ATNP WG2/WP 450
8 June 1998

ATNP WG2
Utrecht, Netherlands
29 June – 1 July 1998

IDRP Security

Prepared by Ron Jones

Summary
This working paper presents a review of ISO/IEC 10747 and Sub-Volume 5 as regards the capability of IDRP to support the proposed ATN security enhancements and the related impact on the ATN technical provisions. It also briefly discusses the capability of ISO/IEC 10589 to support the ATN security provisions.

Attachment 1: Excerpt from "Proposed Work Plan and Solution for IDRP Authentication," Flimsy 4 from 14th meeting of WG2

1. INTRODUCTION

The proposed security enhancements for the ATN SARPs includes authentication of IDRP exchanges from airborne BISs to air-ground BISs and between air-ground and ground BISs. This topic was discussed at the 14th meeting of WG2 in Rio de Janeiro and Flimsy 4 (attachment 1 to this working paper) was prepared at that meeting. This paper presents a review of ISO/IEC 10747 and Sub-Volume 5 as regards the capability of IDRP to support the proposed ATN security enhancements and the related impact on the ATN technical provisions.

2. DISCUSSION

2.1 A review of ISO/IEC 10747 (1993) to determine the IDRP provisions to support authentication of routing information exchanges has revealed the following:

a) Para. 6.1 of ISO 10747 defines the header of the BISPDU to include a 16 octet *Validation Pattern* field. The BISPDU header has a fixed size of 30 octets and is used as the initial 30 octets of each IDRP PDU (e.g., OPEN PDU, UPDATE PDU, etc.).

b) The OPEN PDU, defined in para. 6.2 of 10747, has a 1 octet field for *Authentication Code* followed by a variable length field for *Authentication Data*. Three values, sometimes referred to as authentication type 1 2 or 3, are allowed for Authentication Code where a value of 2, as defined below, appears appropriate to support the desired ATN security services.

> *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.*

The *Authentication Data* field of the OPEN PDU is defined as:

> *The form and meaning of the this field is a variable-length field that depends on the Authentication Code, as described in D.1. The length of the authentication data field can be determined from the Length field of the BIS PDU header.*

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.*

Note 2 in Annex D.1 of ISO 10747 indicates that

> *"……This international standard does not mandate the use of a specific encryption algorithm. Explicit indication of the specific algorithm to be used is outside the scope of IDRP. 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."*

2.2 The implications of the above cited ISO 10747 provisions are that in order to support the proposed ATN security provisions for authentication of routing exchanges the OPEN PDU should specify an *Authentication Code* value of 2 and the value indicated in the *Authentication Data* field should be as defined in the ATN SARPs to identify the specific encryption algorithm, or version number. This would require that all PDUs exchanged over this connection would include an encrypted checksum (i.e., digital signature) in the *Authentication Pattern* field of the fixed length header of every IDRP PDU. This creates a number of transition issues for the ATN to deal with. Since ISO 10747 does not define a mechanism to allow peer IDRP implementations to negotiate a compatible level of authentication, ATN specific features will be needed to accommodate a mix of ATN Package-1 users with authentication type 1 (simply ensures integrity by putting a checksum in the

Authentication Patter field) and Package-2 users with authentication type 2. Also the ATN requirement is for only authentication of air-to-ground IDRP exchanges while ISO 10747 would require the same type of authentication for all PDUs, both uplink and downlink, over a given IDRP connection.

2.3 The impact on Sub-Volume 5 of the ATN SARPs would be:

a) Sub-Volume 5, para. 5.8.3.4.3 (IDRP General APRL) indicates that Authentication Type 1 is required (integrity only) while support for authentication types 2 and 3 are optional. The IDRP APRL (items INTG1 and INTG2) would need to be updated to require support for Type 2 authentication while perhaps still allowing Type 3 as an option. However, we will need to still permit support for Type 1 for CNS/ATM-1 Package implementations. It is an issue of how to best reflect this in the APRL. Also consideration should be given to restricting the option for authentication type 3 (authentication plus password) for use only between peer ground BISs where the use of authentication/passwords has been coordinated through bilateral agreements or are under the control of a single administration.

b) The note under 5.8.3.4.8 would need to be revised because it now reads: "Only support for an Authentication Code 1 is required." This would need to be revised to indicate that for BISs supporting the ATN security services Authentication Code 2 will be required in addition to support for Authentication Code 1, in order to accommodate peer BISs either supporting the ATN security services or not.

c) Although the proposed ATN security architecture does not require authentication of IDRP exchanges from an air-ground BIS to an airborne BIS, with IDRP authentication type 2 both the airborne and the air-ground BIS's digital signature, in the form of an encrypted checksum, would normally be included in the *Authentication Pattern* field of every IDRP PDU. It would be an ATN specific feature for the airborne-ground BIS to <u>not</u> encrypt the checksum in the IDRP PDUs it sends to an airborne BIS. Thus, the air-ground BIS, when interacting with airborne BISs, would always generate the *Authentication Pattern* as if the airborne BIS only supported authentication type 1 regardless of whether the IDRP connection was opened with Type 1 or Type 2 authentication. This could be reflected in Sub-Volume 5 by adding a new subparagaph under 5.8.3.2 (i.e., ATN Specific Features).

d) The encryption algorithm for generating the digital signature would need to be specified in the ATN SARPs. If this is the same algorithm as will be specified for generating the digital signature conveyed by ACSE, then it should only be specified in a single place within the SARPs (i.e., perhaps simply referenced in SV-5). Note the IDRP definition of a fixed length field of 16 octets could constrain the choice.

e) Sub-Volume 5 defines, under paragraph 5.8.3.2.2, the use of the ATN specific definition for the IDRP security path attribute. Multiple Security Tag Sets may be

included in the IDRP Security Path Attribute. The current Sub-Volume 5 (CNS/ATM-1 Package) defines tag sets for identifying the air/ground subnetwork type and the traffic types supported over a given path. An additional tag set could be defined, if desired, in support of the ATN security enhancements to indicate the path had been authenticated. This would only be needed if the routing decision could be influenced by whether IDRP had authenticated the peer BIS (e.g., the routing policy would give preference to forwarding via an authenticated path vs. one not authenticated). The need for this capability will require further investigation and coordination with WG1.

f) Sub-Volume 5 would need to define the use of ATN specific features to allow establishment of an IDRP connection when one BIS only supports Type 1 authentication and the peer BIS supports Type 2 authentication. Flimsy 4 from the 14th meeting of WG2 (attachment 1 to this working paper) attempted to address this issue. However, the approach proposed by this flimsy will need refinement and other alternatives should also be considered. The proposed solution in Flimsy 4 is incomplete as it does not address the case where the air-ground router only supports authentication type 1 (i.e., a Package-1 router) and would thus reject any OPEN PDU specifying type 2. The solution proposed in Flimsy 4 also indicates that "the air-ground router will not digitally sign IDRP exchanges to the airborne router." The proposal also states for airborne routers "the router will ignore any value in the authentication field received from an air-ground router." Given the first statement it would not be necessary for the airborne router to "ignore any value in the authentication field" since this field would only contain an unencrypted checksum.

2.4 A initial investigation of IS-IS standard (ISO/IEC 10589) indicates that it supports authentication services in a manner similar to ISO/IEC 10747. Support for authentication of ES-IS (ISO/IEC 9542) exchanges will require further investigation. It would be appropriate to develop guidance material for incorporation into a future version of the CAMAL to discuss the applicability of authentication with ISO/IEC 10589 and ISO/IEC 9542.

3. PROPOSAL

It is proposed that WG2 accept to develop the revisions to Sub-Volume 5 and the CAMAL based on the information provided in 2.3 above and:

a) coordinate with WG3 (SG3) on the feasibility of defining of a single encryption algorithm for the generation of digital signatures for use by ESs and by BISs;

b) coordinate with WG1 to determine if there is a system-level requirement to influence a routing decision based on whether IDRP had authenticated the peer BIS or not;

c) investigate alternative solutions for ensuring backward compatibility with CNS/ATM-1 Package implementations. Viable solutions will need to enable any

combination of Package-1/Package-2 airborne BISs and air-ground BISs to interoperate and provide for authentication services when supported by both peer BISs;

d) draft proposed changes to SV-5 consistent with the WG2 approved solution. Such a solution is expected to require the definition of ATN specific features within Sub-Volume 5; and

e) prepare ICS guidance material for the CAMAL addressing the IDRP related security provisions as well as guidance on the use of authentication with ISO/IEC 10589 and/or ISO/IEC 9542 implementations.

ATTACHMENT 1

WG2/FLIMSY 4
March 17, 1998

WG 2 Flimsy
Proposed Work Plan and Solution for IDRP Authentication

1. For the purpose of IDRP authentication, only the use of digital signatures.

2. Both IDRP connection requests and IDRP routing updates will use digital signatures.

3. For airborne routers, only the down-link IDRP exchanges will be authenticated.

4. Proposed Solution
   - For airborne routers:
     - the aircraft will have a pre-loaded private key.
     - the certificate will be (at a minimum) aircraft-based.
     - the router will calculate a digital signature using its private key and place it in -the IDRP header.
     - the router will ignore any value in the authentication field received from an air-ground router.
   - For air-ground routers:
     - the air-ground router will authenticate the digital signature on each airborne router exchange based on the retrieved public key.
     - the air-ground router may obtain the public key through any means available to it including the use of an X.500 look-up or through local caching.
     - the air-ground router will not digitally sign IDRP exchanges to the airborne router.
   - For ground-ground BIS routers:
     - all BIS routers will use authentication.
     - each BIS will use its private key (pre-loaded) to generate a digital signature for all IDRP exchanges.
     - each BIS will authenticate the IDRP exchanges by obtaining the public key of the associated BIS and confirming the digital signature. A BIS can obtain the public keys through several different methods such as X.500 look-up, local cache, or other local means. The method used is a local matter.

5. Guidance Material is needed on obtaining keys, the use of authentication for routers in a single administrative domain, and use of authentication.

6. Proposed detailed SARPs text is expected before the Utrecht WG 2 meeting.

7. An investigation as to whether there is a place in the IDRP UPDATE pdu for authentication information is required to ensure that a standard way of protecting these pdus can be used.