WG1/SG2 WP___
WG2/**WP 492**

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

Mutual Authentication Service for IDRP Air-ground Connections

Presented by Tom McParland

Summary

The draft SARPS materials require mutual authentication among Air-ground and Ground BISs and single entity authentication (only) between Air-ground and Airborne BISs. It is proposed that optional mutual authentication be provided between Air-ground and Airborne BISs subject to local policy constraints on its operation.

1. Introduction

The draft SARPS materials require mutual authentication among Air-ground and Ground BISs and single entity authentication (only) between Air-ground and Airborne BISs. The motivation for this distinction is to save air-ground bandwidth, since it is recognized that mutual authentication would require transmission of the Air-ground router's certificate. Additionally, it is recognized that potential loss of service of an Air-ground router would have more severe consequences than loss of service of an airborne router. Although bandwidth is a serious constraint with current generation air-ground subnetworks, it may be possible to minimize the certificate size. It may also turn out that the likelihood of an attack will increase over time, thereby increasing the risk level to the airborne router.

It is proposed that optional mutual authentication be provided between Air-ground and Airborne BISs; however, local policy should determine whether it is in fact performed on a particular subnetwork.

2. Discussion

2.1 Single entity and mutual authentication

Annex B (clause B.2.a) in X.509, describes peer entity authentication as follows:

> "*Peer entity authentication* – This service provides corroboration that a user in a certain instance of communication is the one claimed. Two different peer entity authentication services may be requested:
>
> – *single entity authentication* (either *data origin* entity authentication or *data recipient* entity authentication).
>
> – *mutual authentication*, where both users communicating authenticate each other. "

2.2 Current requirement for single entity authentication

ATNP WG1/WP14-08, which presents draft text for Sub-Volume VIII of Doc 9705, contains the following:

> 8.3.1.5.1.1 ATN Boundary Intermediate Systems (BISs) supporting ATN security services shall support the use of ATN security provisions for authentication, using digital signatures, of routing exchanges between air-ground and ground BISs and from airborne BISs to air-ground BISs, but not vice versa, as defined in Sub-Volume V.

This requirement specifies mutual authentication among Air-ground and Ground BISs and single entity authentication between Air-ground and Airborne BISs. It prohibits mutual authentication between Air-ground and Airborne BISs.

2.3 ISH signaling of mutual authentication service

In previous working group 2 activities, the concept of using the ISH exchange to signal additional information was developed. In the context of authentication, the concept was for the Air-ground router to use the ISH PDU to direct the Airborne router to send back its public-key certificate in the Authentication Data field of the Open PDU. In this way authentication could be performed even if the Air-ground router could not access a directory of public-key certificates.

It is proposed that this approach be taken a step further and that the ISH exchange also be used by an Airborne router to signal mutual authentication of the BIS-BIS connection. Similar to the above, the concept would be for the Air-ground router to respond to such an ISH PDU by sending its public-key certificate in the Open PDU. In this way each BIS would have the public key of its peer and thus mutual authentication could be performed.

2.4 Local policy control of mutual authentication service

It is further proposed that local policy determine if mutual authentication is to be performed on a particular subnetwork. In the event that mutual authentication has been signaled by the Airborne router in the ISH exchange, the Air-ground router will send its certificate in the Authentication Data field only if local policy of the Air-ground router permits mutual authentication. If local policy prohibits mutual authentication, the Air-ground router would not send its certificate. If the Airborne router receives an Open PDU without Air-ground router authentication data, it will continue the connection with single entity authentication or terminate it based on its own local policy (i.e., whether or not to negotiate down to single entity authentication)

2.5 Single entity authentication in IDRP

Clause 6.2, OPEN PDU, Authentication Code, b) of the ISO 10747 defines Code 2 as follows:

> “Code 2 indicates that the Validation Pattern field in the header of each BISPDU provides both peer-BIS authentication and data integrity for the contents of the BISPDU. The specific mechanism used to generate the validation pattern is mutually agreed to by the pair of BISs, but is not specified by this International Standard.”

Annex D.1 of ISO 10747 states:

> “For an OPEN PDU with an authentication code field of 2, and for all BISPDUs that flow on a BIS-BIS connection established by this OPEN PDU, the validation field will contain a 16-octet encrypted checksum.”

The above descriptions imply support for mutual authentication only, that is, there no explicit provision for type 1 authentication in one direction of an IDRP connection with concurrent type 2 authentication in the other direction.

It is proposed that in order to support single entity authentication, Code 1 be interpreted to indicate data integrity in the direction of the Open PDU and Code 2 be interpreted to indicate data origin peer-BIS authentication in the direction of the Open PDU.

2.6 Use of the Authentication Data field

Clause D.1, a), 2), 1) of ISO 10747 describes use of the Authentication Data field as follows:

> "However, the "Authentication Data" field of IDRP's OPEN PDU can be used to specify an algorithm indirectly in accordance with the local agreements of the two communicating BISs."

As the above text describes, the Authentication Data field was intended as an indicator of which algorithm to apply for mutual authentication; however, it is not restricted to such use. Therefore, it is proposed as described above, that the Authentication Data field be used as a vehicle for obtaining the aircraft certificate in the event that the Air-ground router does not have access to a supporting directory service and it is also proposed that the Authentication Data field be used for exchange of the air-ground router's certificate in support of mutual authentication.

3. IDRP peer entity authentication scenarios

3.1 Single entity authentication

1. During the ISH exchange, the Airborne router signals single entity authentication.

2. The Air-ground router retrieves the aircraft's public-key certificate from a supporting directory service. The Air-ground router authenticates the aircraft's certificate using the certificate authority's public key.

3. The Air-ground router sends an Open PDU with Code 1 in the Authentication Code field and with a type 1 (MD4) authenticator in the Validation Pattern field.

4. The Airborne router sends an Open PDU with Code 2 in the Authentication Code field and its digital signature in the Validation Pattern field.

5. Upon receipt of the Open PDU, the Air-ground router authenticates the aircraft's signature using the aircraft's public key. If authentication fails, the connection is terminated.

6. The Air-Ground router sends a type 1 authenticator as the Validation Pattern field in the header of all subsequent BISPDUs.

7. The Airborne router sends its digital signature as the Validation Pattern field in the header of all subsequent BISPDUs.

3.2 Single entity authentication without supporting directory service

1. During the ISH exchange, the Airborne router signals single entity authentication and the Air-ground router signals non-availability of the directory service.

2. The Air-ground router sends an Open PDU with Code 1 in the Authentication Code field and with a type 1 authenticator in the Validation Pattern field.

3. The Airborne router sends an Open PDU with Code 2 in the Authentication Code field, its certificate in the Authentication Data field, and its digital signature in the Validation Pattern field.

4. Upon receipt of the Open PDU, the Air-ground router authenticates the aircraft's certificate using the certificate authority's public key and authenticates the aircraft's signature using the aircraft's public key. If authentication fails, the connection is terminated.

5. The Air-Ground router sends a type 1 authenticator as the Validation Pattern field in the header of all subsequent BISPDUs.

6. The Airborne router sends its digital signature as the Validation Pattern field in the header of all subsequent BISPDUs.

3.3 Mutual authentication

1. During the ISH exchange, the Airborne router signals mutual authentication.

2.a If local policy is to support mutual authentication, the Air-ground router sends an Open PDU with Code 2 in the Authentication Code field, its certificate in the Authentication Data field, and its digital signature in the Validation Pattern field.

2.b If local policy is not to support mutual authentication, the Air-ground router sends an Open PDU with Code 1 in the Authentication Code field and a type 1 authenticator in the Validation Pattern field.

3. The Airborne router sends an Open PDU with Code 2 in the Authentication Code field, its certificate in the Authentication Data field, and its digital signature in the Validation Pattern field.

4. Upon receipt of the Open PDU, the Air-ground router authenticates the aircraft’s certificate using the certificate authority’s public key and authenticates the aircraft’s signature using the aircraft’s public key. If authentication fails, the connection is terminated.

5. Upon receipt of the Open PDU, the Airborne router examines the Authentication Code field,

> a. if Code 2 is indicated, the Airborne router authenticates the Air-ground router’s certificate using the certificate authority’s public key and authenticates the Air-ground router’s signature using the Air-ground router’s public key. If authentication fails, the connection is terminated.
>
> b. if Code 1 is indicated and the Airborne router’s local policy is not to negotiate to single entity authentication, the connection is terminated.

5.a If local policy is to support mutual authentication, the Air-ground router sends its digital signature as the Validation Pattern field in the header of all subsequent BISPDUs.

5.b If local policy is not to support mutual authentication, the Air-ground router sends a type 1 authenticator as the Validation Pattern field in the header of all subsequent BISPDUs.

6. The Airborne router sends its digital signature as the Validation Pattern field in the header of all subsequent BISPDUs.

4. Recommendations

a) Previous WG2 recommendations to use optional ISH PDU parameters field to signal non-availability of the directory service should be extended to optionally signal mutual authentication.

b) The Authentication Code field should apply in the direction of the Open PDU in support of single entity authentication.

c) Previous WG2 recommendations to use the Authentication Data field as a vehicle for exchange of the Airborne router’s certificate should be extended to include optional exchange of the air-ground router’s certificate in support of mutual authentication.

d) WG1 should modify Sub-Volume VIII of Doc 9705 such that mutual authentication between Air-ground and Airborne BISs is not explicitly prohibited.