AERONAUTICAL COMMUNICATIONS PANEL (ACP)

17th MEETING OF WORKING GROUP M (Maintenance)

Bangkok, Thailand 31 January – 1 February 2011

Agenda Item 3a: ATN/OSI Document 9880 Update Status – Security Updates

ATN Certificate and CRL Analysis Report – Summary

(Presented by Michael Olive, Honeywell International Inc., United States)

SUMMARY

This working paper provides a summary overview of the analysis, results, and recommendations presented in the ATN/OSI Doc. 9880 Security Validation Report. The detailed validation report is included as an appendix to ACP-WGM17-WPXX.

ACTION

The working group is invited to review the analysis results and consider recommended improvements to certificate and CRL provisions in Part IV-B.
Background

• WGM-WP1608, *ICAO Doc. 9880 Part IV-B Security Validation Report*, included the following recommendation:

<table>
<thead>
<tr>
<th>Recommendation 1: Certificate and CRL Profile Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Improvement Opportunity</strong></td>
</tr>
<tr>
<td>• Detailed certificate and CRL profiles transferred from Doc. 9705 SV-VIII were developed in the late 1990’s and do not necessarily reflect current industry standards (commercial or aero)</td>
</tr>
<tr>
<td><strong>Recommendation</strong></td>
</tr>
<tr>
<td>• Replace Sections 4.1-4.4 with wording consistent with ICAO Doc. 9896:</td>
</tr>
<tr>
<td>• X.509 certificate/CRL profiles per IETF RFC 5280</td>
</tr>
<tr>
<td>• Certificate policy and practices framework per IETF RFC 3647</td>
</tr>
<tr>
<td>• Note indicating that ATA Spec 42 is available for use by the aero community</td>
</tr>
<tr>
<td><strong>Potential Pros</strong></td>
</tr>
<tr>
<td>• Harmonization with ATA Spec 42 and industry standard practice</td>
</tr>
<tr>
<td>• Harmonization between text in Doc. 9880 Part IV-B and Doc. 9896</td>
</tr>
<tr>
<td>• Significant simplification of text in Doc. 9880 Part IV-B</td>
</tr>
<tr>
<td><strong>Potential Cons</strong></td>
</tr>
<tr>
<td>• None identified.</td>
</tr>
</tbody>
</table>

• WGM-WP1608 also suggested a follow-up action to perform a detailed analysis of existing ATN/OSI Certificate/CRL provisions with respect to the PKI industry standards.
### Analysis Report Table of Contents

#### 1. Introduction
- 1.1. **Purpose**
- 1.2. **Scope**
- 1.3. **Document Overview**
- 1.4. **Terminology**
- 1.5. **Reference Documents**

#### 2. Analysis Approach
- 2.1. **Background**
- 2.2. **Approach**

#### 3. Analysis Results
- Analysis format and example
- 3.1. **ATN PKI Certificate Format**
- 3.2. **ATN PKI CRL Format**

#### 4. Conclusions
- 4.1. **Summary Results**
- 4.2. **Recommendations**

Analysis report topics highlighted in **RED** are summarized in this working paper presentation.
1. Introduction

1.1 Purpose

- The purpose of the report is to present the results of a detailed comparative analysis between the ATN certificate and CRL provisions contained in Part IV-B and the following industry standards specified in ICAO Doc. 9896:
  - Internet Engineering Task Force (IETF) RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, and
- The report recommends specific improvements to Part IV-B to align Certificate/CRL provisions with industry standards.
- Honeywell was tasked by the FAA to perform this validation as part of the FAA Data Communications (DataComm) Avionics contract.
2. Validation Approach  [1/2]

- Provision-by-provision analysis of every ATN/OSI certificate and CRL requirement and note in Part IV-B with respect to:
  - RFC 5280
  - ATA Spec 42

- If the ATN provision is aligned precisely with the industry standards, then:
  - References to the industry standards are sufficient, and
  - The ATN provision may be removed from Part IV-B without any undesirable consequences.

- For cases where alignment is not exact or there are differences:
  - Recommendations for supplementing the industry standard references and accommodating the differences are proposed.
2. Validation Approach [2/2]

• Starting Point
  – ICAO Doc. 9880 Security Validation Report (WGM-WP1608) recommendation
    • Replace detailed ATN certificate/CRL profiles with references to industry
      standards, consistent with the approach taken in ICAO Doc. 9896

• Using Doc. 9896 as a guide, the following represent an Initial
  set of ATN/OSI PKI Provisions
  – The ATN/OSI PKI shall use the Internet X.509 Public Key Infrastructure
    3647.
  – The ATN/OSI PKI shall use the Internet X.509 Public Key Infrastructure
    Certificate and Certificate Revocation List (CRL) Profile as specified in RFC
    5280.
  – Note— The Air Transport Association (ATA) Digital Security Working Group
    (DSWG) has developed a Certificate Policy (ATA Specification 42) for use in
    the aviation community. ATA Specification 42 includes certificate and CRL
    profiles that are suitable for aeronautical applications and interoperability with
    an aerospace industry PKI bridge. These profiles provide greater specificity
    than, but do not conflict with, RFC 5280.
3. Analysis Results [1/2]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ICAO Doc. 9880, Part IV-B</td>
<td>ATA Spec 42 [42]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Column 1* | *Column 2* | *Column 3* | *Column 4*

**Paragraph number and text for each specific ATN certificate/CRL provision analyzed.**

**Paragraph number associated with the provision in RFC 5280 and/or ATA Spec 42 that corresponds to the ATN security provision in Column 1. Where appropriate, text applicable to the analysis is quoted from the industry standard.**

**Assessment of provision alignment in terms of:**

- **Y** – Provisions aligned and equivalent technically.
- **Y** – Provisions aligned with exceptions noted in Column 4.
- **N** – Provisions not aligned.

**Where differences exist, rationale for accepting the differences and/or recommendations for accommodating the differences.**
### 3. Analysis Results [2/2]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.3.1.3.1</strong> The version field shall indicate a version 3 certificate, i.e., contain the value 2.</td>
<td><strong>[5280]</strong> Section 4.1.2.1: When extensions are used, as expected in this profile, version MUST be 3 (value is 2).</td>
<td>Y</td>
<td>If references to RFC 5280 and ATA Spec 42 are included in Part IV-B, the ATN provision may be removed with no undesirable consequences.</td>
</tr>
<tr>
<td><strong>4.3.1.3.2</strong> The serialNumber field shall indicate the certificate serial number, which may be any integer value.</td>
<td><strong>[5280]</strong> Section 4.1.2.2: The serial number MUST be a positive integer assigned by the CA to each certificate.</td>
<td>Y</td>
<td>If references to RFC 5280 and ATA Spec 42 are included in Part IV-B, the ATN provision may be removed with no undesirable consequences.</td>
</tr>
<tr>
<td><strong>4.3.1.3.2.1</strong> The use of short serial numbers is encouraged to reduce the size of ATN certificates.</td>
<td><strong>[5280]</strong> Section 4.1.2.2: Certificate users MUST be able to handle serialNumber values up to 20 octets.</td>
<td><em>Y</em></td>
<td>If reference to RFC 5280 is included in Part IV-B, the ATN comment should be removed to ensure compliance with the industry standard. <strong>Recommendation:</strong> In addition, include the following comment in Part IV-B as a caution to implementers: RFC 5280 specifies that users must be able to handle certificate serial number values up to 20 octets; however, CAs should be encouraged to use short serial numbers (if possible without impacting conformance) to reduce the size of ATN certificates.</td>
</tr>
<tr>
<td><strong>4.3.1.3.3</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Example*
4. Conclusions  [1/6]

4.1. Summary Results

<table>
<thead>
<tr>
<th>Certificate Provision Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject Field</strong></td>
</tr>
<tr>
<td>• Part IV-B specifies that the certificate <strong>subject</strong> field be empty if the subject is not a CA or AMHS entity, which was necessary to support compressed certificates. Although RFC 5280 permits an empty subject if the Subject Alternative Name extension is included, it is important to note that ATA Spec 42 requires that all certificates include a unique, meaningful name in the <strong>subject</strong> field.</td>
</tr>
<tr>
<td><strong>Parameters Field</strong></td>
</tr>
<tr>
<td>• Part IV-B redefines standard syntax for <strong>ECPParameters</strong> as ATN-specific <strong>EcpkParameters</strong> to support compressed certificates. This is no longer necessary since provisions ATN-specific compression have been removed.</td>
</tr>
<tr>
<td><strong>Certificate Extensions</strong></td>
</tr>
<tr>
<td>• RFC 5280 permits, and ATA Spec 42 includes, additional certificate extensions beyond those required in Part IV-B.</td>
</tr>
<tr>
<td><strong>Certificate Extension Order</strong></td>
</tr>
<tr>
<td>• Part-IV specifies that the key usage extension be marked non-critical; however per RFC 5280 industry standard practice is to mark the extension critical.</td>
</tr>
<tr>
<td><strong>SubjectAltName Extension</strong></td>
</tr>
<tr>
<td>• Part IV-B provisions for this extension are consistent with RFC 5280; however, the Part IV-B naming provisions need to be retained since the industry standards do not include specification of ATN-specific names.</td>
</tr>
<tr>
<td>• Extension must be marked critical if the <strong>subject</strong> field contains an empty sequence.</td>
</tr>
<tr>
<td><strong>IssuerAltName Extension</strong></td>
</tr>
<tr>
<td>• Part IV-B specifies this extension to support compressed certificates. This is no longer necessary since provisions ATN-specific compression have been removed.</td>
</tr>
</tbody>
</table>

### 4.1. Summary Results (continued)

#### CRL Provision Differences

<table>
<thead>
<tr>
<th>CRL Entry Extensions</th>
<th>Part IV-B provisions specify that CRL Entry Extensions be absent from ATN CRLs. However, RFC 5280 recommends that CRL Entry Extensions should be included when reason code information is available.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IssuerAltName CRL Extension</td>
<td>Part IV-B specifies this extension to support compressed certificates. This is no longer necessary since provisions ATN-specific compression have been removed.</td>
</tr>
</tbody>
</table>

#### Editorial Defects

| 4.3.1.2.1.1 | Typographical error: missing a “4” in the OID value, which should be “{1 2 840 10045 4 3 2}” |
| 4.3.1.3.3 | Typographical error: cross reference “8.4.3.1.2.1” should be “4.3.1.2.1” |
| 4.4.1.3 | Typographical error: cross reference “8.4.3.1” should be “4.3.1” |
| 4.4.2.3 | Typographical error: cross reference “8.4.3.2” should be “4.3.2” |

4.2. Recommended Part IV-B Certificate/CRL Provisions
-- Initial Set of ATN/OSI Provisions (grey) plus notes


Note— The Certificate Policy and Certificate Practice Statements of a given State could be used by other States in establishing their trust relationships and operating policies such as cross certification.

The ATN/OSI PKI shall use the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile as specified in RFC 5280.

Note— The Air Transport Association (ATA) Digital Security Working Group (DSWG) has developed a Certificate Policy (ATA Specification 42) for use in the aviation community. ATA Specification 42 includes certificate and CRL profiles that are suitable for aeronautical applications and interoperability with an aerospace industry PKI bridge. These profiles provide greater specificity than, but do not conflict with, RFC 5280.

Note— RFC 5280 specifies that users must be able to handle certificate serial number values up to 20 octets; however, CAs should be encouraged to use short serial numbers (if possible without impacting conformance) to reduce the size of ATN certificates.

4.2. Recommended Part IV-B Certificate/CRL Provisions (continued)
-- Provision for elliptic curve information

The ATN/OSI PKI shall use the following Elliptic Curve Public Key Information as specified in RFC 5480:

- **ASN.1 Syntax**
  - ECDSA-Sig-Value
  - ECParameters
  - ECPoint

- **Object Identifiers**
  - ecdsa-with-SHA256 {1 2 840 10045 4 3 2}
  - id-ecPublicKey {1 2 840 10045 2 1}
  - sect233r1 {1 3 132 0 27}

4.2. Recommended Part IV-B Certificate/CRL Provisions (continued) -- Provision for ATN-specific Naming

The subject field of ATN/OSI certificates shall contain the unique distinguished name (DN) of the subject in accordance with the directory schema specified in Part IV-A.

Note—Commercial and aerospace CAs may impose constraints on the distinguished name form to ensure that verifiable information is used to uniquely identify the device in the global context of the CA’s PKI.

If the subject is an ATN ATS end system other than an AMHS end system, the subject alternative name extension shall contain the entity's AP-title encoded as a registeredID.

If the subject is an AMHS entity, the subject alternative name extension shall contain either:

- The AMHS entity's distinguished name encoded as the value directoryName OR
- The AMHS entity’s X.400 address encoded as the value x400Address.

If the subject is an intermediate system, the subject alternative name extension shall contain the entity's Network Entity Title (NET) encoded as ipAddress with length up to 20 octets.

4.2. Recommended Part IV-B Certificate/CRL Provisions (continued)

-- Provisions for Key Usage and Cert Path Validation

ATN/OSI user certificates shall assert the `digitalSignature` and/or `keyAgreement` bits in the key usage extension.

Note— Key usage will have an abstract value of `digitalSignature` or `keyAgreement`, OR both `digitalSignature` and `keyAgreement` if use of a single certificate is permitted by the applicable Certificate Policy.

When validating a certificate path, ATN entities shall check that the certificate path contains at most one certificate issued by a State CA to another State CA.

Note— Trust among States is not transitive - a certificate issued to State B's CA from State A's CA together with a certificate to State C's CA from State B's CA does not indicate that State A trusts State C.
Action by the Meeting

• The ACP WG-M is invited to:
  – Review the detailed ATN Certificate and CRL Analysis results, and
  – Consider recommended improvements to certificate and CRL provisions in Part IV-B.

Note: The ATN Certificate and CRL Analysis Report contains the complete analysis results and recommended improvements. The report is included as Appendix A to working paper ACP WGM17/WP-XX.
Honeywell Aerospace Advanced Technology

Michael Olive
Fellow, Advanced Technology
E-mail: mike.olive@honeywell.com
Tel: +1 (410) 964-7342

Questions?