Multi Domain PKI Test Suite
-- Result of JNSA Challenge PKI 2002 --

Ryu Inada <Ryu.Inada@fujixerox.co.jp>

As representative of

NPO Japan Network Security Association

Sponsored by IT Promotion Agency, Japan
JNSA Challenge PKI 2002

• As we reported on 11-Nov-2002/56th IETF, we, JNSA, make a Multi Domain PKI Test Suite.
• We finished work at 28-Feb-2003, and prepare to open it public and translation to English.
  – Estimated date of open to public: End of June 2003
  – Estimated date of translation to English: End of June 2003
Challenge PKI 2002-Project scope

Public key

Cryptographic

Standard

X.509

RFC3280

Implementation

JDK / JCE

CryptoAPI

Interoperability
test

Test Case Report

Interoperability Test Suit

PKI Interoperability framework

CryptoAPI JDK 1.4/JCE

sample Implementation
PKI interoperability test suite
Challenge PKI 2002 - Test Cases

- ENIST/DoD
  - X.509 Path Validation Test Suite, Version 1.07
  - Total 130 cases

- GPKI (Japanese Government’s PKI)
  - GPKI simulation environment
  - Total 81 cases

- JNSA Original
  - UTF8 encoding matter (name rollover certificate) which is described in RFC 3280.
  - Key update issues.
  - Some CRL extensions including IDP
  - Total 45 cases

- Can easily add test case.
Sample implementations

• In Java
  – Worked on JDK 1.4
    • Based on Path Discovery/Path Validation API which provided from reference implementation.
    • And additional Path Discovery/Path Validation logic which concerned multi domain PKI environment.

• In C++
  – Worked on Microsoft Crypto API.
    • Using Windows original Revocation Service Provider and additional Path Discovery/Path Validation logic which concerned multi domain PKI environment.
## Requirement of GPKI and implementations

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Constrain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path Construction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRL IDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIA / OCSP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Constraints</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Constraint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*1 CRL IDP (issuing distribution point)
Sample implementation for CryptoAPI
Sample implementation for JAVA

We extend original JDK’s path builder/path checker interface.
To achieve more Applicable Test Suite ...

- Provide Framework more applicable & reusable
- Easy to extract minimal test case
  - There are too many test cases … about 256 cases.
  - For easily modified to you purpose: PKIX, GPKI, and other frameworks
- **Ready for Multi-domain PKI**
- **Re-usable** for others
- **No depend on environment**
  - Run on your local environment
  - maybe linux or cygwin?

We need two Reference!!

- Define multi-domain PKI
- Define DB Schema to re-use
Related Links

- NPO JNSA
  - http://www.jnsa.org/english/e_index.html
- IPA Security Center
  - http://www.ipa.go.jp/security/index-e.html
- JNSA Challenge PKI 2002
  - http://www.jnsa.org/english/e_active2_10.html
- Implementation Problems on PKI (JNSA Challenge PKI 2001)
- The report of Challenge PKI in IETF Atlanta
Demonstration