WG2/**WP 493**

International Civil Aviation Organization
Aeronautical Telecommunication Network Panel (ATNP)
WG2 and WG1/SG2 Meetings
Honolulu, Hawaii, USA
January 1999

Proposed Revisions to ICS (Doc 9705, Sub-Volume V) for IDRP Authentication

Presented by Tom McParland

Summary

The paper presents draft 0.1 text for Doc 9705, Sub-Volume V ATN Internet Security.

Attachment: Version 0.1 draft ATN Internet Security for DOC 9705, Sub-Volume V.

1. Introduction

This initial draft is based on scenarios described inW2WP492 which includes provision for optional mutual authentication of IDRP air-ground connections subject to local policy. This draft does not include provision for symmetric authentication mechanisms as described in working paper W2WP488.

2. Recommendation

Working Group 2 is invited to review the attached draft updates to Sub-VolumeV of Doc 9705.

Section 5.2.7 ATN Security Concept

Add item d) to Note 1:

d) Protecting routing information exchanges among ATN BISs.

Modify Notes 2 and 3 to:

Note 2. - There are no security mechanisms provided in the ATN Internet for protecting ATN Data Link applications. ATN Data Link applications are protected by upper layer security capabilities defined in Sub-volume IV in end systems which implement security services.

Note 3. – The ATN Internet supports item (d) through the use of ISO/IEC 10747 type 2 authentication in intermediate systems which implement security services.

Section 5.3.5.2 Air-Ground Route Initiation

Add the following requirements:

5.3.5.2.1.6 Airborne and Air-Ground routers which implement ISO/IEC 10747 type 2 authentication shall comply with the procedures specified in 5.3.5.2.14.

5.3.5.2.14 Procedures for exchanging authentication information

5.3.5.2.14.1 Signalling authentication information

5.3.5.2.14.1.1 If an Airborne or Air/Ground Router only supports authentication type 1 or if local policy is for type 1 authentication only for the Mobile Subnetwork, then the options part of the ISH PDU shall not contain the ATN authentication parameter.

5.3.5.2.14.1.2 If an Airborne or Air/Ground Router supports authentication type 2 and local policy requires signalling of single entity authentication for the Mobile Subnetwork, then the options part of the ISH PDU shall contain the ATN authentication parameter with the parameter value set to indicate single entity authentication.

5.3.5.2.14.1.3 If an Airborne or Air/Ground Router supports authentication type 2 and local policy requires signalling of mutual authentication for the Mobile Subnetwork, then the options part of the ISH PDU shall contain the ATN authentication parameter with the parameter value set to indicate mutual authentication.

5.3.5.2.14.1.4 If an Air/Ground Router supports authentication type 2 and the public key certificate of the aircraft is not in the Air/Ground Router's local cache, then if access to a supporting directory service is not available, the options part of the ISH PDU shall

contain the ATN authentication parameter with the parameter value set to indicate that the aircraft s certificate is required.

5.3.5.2.14.2 Encoding of the ATN authentication parameter in the ISO/IEC 9542 ISH PDU

The ATN authentication parameter shall be encoded as follows:

Parameter Code: 0000 0001
Parameter Length: 1 octet
Parameter Value:
Bit 1 = 1 Single Entity Authentication
Bit 1 = 0 Mutual Authentication
Bit 2 = 1 Aircraft Public-Key Certificate Required
Bit 2 = 0 Aircraft Public-Key Certificate Not Required
Bits 3 through 8 = 0

Renumber current 5.3.5.2.14 to 5.3.5.2.15

Section 5.8

Modify 5.8.1.2 as follows: (change references to 5.8.3.2.10)

5.8.1.2 Applicability of Requirements

5.8.1.2.1 All ATN Airborne Routers, with the exception of Airborne Routers implementing the procedures for the optional non-use of IDRP, shall comply with the provisions contained in 5.8.2, 5.8.3, 5.8.3.2.2 to 5.8.3.2.5 inclusive, 5.8.3.2.8 to 5.8.3.2.9 inclusive, 5.8.3.2.11, 5.8.3.3.2.1, 5.8.3.3.3 and the APRLs specified for an Airborne Router in 5.8.3.4.

5.8.1.2.3 All ATN Air/Ground Routers shall comply with the provisions contained in 5.8.2, 5.8.3, 5.8.3.2.2 to 5.8.3.2.9 inclusive, 5.8.3.2.9.11, 5.8.3.3.2.2, 5.8.3.3.3 and the APRLs specified for an Air/Ground Router in 5.8.3.4.

5.8.1.2.4 All Ground/Ground Inter-Domain Routers shall comply with the provisions contained in 5.8.2, 5.8.3.2.2 to 5.8.3.2.9 inclusive, 5.8.3.2.11, 5.8.3.3.2.2, 5.8.3.3.3 and the APRLs specified for an Ground/Ground Router in 5.8.3.4.

5.8.1.2.5 All ATN Routers shall be compliant with 5.8.3.2.10.1

5.8.1.2.6 ATN Routers implementing authentication type 2 procedures shall be compliant with 5.8.3.2.10.2

Modify current note and add note to 5.8.2.1.2

Note 1.¥The use of ISO/IEC 9542 Configuration Information over Mobile Subnetworks in support of Air/Ground route initiation is specified in 5.3.5.2.6

Note 2.¥ The use of ISO/IEC 9542 Configuration Information over Mobile Subnetworks in support of IDRP Authentication Type 2 is specified in 5.3.5.2.14.

Add to 5.8.2.2

5.8.2.2.2 An implementation which supports IDRP Authentication Type 2 shall comply with the designated option-status qualified by the predicate symbol **A2.**

Modify Table 5.8-1 (APRL)

OOpt-r	<r> (ignore) unsupported or unknown options	ATN SARPs Ref.: 5.3.5.2.14	M	A2:X
OOpt-s	<s> Other options	ATN SARPs Ref.: 5.3.5.2.14	P	A2:M

5.8.3.2.10 BISPDU Authentication

5.8.3.2.10.1 Authentication Type 1

Note. - Authentication Type 1 is performed by an Airborne or Air/Ground Router which does not support authentication type 2 or if local policy (for a router which does support authentication type 2) is for authentication type 1 only for the Mobile Subnetwork.

5.8.3.2.10.1.1 ATN Routers shall support the validation of BISPDUs using Authentication Type 1.

5.8.3.2.10.1.2 When an ATN Router initiates a BIS-BIS connection, it shall set the value of the Authentication Code in the OPEN PDU to 1, in order to indicate that the Validation field in the header of all BISPDU sent over the BIS-BIS connection will contain an unencrypted message digest..

Editor's note: the requirement is carried forward from current SARPs; however, making the qualifying clause ", in order to…" a note rather than part of the requirement statement would simplify many of the requirement statements in this section.

5.8.3.2.10.1.3 When an authentication code of 1 is specified in the Authentication Code of the OPEN BISPDU that initiated a BIS-BIS connection, then an ATN Router shall generate a validation pattern according to clause 7.7.1 of ISO/IEC 10747, for each BISPDU that it sends over that connection, and similarly validate the validation pattern of all received BISPDUs on such a connection.

5.8.3.2.10.1.4 The type 1 authentication code shall be generated according to the MD4 specification published in RFC 1320.

Note 1.¥ The interpretation of MD4 given in Annex B of ISO/IEC 10747 is open to ambiguous interpretation and may lead to interoperability problems.

Note 2.¥ RFC 1320 supersedes RFC 1186 which was the basis for ISO/IEC 10747 Annex B. Specifications of MD4 algorithm contained in these two RFC documents are technically equivalent

5.8.3.2.10.2 Authentication Type 2

5.8.3.2.10.2.1 ATN Routers supporting authentication type 2 shall perform BISPDU validation for BISPDUs in the direction of OPEN PDU.

Note. - Performing BISPDU validation in the direction of the OPEN PDU permits single entity authentication, i.e., authentication type 1 may be performed in one direction of an IDRP connection with concurrent authentication type 2 in the other direction.

5.8.3.2.10.2.2 When an Airborne Router, which supports authentication type 2, initiates a BIS-BIS connection over a Mobile Subnetwork and local policy does not indicate authentication type 1 only, it shall set the value of the Authentication Code in the OPEN PDU to 2, in order to indicate that the Validation field in the header of BISPDUs sent over the BIS-BIS connection in the direction of OPEN PDU will contain a digital signature.

5.8.3.2.10.2.3 When an Airborne Router initiates a BIS-BIS connection over a Mobile Subnetwork on which 'aircraft public-key certificate required' was signalled in the received ISH PDU, it shall store its public-key certificate in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.4 When an Air-Ground Router initiates a BIS-BIS connection over a Mobile Subnetwork on which single entity authentication was signalled in the received ISH PDU, it shall set the value of the Authentication Code in the OPEN PDU to 1, in order to

indicate that the Validation field in the header of BISPDUs sent over the BIS-BIS connection in the direction of OPEN PDU will contain an unencrypted message digest.

5.8.3.2.10.2.5 When an Air-Ground Router initiates a BIS-BIS connection over a Mobile Subnetwork on which Mutual Authentication was signalled in the received ISH PDU and local policy indicates mutual authentication permitted, it shall set the value of the Authentication Code in the OPEN PDU to 2 and store its public-key certificate in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.6 When an Air-Ground Router initiates a BIS-BIS connection over a Mobile Subnetwork on which Mutual Authentication was signalled in the received ISH PDU and local policy does not indicate mutual authentication permitted, it shall set the value of the Authentication Code in the OPEN PDU to 1.

5.8.3.2.10.2.7 When an Airborne Router receives an OPEN PDU with the Authentication Code set to 1 on a BIS-BIS connection on which it has signalled mutual authentication during the ISH exchange, then if local policy is not to negotiate to single entity authentication, it shall terminate the BIS-BIS connection.

5.8.3.2.10.2.8 When an Airborne or Air-Ground Router receives an Open PDU with its peer's public-key certificate in the Authentication Data field, it shall authenticate the certificate using the certificate authority's public key according to the procedure in section *tbd* of Sub-Volume VII.

5.8.3.2.10.2.9 If authentication of a public-key certificate received in an OPEN PDU fails, the Airborne or Air-Ground Router shall terminate the BIS-BIS connection.

5.8.3.2.10.2.10 When an Airborne or Air-Ground Router sends a BISPDU on a BIS-BIS connection in which the Authentication Code was set to 1 in the OPEN PDU, it shall generate a validation pattern according to clause 7.7.1 of ISO/IEC 10747, for each BISPDU that it sends over that connection.

5.8.3.2.10.2.11 When an Airborne or Air-Ground Router sends a BISPDU on a BIS-BIS connection in which the Authentication Code was set to 2 in the OPEN PDU, it shall generate a digital signature according to the procedure in section *tbd* of Sub-Volume VIII, for each BISPDU that it sends over that connection.

5.8.3.2.10.2.12 When an Airborne or Air-Ground Router receives a BISPDU on a BIS-BIS connection in which the Authentication Code was set to 1 in the OPEN PDU, it shall validate the message digest in the BISPDU header according to clause 7.7.1 of ISO/IEC 10747.

5.8.3.2.10.2.13 If validation of the message digest of a received BISPDU fails, the Airborne or Air-Ground Router shall terminate the BIS-BIS connection.

5.8.3.2.10.2.14 When an Airborne or Air-Ground Router receives a BISPDU on a BIS-BIS connection in which the Authentication Code was set to 2 in the OPEN PDU, it shall authenticate the digital signature according to the procedure in section *tbd* of Sub-Volume VIII.

5.8.3.2.10.2.15 If authentication of the digital signature of a received BISPDU fails, the Airborne or Air-Ground Router shall terminate the BIS-BIS connection.

Section 5.8.3.5.8

The note from the current APRL should be deleted:

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
AUTH	Does this BIS correctly authenticate the source of a BISPDU?	7.7.2	O	M	M	M

Note. ¥ Only support for an Authentication Code 1 is required.

The current note is not consistent with the APRL since the reference to 7.7.2 is for Authentication Type 2. This appears to be a problem with the IDRP PICS Proforma which does not have an item for Authentication Type 1 or Authentication Type 3.