**WG2/WP 522**

**International Civil Aviation Organization**
**Aeronautical Telecommunication Network Panel (ATNP)**
**Working Group 2**
**Naples, Italy**
**May 1999**

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

Presented by Tom McParland

Summary

The paper presents draft 1.0 text for Doc 9705, Sub-Volume V ATN Internet Security.

**Attachment:** Version 1.0 draft ATN Internet Security for DOC 9705, Sub-Volume V.

## 1. Introduction

This initial draft is based on W2WP518 which describes scenarios for IDRP authentication using key agreement and message authentication code schemes.

## 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 does not permit authentication type 2, 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 permits authentication type 2, then the options part of the ISH PDU shall contain the ATN authentication parameter.

5.3.5.2.14.1.3 If an Airborne Router supports authentication type 2 and local policy permits mutual authentication and the public key of the Air-Ground router has not been pre-stored, then the options part of the ISH PDU shall contain the ATN authentication parameter with the parameter value set to indicate public key certificate required.

5.3.5.2.14.1.4 If an Airborne Router supports authentication type 2 and local policy does not permit mutual authentication, then the options part of the ISH PDU shall contain the ATN authentication parameter with the parameter value set to indicate public key certificate not required.

5.3.5.2.14.1.5 If an Airborne Router supports authentication type 2 and the public key of the Air-Ground router has been pre-stored, then the options part of the ISH PDU shall contain the ATN authentication parameter with the parameter value set to indicate public key certificate not required.

5.3.5.2.14.1.6 If an Air/Ground Router supports authentication type 2 and if access to a supporting directory service is not available, then the options part of the ISH PDU shall contain the ATN authentication parameter with the parameter value set to indicate public key certificate required.

5.3.5.2.14.1.7 If an Air/Ground Router supports authentication type 2 and if access to a supporting directory service is available, then the options part of the ISH PDU shall contain the ATN authentication parameter with the parameter value set to indicate public key certificate not 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:** 1100 0001
**Parameter Length:** 1 octet
**Parameter Value:**
Bit 1 = 1 Public-Key Certificate Required
Bit 1 = 0 Public-Key Certificate Not Required
Bits 2 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 permits authentication type 1 in the event the peer router does not support authentication type 2.*

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, **which does not support authentication type 2,** initiates a BIS-BIS connection, it shall set the value of the Authentication Code in the OPEN PDU to 1

5.8.3.2.10.1.3 When an Airborne or Air-Ground Router, **which has included the ATN Authentication Parameter in an ISH sent to a peer router,** receives an OPEN PDU with the Authentication Code field set to 1, it shall process the OPEN PDU only if permitted to do so by local policy.

5.8.3.2.10.1.4 When an authentication code of 1 is specified in the Authentication Code of the OPEN PDU 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.

5.8.3.2.10.1.5 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 An ATN Router, which supports authentication type 2, shall initiate a BIS-BIS connection with authentication type 2 only if type 2 authentication is permitted by local policy.

5.8.3.2.10.2.2 An Airborne or Air-Ground Router shall initiate a BIS-BIS connection with authentication type 2 over an Air-Ground subnetwork only if the ATN Authentication Parameter was received from the peer router in the ISH PDU.

5.8.3.2.10.2.3 When an ATN Router initiates a BIS-BIS connection with authentication type 2, it shall set the value of the Authentication Code to 2 in the OPEN PDU.

5.8.3.2.10.2.4 When an ATN Router initiates a BIS-BIS connection with authentication type 2, it shall store a random value, generated with the ATN Random Value Function

(ARVF) according to the procedure of section 8.5 of Sub-Volume VIII, in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.5 When an Airborne or Air-Ground Router initiates a BIS-BIS connection with authentication type 2 over an Air-Ground subnetwork for which 'public-key certificate required' was signalled in the received ISH PDU by the peer router, it shall store its public-key certificate in the Authentication Data field of the OPEN PDU if permitted to do so by local policy.

5.8.3.2.10.2.6 When an Air-Ground Router initiates a BIS-BIS connection with authentication type 2 over an Air-Ground subnetwork and a valid public key certificate for the Airborne could not be retrieved for the Airborne router, it shall signal 'public-key certificate required' in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.7 When an Airborne Router initiates a BIS-BIS connection with authentication type 2 over an air-ground subnetwork for which local policy is to perform mutual authentication and a valid public key certificate for the Air-Ground router could not be retrieved from its pre-stored data base, it shall signal 'public-key certificate required' in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.8 When a Ground-Ground or Air-Ground Router initiates a BIS-BIS connection with authentication type 2 over a ground subnetwork, it shall store its public-key certificate in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.9 When an ATN Router initiates a BIS-BIS connection with authentication type 2, it shall store a type 1 authenticator, generated according to clause 7.7.1 of ISO/IEC 10747, in the Validation Pattern field of the OPEN PDU.

*Note. - Storing a type 1 authenticator in the Validation Pattern field while Code 2 is stored in the Authentication Code field (only for the OPEN PDU) is an ATN specific convention in support of type 2 authentication.*

5.8.3.2.10.2.10 When an ATN Router receives an OPEN PDU with the Authentication Code field set to 2 and the Authentication Data field contains the peer router's public key certificate, it shall verify the certificate using the ATN Verification Primitive (AVP) according to the procedure of section 8.5 of Sub-Volume VIII.

5.8.3.2.10.2.11 When an ATN Router receives an OPEN PDU with the Authentication Code field set to 2, it shall compute a shared secret value using the ATN Secret Value Derivation Primitive (ASVDP) according to the procedure of section 8.5 of Sub-Volume VIII; and derive a shared session key using the ATN Key Derivation Function (AKDF).

5.8.3.2.10.2.12 When an Airborne or Air-Ground Router, which has sent an OPEN PDU, receives an OPEN PDU with which 'public-key certificate required' in the Authentication Data Field, it shall resend its OPEN PDU with its public-key certificate in the Authentication Data field of the OPEN PDU if permitted to do so by local policy.

5.8.3.2.10.2.13 If an ATN Router has derived a shared session key for a BIS-BIS connection, it shall store the Airborne Router's random value, the Air-Ground Router's random value, and a message authenticator over the BISPDU, generated using the ATN Keyed Message Authentication Code Scheme (AMACS) according to the procedure of section 8.5 of Sub-Volume VIII, in the Validation Pattern field of any BISPDU it sends over the BIS-BIS connection.

5.8.3.2.10.2.14 When an ATN Router, which has derived a shared session key, receives a BISPDU with a type 2 message authenticator in the Validation Pattern field, it shall verify the authenticator using the ATN Keyed Message Authentication Code Scheme (AMACS) according to the procedure of section 8.5 of Sub-Volume VIII.

5.8.3.2.10.3 Format and Encoding of IDRP BISPDU fields to support Authentication Type 2

5.8.3.210.3.1 Authentication Data field

*Formats:*

*Random Variable*
*Public Key Agreement Key*
*Public Key Certificate*

5.8.3.2.10.3.2 Validation Pattern Field

*Format:*

*Aircraft Random Variable, Ground Random Variable, HMAC Seal*

**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.*