Multi Domain PKI Test Suite

-- Result of JNSA Challenge PKI 2002 --

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

As representative of

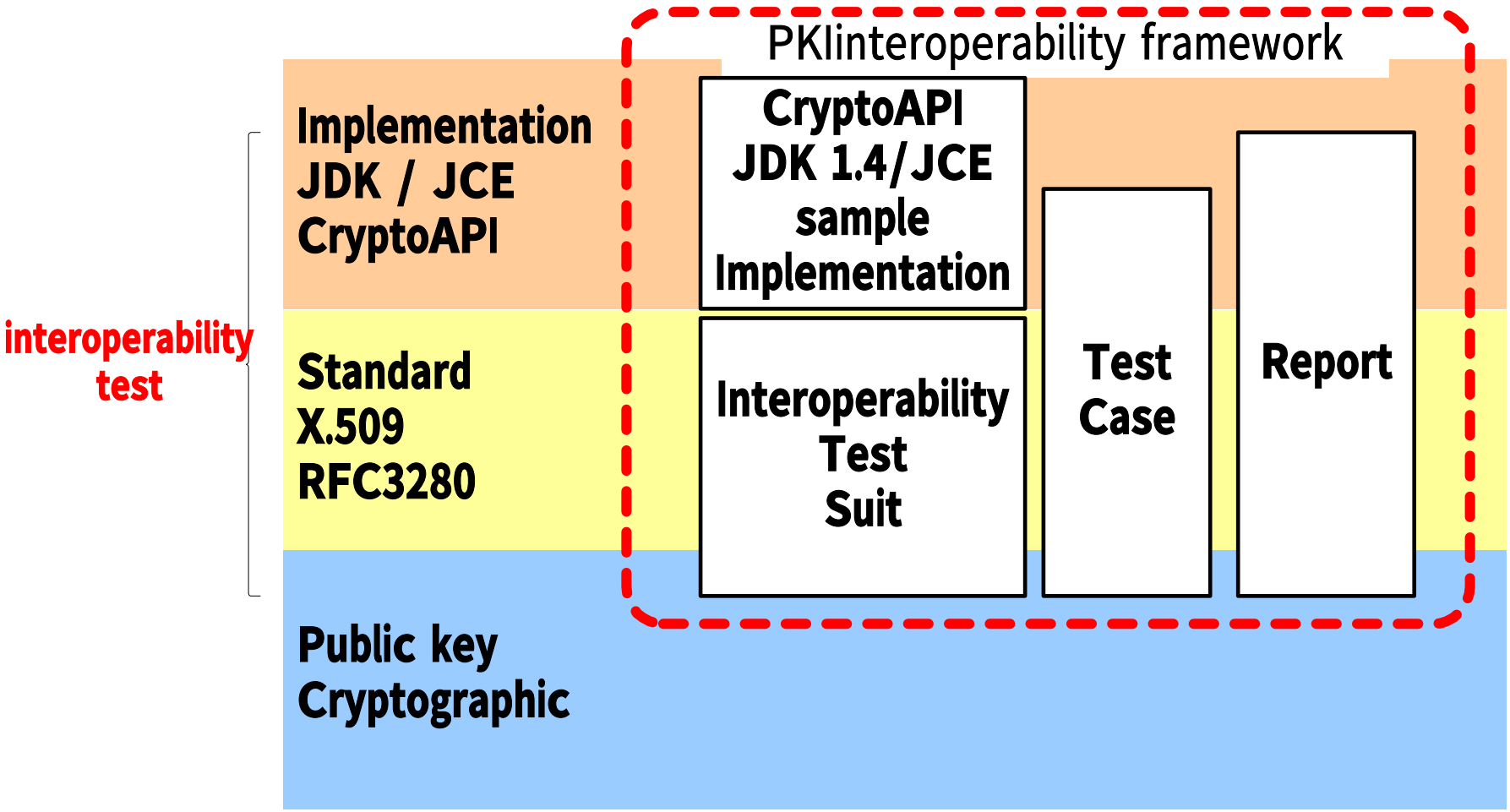
NPO **J**apan **N**etwork **S**ecurity **A**ssociation

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

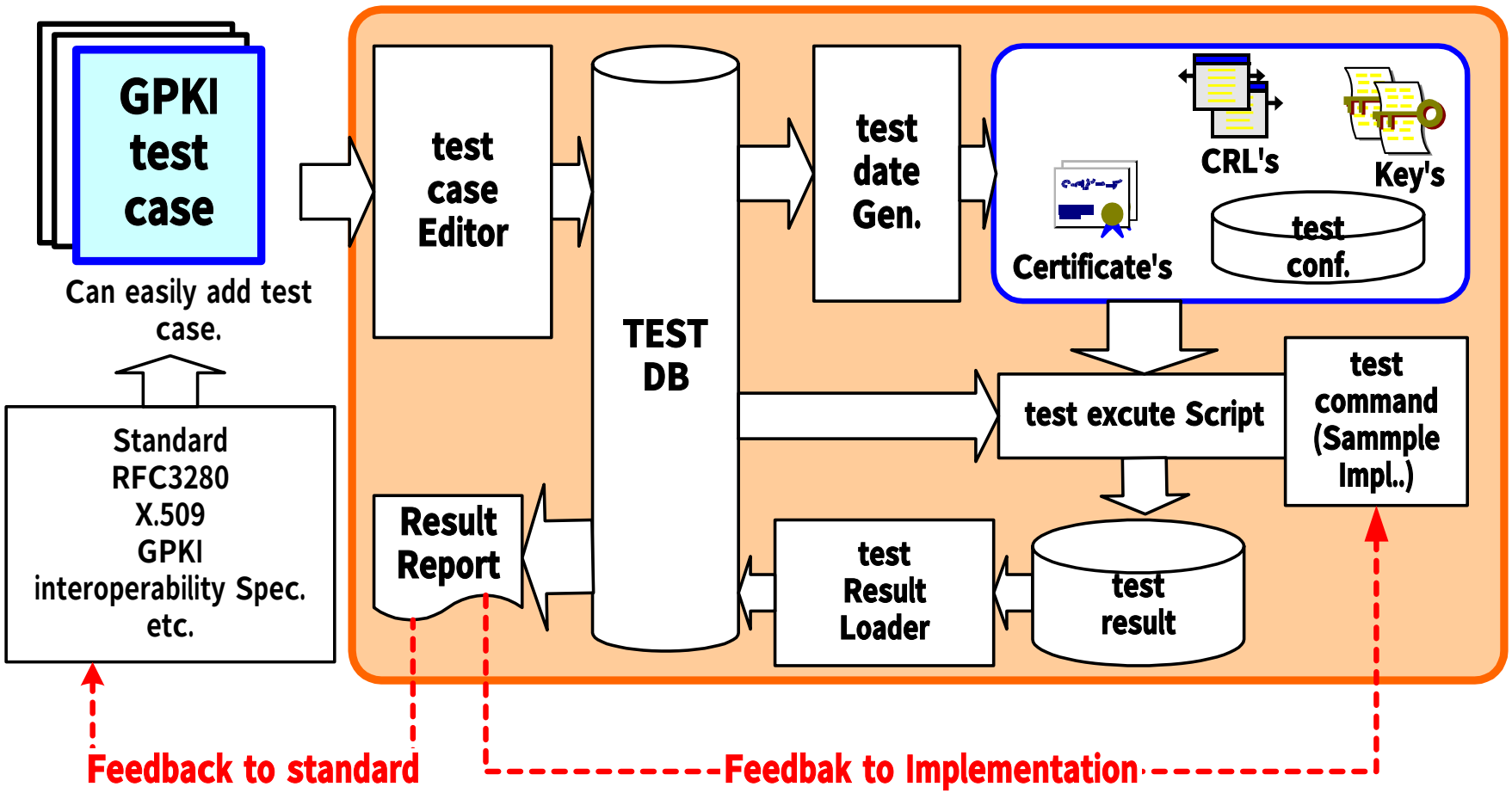
JNSA Challenge PKI 2002

- 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



PKI interoperability test suite



Challenge PKI 2002 - Test Cases

- NIST/DoD
  - X.509 Path Validation Test Suite, Version 1.07
  - http://csrc.nist.gov/pki/testing/x509paths.html
  - Total 130 cases
- GPKI (Japanese Government's PKI)
  - GPKI simulation environment
  - Total 81 cases
- JNSA Original
  - UTF8 encoding matter (name rollover certificate) which described in RFC 3280.
  - Key update issues.
  - Some CRL extensions including IDP
  - Total 45 cases
- Can easily add test case.

Sample implementations

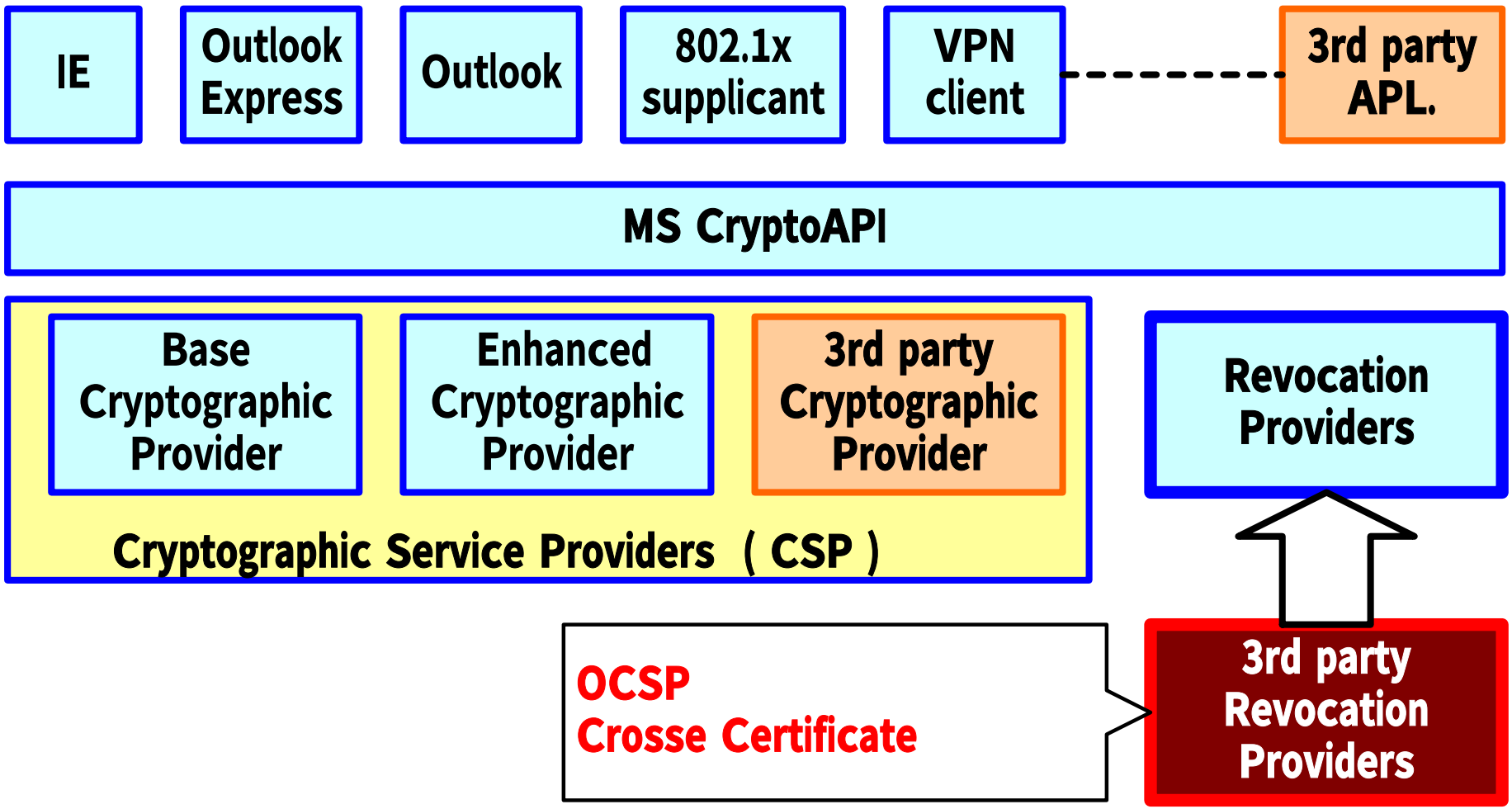
- In Java
  - Worked on JDK 1.4
    - Based on Path Discovery/Path Validation API which provided from reference implementation.
    - And additional Path Discovery/Path Validation logic which concerned multi domain PKI environment.
- In C++
  - Worked on Microsoft Crypto API.
    - Using Windows original Revocation Service Provider and additional Path Discovery/Path Validation logic which concerned multi domain PKI environment.

Requirement of GPKI and implementations

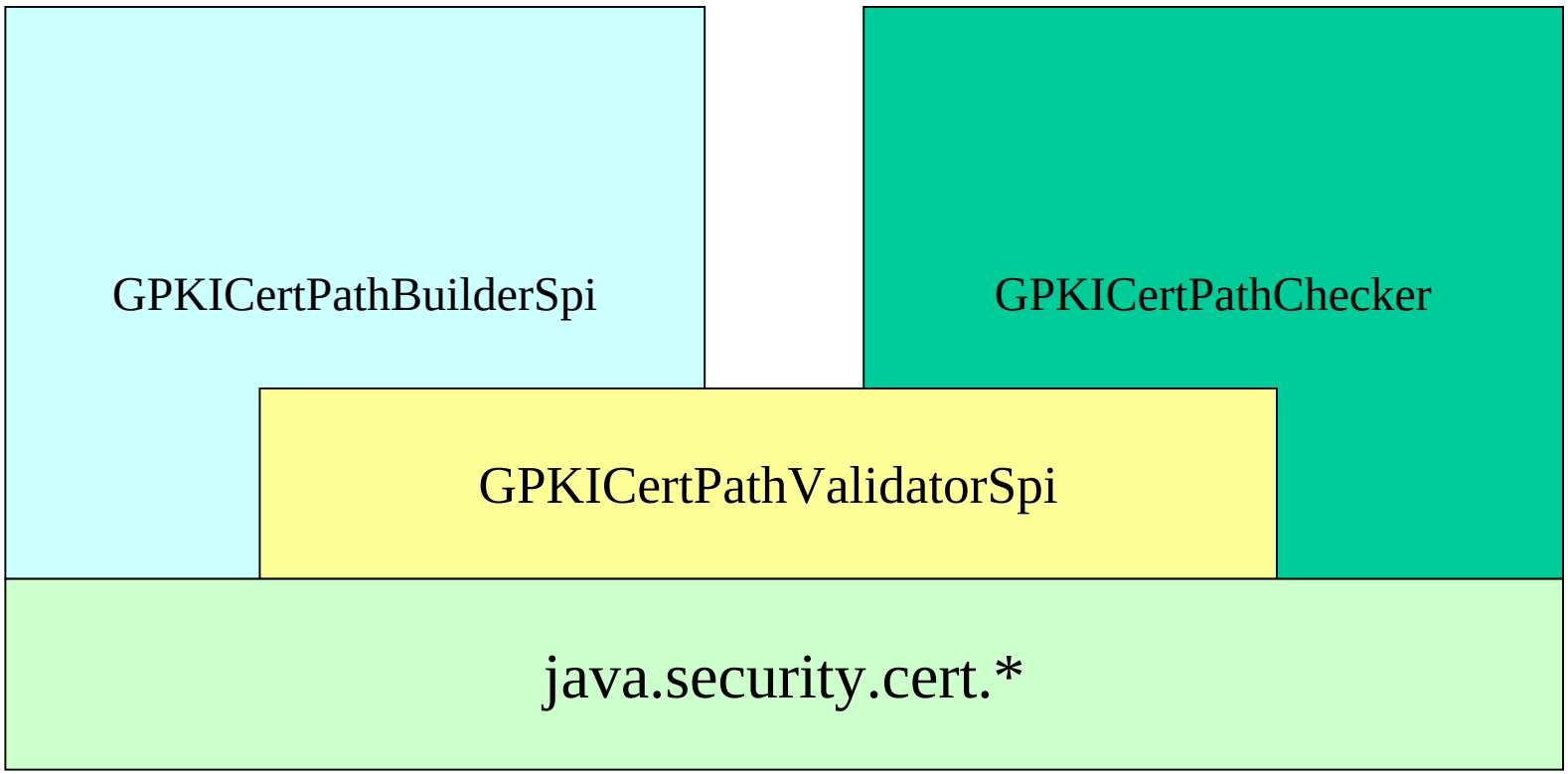
	Microsoft CryptoAPI Win-2000	Microsoft CryptoAPI Win-XP	JDK1.4 Cert. Path lib.	Sample Impl.	Requirement of GPKI
Basic Constrain	○	○	○	○	MUST
Policy Constraints	×	○	○	○	MUST
policy mapping	×	○	○	○	MUST
Name Constrain	×	○	○	○	MUST
AIA / OCSP	×	×	×	○	MUST
Path Construction	×	△	○	○	MUST
CRL IDP *1	×	○	×	○	MUST

***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)**
  - **http://www.ipa.go.jp/security/fy13/report/pki_interop/challange2001.html**
- **The report of Challenge PKI in IETF Atlanta**
  - **http://www.ietf.org/proceedings/02nov/slides/pkix-5.pdf**

Demonstration