WG 2/WP 585

Aeronautical Telecommunication Network Panel (ATNP)
Working Group 2
Meeting 21
July 11 –14, 2000
Limerick, Ireland

Draft
IDRP Authentication
Guidance Material

Presented by Tom McParland

Summary

IDRP authentication draft guidance material is presented which correspond to the IDRP security enhancements in Draft Edition 3 of Sub-Volumes V and VIII.

1. Introduction

This paper is an update to WG2WP534. This paper presents IDRP authentication scenarios using the ATN Key Agreement Scheme (AKAS) and the ATN Keyed Message Authentication Code Scheme (AMACS) which are defined in the draft Sub-Volume VIII. This paper differs functionally from WP534 in that updated requirements terminology and notation from SV V and SV VIII is followed.

Scenarios are presented for authentication of air-ground and ground-ground IDRP connections. The scenarios address local policy for Type 2 authentication support and for unilateral and mutual authentication, certificate availability conditions, and replay and manipulation protection.

2. Terms

The following terms, which are included in Sub-Volume I are used herein.

authentication information - Information used to establish the validity of a claimed identity.

authentication exchange - A mechanism intended to ensure the identity of an entity by means of information exchange.

user certificate; public key certificate; certificate - The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.

certificate authority; certification authority - An authority trusted by one or more users to create and assign certificates.

certificate path; certification path - An ordered sequence of certificates of objects in the DIT which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

cryptographic checkvalue; tag - Information which is derived by performing a cryptographic transformation on the data unit.

cryptographic scheme - A cryptographic scheme consists of an unambiguous specification of a set of transformations capable of providing a cryptographic service when properly implemented and maintained.

data integrity - The property that data has not been altered or destroyed in an unauthorized manner.

data origin authentication - The corroboration that the source of data received is as claimed.

key agreement - A method for negotiating a key value on-line without transferring the key, even in an encrypted form, e.g., the Diffie-Hellman technique.

key agreement scheme - A key agreement scheme is a key establishment scheme in which the keying data established is a function of contributions provided by both entities in such a way that neither party can predetermine the value of the keying data.

key derivation function - A key derivation function is a function which takes as input a shared secret value and outputs keying data suitable for later cryptographic use.

manipulation - The replacement, insertion, deletion, or misordering of user data during a communication by an unauthorized user.

message authentication code or MAC scheme - A message authentication code or MAC scheme is a cryptographic scheme capable of providing data origin authentication and data integrity.

peer-entity authentication - The corroboration that a peer entity in an association is the one claimed.

public key - (In a public key cryptosystem) that key of a user's key pair which is publicly known.

private key; secret key (deprecated) - (In a public key cryptosystem) that key of a user's key pair which is known only by that user.

replay - The recording and subsequent replay of a communication at some later time.

session key - A key established by a key establishment scheme.

shared secret value - An intermediate value in a key establishment scheme from which keying data is derived.

strong authentication - Authentication by means of cryptographically derived credentials

3. Proposed Guidance

3.1 IDRP Authentication Types

ATN Boundary Intermediate Systems are required to provide secured exchanges of routing information based on provisions of ISO/IEC 10747. ISO/IEC 10747 defines three distinct types of "authentication", the first two of which are used by ATN BISs. IDRP Type 1 authentication does not actually provide an authentication service; rather, it is essentially a data integrity service. IDRP Type 1 authentication provides protection from routing information exchanges being altered or destroyed in an unauthorized manner. IDRP Type 1 authentication uses the Message Digest 4 (MD4) algorithm.

IDRP Type 2 authentication on the other hand provides for true authentication. Peer-entity authentication provides the corroboration that a peer ATN BIS in an IDRP connection is the one claimed. Further, once peer entity authentication has been established, data origin authentication is provided for each BISPDU transferred on the connection, i.e., corroboration that the source of received BISPDUs is as claimed is provided. Data integrity is provided along with data origin authentication.

3.2 Mutual Entity Authentication Vs Single Entity Authentication

Only single entity authentication is strictly required on IDRP air-ground connections, that is, the air-ground router must authenticate the airborne router. The rational is based on bandwidth considerations in the context of the relative consequence of an attack against the routing information base of an air-ground router versus an attack against the routing information base of an airborne router. It is clear that the former attack would be of more severe consequence than the latter, and therefore ATN boundary intermediate systems, which support ATN security services, should apply strong authentication to exchanges affecting the ground routing information base. It is important to note, however, that mutual authentication is not precluded. ATN boundary intermediate systems, which provide ATN security services, are required to be capable of mutual entity authentication. Whether or not to invoke mutual entity authentication service is a matter of local policy.

3.3 IDRP Type 2 Authentication Mechanism

Entity authentication can be achieved in an asymmetric cryptographic environment by the claimant demonstrating possession of a private key. In IDRP Type 2 authentication, ATN BISs demonstrate possession their private keys indirectly. They explicitly demonstrate possession of a shared secret key by using the key in a Message Authentication Code applied to the exchange of routing information. Possession of the shared secret key implies possession of a specific private key since the shared secret key could only be successfully derived under the key agreement scheme if the claimant is also in possession of a private key corresponding to a verified public key. Verification of the claimant's public key is accomplished by obtaining it from a trusted third party, i.e., in a certificate signed by a certificate authority.

3.4 Replay and Manipulation Protection

Protection from replay and interception attacks is provided in the following scenarios through a challenge-response exchange. A random variable is generated by each intermediate system and sent in the OPEN BISPDUs. The random variables are included as shared data in derivation of the MAC key for the connection. Verification of the challenge is achieved if the first UPDATE BISPDU contains a valid MAC tag. Subsequent BISPDUs are protected from replay and interception by the IDRP sequence numbers.

3.5 Scenarios for Authentication Of Boundary Intermediate System Exchanges

3.5.1 Air-Ground IDRP Connections

Air-Ground IDRP connection exchanges are depicted in figure 1 and described in the following scenario description.

1. During the ISH exchange, the airborne and air-ground routers signal type 2 authentication by setting bit 1 of the value field of the ATN Data Link Capability Parameter in the ISH PDU and by setting bit 2 to indicate whether or not the peer router needs to send its certificate in the OPEN BISPDU.

   Note 1. – If either router does not signal support for type 2 authentication by setting bit 1 in the ISH PDU (i.e., a Package-1 router) then the IDRP connection will be established without security (i.e., with Type 1 authentication) unless the local policy of either router prohibits an unsecured service.

   Note 2. – For the airborne router, the bit 2 parameter value setting will depend on whether or not an authentic public key of the air-ground router has been pre-stored. The parameter will indicate public key certificate required if the public key has not been pre-stored. The parameter will indicate public key certificate not required if the public key has not been pre-stored.

   Note 3. – For the air-ground router, the bit 2 parameter value setting will depend firstly on whether or not access to a supporting certificate delivery service is available and secondly whether certificate path validation is performed prior to or after sending the ISH PDU. The parameter will indicate public key certificate required if access to a supporting delivery service is not available. The parameter will indicate public key certificate not required if access is available and successful validation is performed prior to sending the ISH PDU. The parameter will indicate public key certificate required if validation is performed subsequent to sending the ISH PDU. If validation fails, the ISH PDU will not be sent for the case of prior validation and the IDRP connection will not be established in either case.

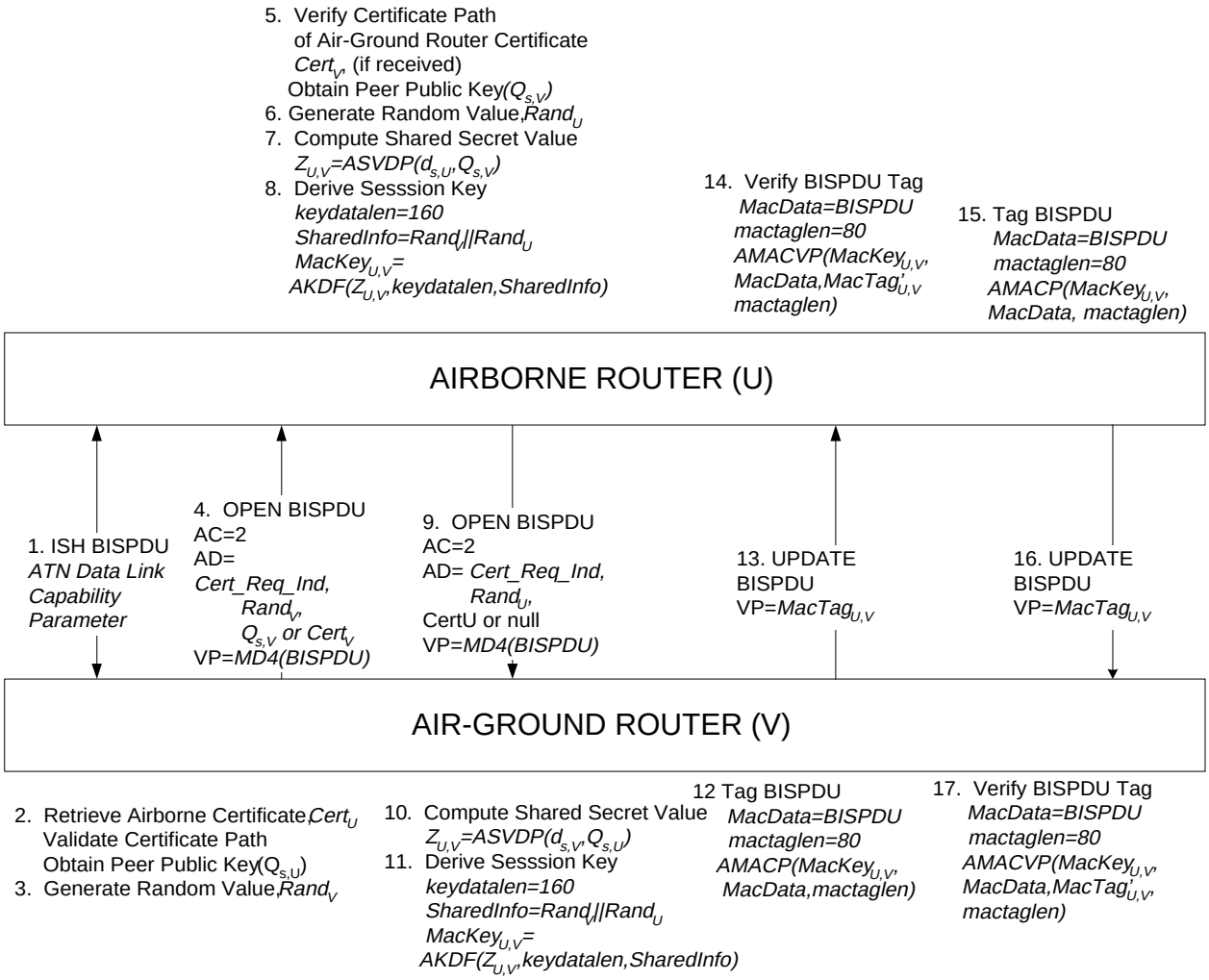

Figure 1 – Airborne and Air-Ground Router IDRP Authentication Exchanges

2. The air-ground router retrieves the aircraft's public-key certificate, $Cert_U$ from a supporting directory service and validates the certificate path. The certificate contains the aircraft's public key agreement key ($Q_{s,U}$).

   Note. – If the air-ground router is unable to retrieve the aircraft's certificate, then the air-ground router will signal (step 4b) that the airborne router should send its public key certificate in the OPEN BISPDU if local policy permits it. If validation of the certificate path fails, then the connection will not be established.

3. The air-ground router generates a 32-bit random value, $Rand_V$.

4. The air-ground router sends an OPEN BISPDU with:

   a. Code 2 in the Authentication Code (AC) field,
   b. the following data in the Authentication Data (AD) field:
   1) a Certificate Required Indicator set to indicate public-key certificate required if access to a certificate delivery service is not available and permitted by local policy. Otherwise, it is set to indicate public-key certificate not required.
   2) A random number $Rand_V$ to protect against interception and manipulation attacks.
   3) If public-key certificate required was signaled by the airborne router in the ISH exchange, the air-ground router's public key certificate path, $Cert_V$, is placed in the Authentication Data field; otherwise, the air-ground router's public key ($Q_{s,V}$) is sent. If the air-ground router's policy is for mutual authentication, the air-ground router's public key certificate path, $Cert_V$, is placed in the Authentication Data field (independent of whether or not requested by the airborne router).
   c. a Type-1 authenticator in the Validation Pattern (VP) field.

5. Upon receipt of the OPEN BISPDU, the airborne router checks to see if the air-ground router's public-key certificate path, $Cert_V$ is in the authentication data field. If present, the certificate path is validated. The certificate contains the air-ground router's public key agreement key ($Q_{s,V}$).

6. The airborne router generates a 32-bit random value, $Rand_U$.

7. The airborne router computes the Diffie-Hellman shared secret value, $Z_{U,V}$, using the ATN Secret Value Derivation Primitive (ASVDP) with its pre-stored private key, $d_{s,U}$, and the received public key, $Q_{s,V}$.

8. The airborne router derives an 160-bit session key, $MacKey_{U,V}$, using the ATN Key Derivation Function (AKDF) with a concatenation of random values, i.e.,

the connection initiator's value concatenated with the peer-BIS's value ($Rand_V||Rand_U$), as shared data.

9. The airborne router sends an OPEN BISPDU with:

   a. Code 2 in the Authentication Code (AC) field,
   b. the following data in the Authentication Data (AD) field:
      1) a Certificate Required Indicator set to indicate public-key certificate not required.
      2) a random number $Rand_U$ to protect against interception and replay attacks.
      3) If public-key certificate required was signaled by the air-ground router in the ISH exchange, the airborne router's public key certificate path, $Cert_U$, is placed in the Authentication Data field
   c. a Type-1 authenticator in the Validation Pattern (VP) field.

10. Upon receipt of the OPEN BISPDU, the air-ground router computes the Diffie-Hellman shared secret value, $Z_{U,V}$, using the ATN Secret Value Derivation Primitive (ASVDP) with its pre-stored private key, $d_{s,V}$, and the received public key, $Q_{s,U}$.

11. The air-ground router derives an 160-bit session key, $MacKey_{U,V}$, using the ATN Key Derivation Function (AKDF) with a concatenation of random values, i.e., the connection initiator's value concatenated with the peer-BIS's value ($Rand_V||Rand_U$), as shared data.

    Note. – If the airborne router has already sent an OPEN BISPDU without including its public key certificate and receives an OPEN BISPDU with public-key certificate required, it will re-send the OPEN BISPDU with its public-key certificate.

12. The air-ground and airborne (step 15) routers tag subsequent BISPDUs with a HMAC seal over the BISPDU using the ATN Keyed Message Authentication Code Generation Primitive (AMACP).

13. The air-ground and airborne (step 16) routers send subsequent BISPDUs with the computed tag, *MacTag*, in the Validation Pattern (VP) field.

14. Upon receipt of a tagged BISPDU, the air-ground and airborne (step 17) routers check the purported tag using the ATN Keyed Message Authentication Code Verification Primitive (AMACVP).

Note. - If verification fails, the BISPDU will be dropped with no further action.

3.5.2 Ground-Ground IDRP Connections

Ground-Ground IDRP connection exchanges are depicted in figure 2 and described in the following scenario description.

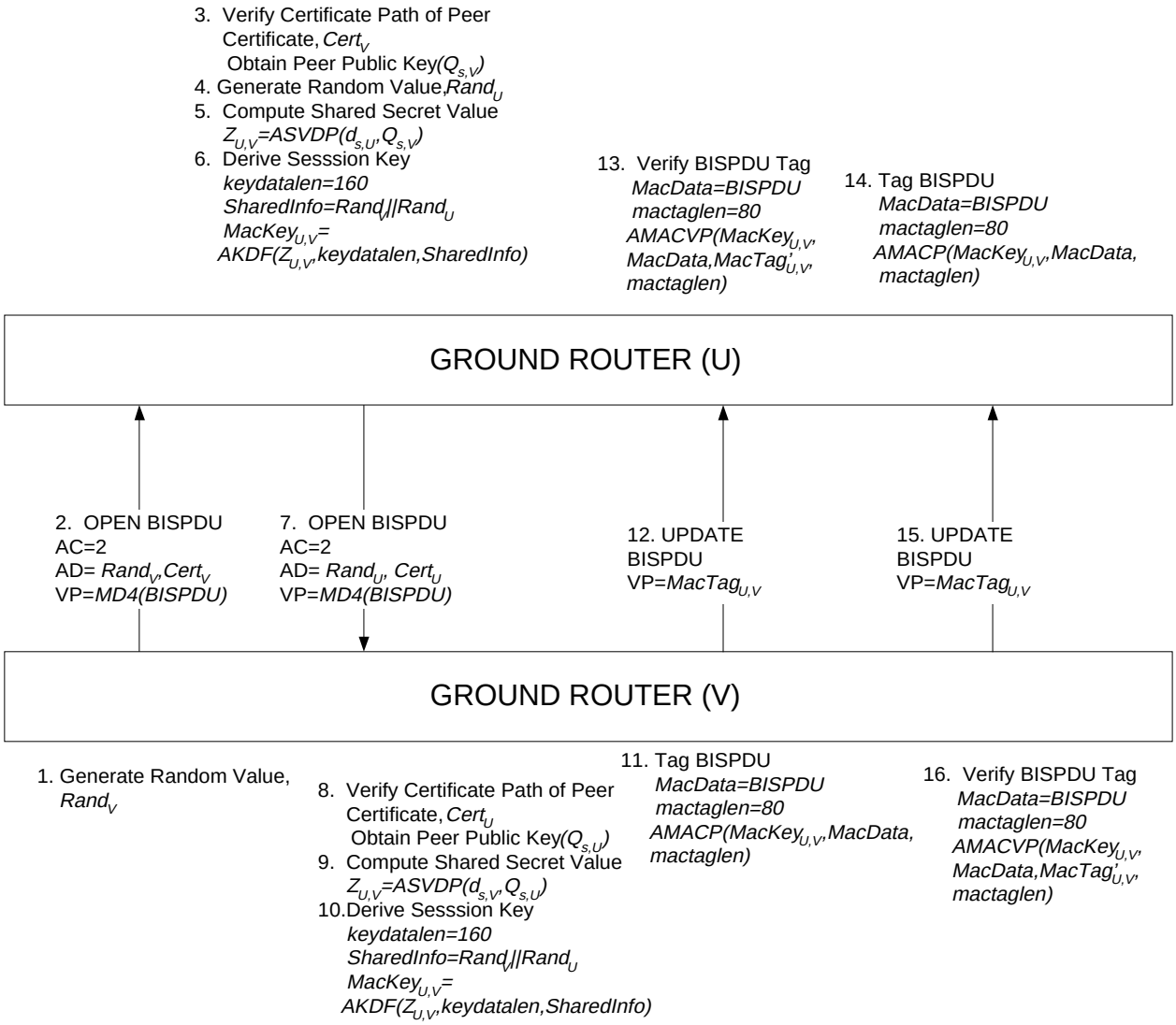

Figure 2 – Ground-Ground Router IDRP Authentication Exchanges

1. The initiating ground router generates a 32-bit random value, $Rand_V$.

2. The initiating ground router sends an OPEN BISPDU with:

   a. Code 2 in the Authentication Code (AC) field,
   b. the following data in the Authentication Data (AD) field:
      1) a random number $Rand_V$ to protect against interception and replay attacks.
      2) Its public-key certificate path, $Cert_V$
   c. a Type-1 authenticator in the Validation Pattern (VP) field.

3. Upon receipt of the OPEN BISPDU, the peer (non-initiating) ground router validates the certificate path of the received certificate, $Cert_V$. The certificate contains the initiating router's public key agreement key ($Q_{s,V}$).

   Note. – If either router is configured for type-2 authentication but does not receive a public-key certificate from its peer, the OPEN BISPDU will be discarded with no further action.

4. The peer router generates a 32-bit random value, $Rand_U$.

5. The peer router computes the Diffie-Hellman shared secret value, $Z_{U,V}$, using the ATN Secret Value Derivation Primitive (ASVDP) with its pre-stored private key, $d_{s,U}$, and the received public key, $Q_{s,V}$.

6. The peer router derives an 160-bit session key, $MacKey_{U,V}$, using the ATN Key Derivation Function (AKDF) with a concatenation of the random values, i.e., the connection initiator's value concatenated with the peer-BIS's value ($Rand_V||Rand_U$), as shared data.

7. The peer router sends an OPEN BISPDU with:

   a. Code 2 in the Authentication Code (AC) field,
   b. the following data in the Authentication Data (AD) field:
      1) a random number $Rand_U$ to protect against interception and replay attacks.
      2) It public key certificate path, $Cert_U$
   c. a Type-1 authenticator in the Validation Pattern (VP) field.

8. Upon receipt of the OPEN BISPDU, the initiating router validates the certificate path of the received public-key certificate, $Cert_U$. The certificate contains the peer router's public key agreement key ($Q_{s,U}$).

9. The initiating router computes the Diffie-Hellman shared secret value, $Z_{U,V}$, using the ATN Secret Value Derivation Primitive (ASVDP) with its pre-stored private key, $d_{s,V}$, and the received public key, $Q_{s,U}$.

10. The initiating router derives an 160-bit session key, $MacKey_{U,V}$, using the ATN Key Derivation Function (AKDF) with a concatenation of the random values, i.e., the connection initiator's value concatenated with the peer-BIS's value ($Rand_V||Rand_U$), as shared data.

11. The initiating and peer (step 14) routers tag subsequent BISPDUs with a HMAC seal over the BISPDU using the ATN Keyed Message Authentication Code Generation Primitive (AMACP).

12. The initiating and peer (step 15) routers send subsequent BISPDUs with the computed tag, *MacTag*, in the Validation Pattern (VP) field.

13. Upon receipt of a tagged BISPDU, the initiating and peer (step 16) routers check the purported tag using the ATN Keyed Message Authentication Code Verification Primitive (AMACVP).

Note. - If verification fails, the BISPDU will be dropped with no further action.

2. Recommendations

1. It is recommended that WG2 review the above material for inclusion in the CAMAL.