**ATNP WG2/WP447**
**March 16, 1998**

**Aeronautical Telecommunication Network Panel (ATNP)**
**Working Group 2**
**Rio de Janeiro, Brazil**
**16-19 March 1998**

# Alternatives for BIS Access to X.509 Certificates

**Presented by R. Jones**

WG1 of ATNP has been developing the system level requirements (Core and SV-1) for security based on X.509. Ground BISs and Air-Ground BISs will need to access the X.509 certificates of peer ground, air-ground and airborne BISs. This working paper describes alternatives for providing this access.

## References:

1. "ATN Security Provisions, SV-1 Version 2.0, draft text," WG1/WP11-14a
2. ITU-T Recommendation X.509|ISO/IEC 9594-8, "Directory Authentication Framework"

## 1. Introduction:

WG1 of ATNP has been developing the system level requirements (Core and SV-1) for security based on X.509. Ground BISs and Air-Ground BISs will need to access the X.509 certificate of peer ground, air-ground and airborne BISs. This working paper describes alternatives for providing this access.

## 2. Discussion

The current draft SV-1 security provisions [ref. 1] identifies a requirement for:

> ATN intermediate systems (ISs) supporting secured ATN services shall support the use of the ATN security provisions for authentication, using digital signatures, of routing information exchanges between air-ground and ground BISs and from airborne BISs to air-ground BISs, but not vise versa, as defined in 5.x.x.
>
> *Note 1. — The approach selected for the distribution of security certificates to ATN air-ground and ground intermediate systems is a local implementation matter. Alternatives for the distribution of certificates for air-ground and ground BISs include use of X.500 user agents within the intermediate systems, local site management of the certificate information and the use of a centralized systems manager for distribution of certificate information to the intermediate systems. In the case where an air-ground BIS must obtain the certificate for an airborne BIS, the use of the ground context management application for the distribution of certificates for airborne users to the local air-ground BISs is an alternative to having X.500 user agents within each air-ground BIS.*
>
> *Note 2. — No requirements are defined herein for securing exchanges of routing information from air-ground BISs to airborne BISs.*

Note 2 from the quoted draft SV-1 text above describes several alternatives for air-ground and ground BISs to obtain the X.509 certificate that will be needed to authenticate routing exchanges with peer BISs. The alternatives are more fully summarized in the following table form.

# Alternative Sources for X.509 Certificates

| BIS type | Peer BIS type | Alternative # | Source of X.509 certificate | BIS user agent/access protocol |
|---|---|---|---|---|
| A-G BIS | Ground BIS | 1 | X.500 server | X.500/full ISO stack |
| | | 2 | X.500 server | X.500/efficient ISO stack |
| | | 3 | Systems Manager | Systems Management/ CMIP or SNMP |
| | | 4 | peer ground BIS | Certificate passed by IDRP when initiating BIS-BIS connection |
| | | | | |
| | Airborne BIS | 1 | X.500 server | X.500/full ISO stack |
| | | 2 | X.500 server | X.500/efficient ISO stack |
| | | 3 | peer airborne BIS | Certificate passed by IDRP when initiating BIS-BIS connection |
| | | 4 | Context Management server | ATN specific CM access protocol (CM server would include an X.500 user agent for retrieving the X.509 certificate from an X.500 server) |
| | | | | |
| Ground BIS | Ground BIS | 1 | X.500 server | X.500/full ISO stack |
| | | 2 | X.500 server | X.500/efficient ISO stack |
| | | 3 | Systems Manager | Systems Management/ CMIP or SNMP |
| | | 4 | peer ground BIS | Certificate passed by IDRP when initiating BIS-BIS connection |
| | | | | |
| | A-G BIS | 1 | X.500 server | X.500/full ISO stack |
| | | 2 | X.500 server | X.500/efficient ISO stack |
| | | 3 | Systems Manager | Systems Management/ CMIP or SNMP |
| | | 4 | peer ground BIS | Certificate passed by IDRP when initiating BIS-BIS connection |

## 3. Recommendation:

a) WG2 is invited to consider the most appropriate alternative(s) for air-ground BISs and ground BISs to obtain X.509 certificates and to develop SARPs and Guidance Material accordingly. Standards will be required to define how an air-ground BIS will obtain the X.509 certificate for an airborne BIS. Also Standards will be required for how a backbone ground BIS will obtain the X.509 certificate for a peer backbone ground BIS operated by a different administration. The appropriate technique(s) for obtaining the X.509 certificate from a peer air-ground or ground BIS within the same administrative domain is a local matter for with a recommended approach and/or guidance material will be needed.

b) WG2 is invited to coordinate with WG3 to determine the most suitable method for providing access to X.500 servers (i.e., full ISO stack, efficient ISO stack or support for both).

c) WG2 is invited to coordinate with WG1 to more fully define the ATN security architecture for the distribution of X.509 certificates.