Use of separate keys for signing and encryption (key exchange)	Recommendation is that different keys be used for encryption from those used for signing. Consideration must be given to storage and complexity of resultant system.	
16	Implementation of levels of security by applications	Ian Valentine noted at Meeting 12 that the implementations by the A/G applications groups is on an all or nothing basis rather than rather than selection of a level.	Action to MPB to generate communiqué to WG3SG2 on the selection of security
17	How would certificates be revoked?	Normal process is via CRL.	**CRL will be used.**

WG1 SG2 – Security Issues List			
#	Issue	Comments	Status
18	What is the CA hierarchy and the CA relationship? Is there a need for cross certification?	**Proposed in W1512**	**Paper reviewed; Will be incorporated in SV-8 and reviewed there.**
19	After the CM dialogue has been initiated, the subsequent application dialogues can be both air or ground initiated. The proposed security architecture should not preclude one or the other.		**Agreed and implemented.**
20	Should ground applications access a certificate authority (CA) directly to retrieve certificates or should they rely on the ground CMA to validate required certificates and only pass the public key information to the applications?		**Proposed that the Ground CMA retrieve and validate certificates. Incorporated in SV-8 that way.**
21	A standard notation should be adopted for security functions and it should be used consistently on all related ATN documents. The notations provided in WP1308 can be used as a starting point and should follow the ANSI 9.63 standard as the prime governing document.	**The group agrees and this will be followed**	**In progress**
22	A National Common Criteria (required security levels and performance requirements) should be specified in ATN sub-volume 8. [One option is to follow the US FIPS-140]	**Paper to be produced Action B. Ramsey**	
23	Should the certificates (of ground CMAs and ground applications) be transferred over the air/ground interface or should they be pre-stored in the aircraft?		
24	How will the security SARPs be validated? What validation coordination is necessary?	**See Action 29**	
Completed Issues			

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
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

4. Recommendations

1. The Working Group is invited to review WP1607 as Version 4.1 draft Core SARPs. The Working Group is requested to accept this as new baseline Version 5.0. Further, because this is considered final text by WG1SG2 for the Security area, WG1 is invited to nominate an editor outside WG1SG2 to advance the changes in other areas in preparation for the WGW in December.

2. The Working Group is invited to review WP1608 as Version 6.1 draft SV-1 material for Doc 9705. The Working Group is requested to accept this as Version 7.0 noting, as above, that no major change is expected between this version and its final form relative to the Security material. As with the Core, WG1 is invited to nominate an editor outside WG1SG2.

3. The Working Group is invited to review WP1610 as Version 1.2 draft SV-8 material for Doc 9705. This version is substantially complete with the exception of areas previously noted. These areas will be completed prior to the December WGW meeting. The Working Group is asked to recall that the entire SG has only been able to review this electronically. The Working Group is requested to accept this as new baseline Version 2.0.