ATNP WG1WP1508
WG2WP515
WG3WP16-21

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL (ATNP)

WG1 – SYSTEMS PLANNING AND CONCEPT WORKING GROUP

24 - 26 May 1999
Naples, Italy

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 14th 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 WG1/14 meeting held January in Honolulu.

2. Work Plan

2.1 The subgroup has held two full subgroup meetings during this time. The first (SG meeting 11) was held immediately following the WG1 meeting in Honolulu (January) and the second (SG meeting 12) in early March in Annapolis MD. During meeting 12, an ad-hoc group was charged with working with cryptographic experts, provided through the good offices of NASA Ames, to come to agreement on the specific approach to a system of algorithms to meet the ATN need for Security. This group met several times, one of those in conjunction with WG3SG3 and the JSG.

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: a difference in this report from previous is that the new material in the tables is highlighted in **bold**)*

2.3.1 Major breakthrough in resolution of the issue on cryptographic algorithm selection. At its 11th meeting the subgroup came to grips with the reality that a change was necessary to the security framework originally proposed for the ATN and conveyed that change to the other working groups via communiqué to the rapportuers. The flimsies distributed with this communiqué described the new framework as a hybrid system of authentication utilizing both symmetric and asymmetric algorithms. In general terms, the asymmetric Public Key Infrastructure supports the initial authentication exchanges as well as establishment of the symmetric (session) key that is then used in subsequent exchanges. The general structure existed by meeting 12 (March 8 – 10) and there was agreement that the algorithm would be based on Elliptic Curve because of their shorter key lengths. However, at that point the approach centered on transport of the session key and two different methods were proposed to accomplish that. In addition, an alternative approach of session key establishment was being considered. Since there was a strong desire to convey as complete a picture as possible to WG3SG3 at its April meeting

in Palo Alto, an ad-hoc group was formed to work out the remaining details. Despite considerable effort, we were not able get all issues resolved. We were nonetheless able to provide WG3SG3 considerable detail relative to the framework and its operation. This was documented in a flimsy that was then distributed to SG2 and SG3 of WG3 (WG3SG3 PA Flimsy 1a). As noted in the flimsy, not all issues were resolved. The major one concerning WG3 involved determining the mechanism for establishment of a session key. At a meeting April 30 completed that determination and came to the agreement that follows. The general mechanism is that the aircraft and ground to establish a key derivation parameter during the CM logon exchange. The key derivation parameter is provided to application instantiations of the dialogue service. Each dialogue service instantiation creates a session key by first invoking the Elliptic Curve Key Agreement Scheme - Diffie-Hellman version (ECKAS-DH1) to derive a shared secret value and then invoking a Key Derivation Function (KDF1) using as input the shared secret value, the provided common key derivation parameter and other application unique key derivation parameters. WG1SG2 has provided the requirements for the complete approach in draft text for Sub-Volume VIII and further details of the approach in a WG1SG2 Working Paper both of which will be reviewed at WG1SG2's working meeting in Naples. Interested individuals involved in security are invited to attend the subject meeting.WG1SG2 regrets any delay caused to the other Working Groups deliverables but we are confident that as a result of the efforts of everyone involved we have a solid framework for ATN Security that meets the requirements with minimal A/G bandwidth utilization.

2.3.2 Updates have been made to the draft Core and SV-1 SARPs to reflect the new framework and these versions are proposed for acceptance as new baselines. The authentication framework has been incorporated into a draft of SV-8. This and proposed text for the section on the ATN X.509 certificate will be reviewed by WG1SG2 during our meeting here in Naples (Meeting 13 - May 26 – 28)

2.3.3 Coordination with the other Working Groups continues. One day of a combined WG3SG3 and JSG meeting held in Palo Alto was devoted to Security. In addition to the groups mentioned a representative of WG3SG2 and a number of WG1SG2 members attended the meeting.

2.3.4 Validation planning is underway. A proposal for an overall approach has been tabled and discussed and input paper(s) to this WG1 meeting are expected.

2.3.5 Work continues on the Guidance Material but focus has been on the algorithm-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	**May 1999**	Open
3		Draft Certification Practices Statement	M. Bigelow	**May 1999**	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	**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 - Closed
	B	Addition of high level requirements to guidance	M. Bigelow	**September 1999**	
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

WG1SG2 Deliverable and Action List

#		Description	Assigned To	Due Date	Status
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**
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). 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

WG1SG2 Deliverable and Action List					
#		**Description**	**Assigned To**	**Due Date**	**Status**
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
29		Validation Plan	M. Bigelow	May 1999	
30		Version *y.x* Proposed Final ATN Security SARPs text for Core, SV1, & SV8	SG2	September 1999	
31		Version *y.x* Proposed Final ATN Security GM	SG2	December 1999	
32		Validation Report	WG1SG2	November 1999	

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	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**.

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	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.	
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	

WG1 SG2 – Security Issues List			
#	Issue	Comments	Status
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.	

4. Recommendations

1. The Working Group is invited to review WP1513 as Version 3.1 draft Core SARPs. The Working Group is requested to accept this as new baseline Version 4.0 noting that, while this material is not expected to be final until the September meeting in Spain, no major change is envisioned from the version presented here.

2. The Working Group is invited to review WP1514 as Version 5.1 draft SV-1 material for Doc 9705. The Working Group is requested to accept this as Version 6.0 noting, as above, that no major change is expected between this version and its final form.

3. The Working Group is invited to note WP1515 as Version 1.2 draft SV-8 material for Doc 9705. This version contains only the changes related to the cryptographic algorithm selection and the hybrid system framework. The detail of this material will be reviewed by the subgroup in its meeting immediately following this Working Group 1 meeting. Additional working papers on proposed SV-8 material will also be considered in that meeting. Because of the and other material is requested to accept this as Version 1.0.