ATNP/WG3/WP3-16/07
May 11, 1999

INTERNATIONAL CIVIL AVIATION ORGANIZATION
AERONAUTICAL TELECOMMUNICATION NETWORK PANEL
Working Group 3

Napoli, 18-21 May 1999

ATNP/WG3/SG3 Activity Report

(Presented by Stephen Van Trees (USA))

Summary
Progress and prospects of SG3 (Upper Layer Architecture) are presented.

1. Introduction

ATNP/WG3 is responsible for Upper Layer Architecture (ULA). The group is responsible for SARPs Sub-Volume 4 (Upper Layer Communications Service), SARPs Sub-Volume 4 Enhancements (Secure Dialogue), and SARPs Sub-Volume 7 (Data Dictionary).

2. ATNP/WG3/SG3 Requirements

ATNP/WG3/SG3 in its work plan responds to the following requirements of ATNP/WG1.

Task	**Description**
B&C	Develop a Security Strategy for the ATN
X	Multicast

3. ATNP/WG3/SG3 Work Plan

ATNP/WG3/SG3 offers the following overview of its work plan.

SARPs	**Topic**	**Responsible**	**Napoli Deliverable**	**Madrid Deliverable**
Sub-Volume 4	Secure Dialogue	Mittaux-Biron	Security Draft	9705/ed 2 clause 4.8
Sub-Volume 4	Naming and Addressing	Kerr	9705/ed 2 clause 4.3bis	
Sub-Volume 4	Connectionless Dialogue	Van Trees	9705/ed 2 clause 4.7	
Sub-Volume 4	Generic ATN Comms	Kerr	9705/ed 2 clause 4.9	
Sub-Volume 4	ASO-ACSE	Van Trees		ASO-ACSE GM
Sub-Volume 7	Data Dictionary	Moulton	X.500 Schema Draft	9705/ed 2 clause 7

4. WG3 Issues

There are no issues to be co-ordinated at this meeting. The following issues bear watching:

- Security progress depends on a stable requirement from WG1/SG2,
- Directory validation must begin quickly
- System management notification of security fault must be specified.

5. Schedule

Observing the work plan, we note that Naming and Addressing, Connectionless Dialogue, and GACS are all in the validation phase.

The Secure Dialogue Service continues its intensive schedule.

The work on the Data Dictionary (X.500 Schema) begins validation.

6. Recommendation

WG3 is invited to approve the work plan provided.

ATNP/WG3/SG3 (Upper Layer Architecture)
19-22 April 1999
Palo Alto

ATNP/WG3/SG3 Meeting

The meeting was hosted by Jim Moulton on behalf of the US FAA.

Attendance

Mike Bigelow, ARINC [Security]
Tony Kerr, Eurocontrol
Gerard Mittaux-Biron, France
Jim Moulton, USA
Greg Saccone, USA
Steve Van Trees, USA

1. Review of SARPs

SG3 reviewed four PDRs at Toulouse. PDR 999010002 concerned re-use of transport. It had been discussed that re-use of transport after failure to set up an upper-layer association was allowed and implemented. The PDR was withdrawn in favor of 99040003. PDR 99030004 concerns abort inconsistencies in ULCS. P-ABORT Ind is indicated in text as illegal in RELEASE COLLISION. In fact, the state table indicates this is possible. The state table is correct. The PDR offers a little history of a flawed GEODE verification effort. PDR 99040002 suggests that the upper layers validate the received transport address. In fact, the flexibility between calling peer id and calling PSAP address. This will be noted in Guidance Material. PDR 99040003 is a PDR on the ISO/IEC 8327-1 handling of re-use of transport by the efficient session. The PDR has been investigated and the base standard stands.

Tony Kerr then presented the 9705/Amd 1 change pages. Most changes are in the registration area.

2. CNS/ATM-2 SARPs

Tony Kerr then presented the CNS/ATM-2 SARPs with enhancements listed as yellow pages. The incorporated enhancements are Generic ATN Comms Service (GACS), Connectionless Dialogue Service (CLDS), and Naming and Addressing. The text for each enhancement is complete and now under configuration control.

Tony Kerr then presented the CNS/ATM-2 Guidance Material, a compendium of associated issue papers on the enhancements.

Tony Kerr then presented the ATNP/3 validation paper for the upper-layer enhancements. CENA and the FAA both took and completed actions to describe their current validation efforts.

Gerard Mittaux-Biron then presented a paper on behalf of Frederic Picard. The paper suggests use of the application context name in the application version negotiation process. The paper points out that the notions of application context and version have been conflated in the ULCS SARPs. The assumption had been that a version of software would represent a complete implementation of an edition of SARPs. However, there are now many partial implementations from the same edition. There is a project need to announce the message set supported.
Upon examination it was felt that there did exist a requirement for application context, but that the solution was too radical. Flimsy 2 was issued to WG3/SG2 with a view to considering other options such as multiple ASEs, fna frequent version rolls.
It was noted that the SV4 makes frequent reference to the 'last' field of the OID, which is not an extensible way to have written the SARPs, if application context is later added.

3. Security

The group met for an entire day with WG1/SG2. Flimsy 1 records the results of that meeting. The general authentication requirements are peer entity authentication, data origin authentication, and protection from replay. The proposal is for entity authentication to be demonstrated by ground and airborne entities demonstrating possession of private keys. Replay protection is provided by timestamp or random-number exchange. Data origin authentication is provided by including HMAC (Hashed Mutual Authenticatio Code) . Each aircraft carries the public key of its Certificate Authority (CA). Each application is assigned a public and private key pair. The ULCS is responsible for exchange of the session CM key. Authentication of ground CM is also required.

The groups also derived a major clarification in that authentication failure is classed as a protocol error, rather than a quality of service failure. Thus, an aircraft may log on in clear, but if the aircraft attempts a secured logion and fails, it is not an aircraft. This had major implications for the security ASE. The security ASE will be rewritted for Napoli, and integrated in the 9705/ed 2 thereafter.

ACTION: (Van Trees) Overview of Security Service
ACTION: (Mittaux-Biron) Expansion of Security Macro Notation
ACTION: (Mittaux-Biron) Security-CM Relation

4. Directory

Jim Moulton presented the first draft of the X.500 schema and Directory Information Tree (DIT). SV7 requires review of the DIT for ATN-specific usage. Steve Van Trees took and completed actions to provide X.500 profile material for SV7. There is a tentative plan for a SV7-specific meeting in the Eastern USA the week on 26 July 1999. The work is critical for .the implementation of CNS/ATM-2 security and MHS.

5. Miscellaneous CNS/ATM-2

ACTION: (Van Trees) Upper Layer Multicast Addressing
ACTION: (Van Trees) ASO Template Development
ACTION: (Kerr) Fast Associate Enhancement

6. Base Standards

There is no current base standards activity. The connectionless upper-layer fast-byte amendments, and a connectionless ACSE defect report, will attain international standard status at the ITU-T SG7 meeting in Geneva in June 1999. The ASN.1 enhancements will also attain international standard status.

7. WG3 Napoli Prep

SG3 Report (Van Trees)
SV4/ed 1 Defect ("Rose") Pages (Kerr)
SV4/ed 2 Enhancement ("Yellow") Pages (Kerr)
Sub-Volume 4.8 Security (Mittaux-Biron)
Sub-Volume 7 Directory (Moulton)

8. Next Meeting

SG3 is contemplating its next meeting in 8-10 September 1999 in Toulouse collocated with JSG.