JNSA Challenge PKI 2002
– Work in progress –

An approach of Multi-Domain PKI Test Suite

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

As representative of

NPO **J**apan **N**etwork **S**ecurity **A**ssociation

Sponsored by **I**T **P**romotion **A**gency, Japan

Apology

- At first, we make a an apology of delayed to public our interoperability report of last year experience JNSA Challenge PKI 2001 translated in English which we promised in PKIX meeting on 54th IETF at Yokohama.
- In current status, we will open it public at end of this year. We have some difficulties to select appreciate translate engineer by using Government fund X-<.

JNSA Challenge PKI 2002

- As we experienced in last year
  - the interoperability experiment is very difficult.

- Why ?
  - Lack of knowledge.
    - The concept of Multi-Domain PKI is complex and difficult.
      - Especially, Path Discovery/Path Validation.
  - Lack of Experience
    - There are no handy environment for testing.
    - Experience of JNSA Challenge PKI 2001
      - We needs 2 expert engineers in 2 months for concept make, create a brief design of test site.
      - We needs 3 expert engineers in 2 months to make test cases.
      - We needs lots of PCs, network, pizza, coffee and paper !

JNSA Challenge PKI 2002(cont.)

- What we need ?
  - For lack of knowledge
    - There is no royal way of gain a knowledge. :-)
  - For lack of experience
    - We make a decision of to make a handy Multi-Domain PKI testing environment.

Multi Domain PKI Test Suite

- Specially tuned up fake CA
- Specially tuned up fake VA
- Test Cases
- Sample Implementations of PKI application which are concerned Path Validating.
  - Java based(JDK 1.4)
  - Microsoft's CryptoAPI based

Fake CA

- Work on Linux plat home.
- Do not work as a ordinal CA, just generate various type of Certificates/CRLs specified by test cases.
- Base on AiCrypto/AiCA
  - Free implementation of Cryptographic modules/CA
  - Made by Nagoya Institute of Technology
    - http://mars.elcom.nitech.ac.jp/security/aicrypto.html
    - http://mars.elcom.nitech.ac.jp/security/aica.html
    - Sorry ! Japanese only (again X-<)

Fake VA

- Worked on Linux plat home.
- Do not work as ordinal VA, just responding response which is specified in test case.

- Looks like a OCSP version 1 Responder.
  - It fakes a response of OCSP response.
  - Just response fixed response which specified by test cases.
- And works like Japanese GPKI's VA
  - OCSP version 1
  - Private extensions which handle basic path discovery/path validation.

Test Cases

- NIST/DoD
- Japanese Government's GPKI
- JNSA Original
  - UTF8 encoding matter (name rollover certificate) which described in RFC 3280.
  - Key update issues.
  - Some CRL extensions including IDP
- 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.

Time lines

- End of Feb, 2003
  - Finish works
- End of April, 2003 ?
  - Open to public in free
- End of June, 2003 ?
  - Open to public English translated manuals, reports …

Thank you !