Challenge PKI 2002 活動報告
「IETFでのPKI関連技術動向」

NPO日本ネットワークセキュリティ協会
富士ゼロックス株式会社
稲田　龍 <Ryu.Inada@fujixerox.co.jp>

2003年　6月 4日

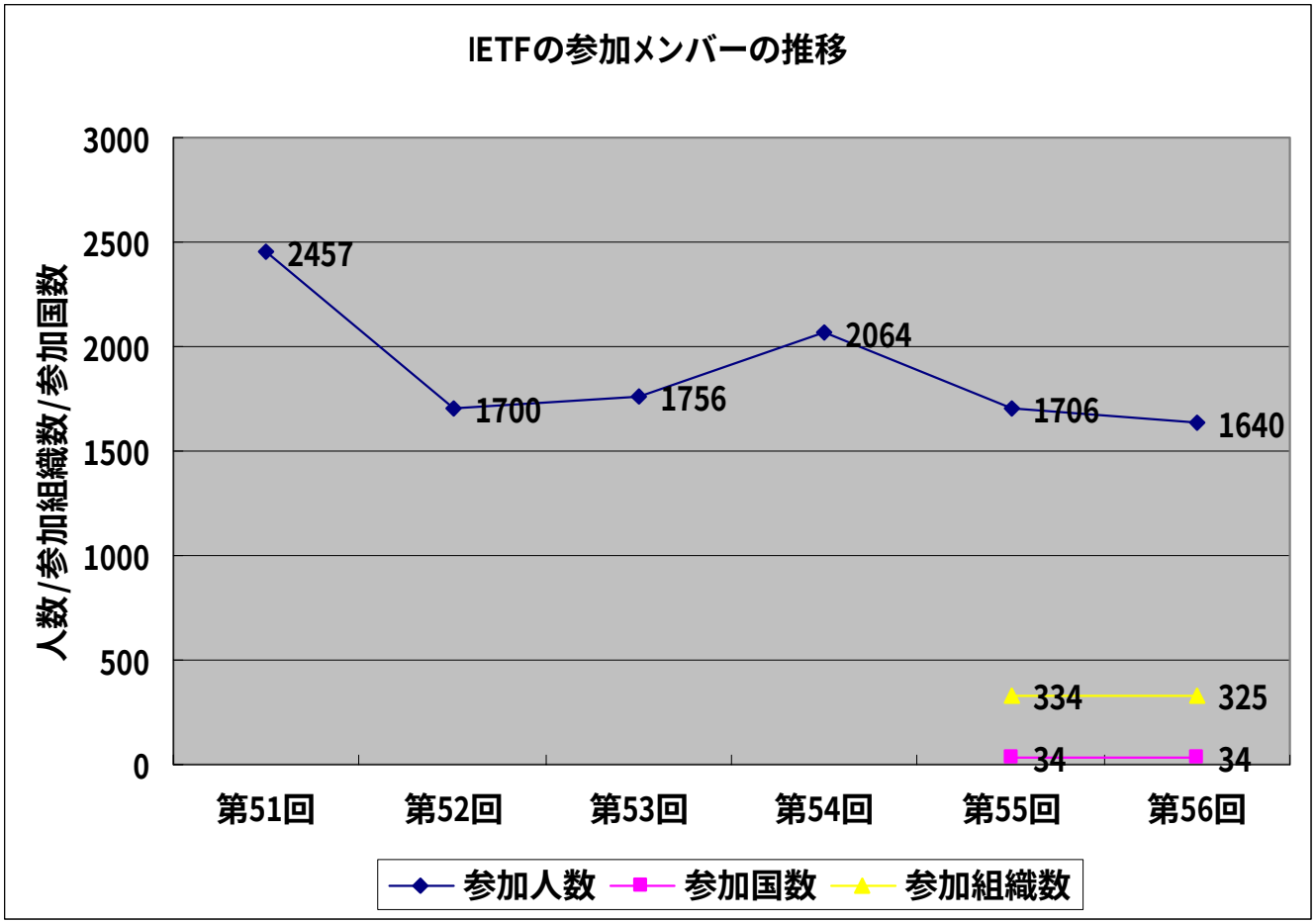
Agenda

- IETFとは?
- IETFにおけるPKIの標準化活動
- JNSAのIETFにおける活動

IETFとは?

- インターネットでの各種プロトコルを決めている団体
  - RFCを発行している
  - www.ietf.org
  - 8つのエリアにわけ、多数のWGで議論と標準化を策定している
    - Applications, General, Internet, Operations and Management, Routing, Security, Sub-IP, Transportの8エリア
    - 電子メールベースの議論が主
    - 年に3回、オフラインでミーティング(2回は米国で開催、1回は米国外で開催)
    - 次回は7月にオーストリアのウィーン(Vienna)で開催

IETFとは(その2)



最近のIETFの活動

- IPv6の標準化
- 音声/画像/動画などへのIPプロトコルの適用
  - IP電話(SIP)
- セキュリティ対策
  - IPsec/SSH/PKIなど

IETFの立場の変化

- Internetの利用範囲の拡大
  - 他の組織との間との協調/協働の増加
  - アプリケーションの増加
  - 技術領域の拡大と細分化
- Internet-Draftsのレビュー率の低下
  - IESGで「待った」がかかることが多くなった
- スポンサー問題
  - 特定の企業に左右されたくない
  - ITバブルの崩壊

56th IETF概要

- 2003年3月16日より3月21日まで
- San Francisco Hiltonにて
- 34カ国325組織1640名(集計中)の参加






IETFにおけるPKIの標準化活動

- Security Areaにおいて**基盤技術**としてPKIX-WGで議論
- **使い方**
  - Security Area
    - S/MIME
    - TLS
  - IP Area
    - IPsec
  - Operation
    - AAA
- IETFの技術領域内の多くでPKI関連の技術が利用されつつある

IETFでのPKIの利用範囲

- **認証目的**
  - S/MIME, TLS, IPsec, SIP, Diameter
- **鍵交換**
  - S/MIME, TLS, IPsec, SIP, Diameter
- **電子署名**
  - S/MIME, IPsec, SIP, Diameter

- **アプリケーションレベルでの電子署名/暗号化に関しての利用の機運が高まっている**
  - PKIXでの議論する範囲が大きくなりすぎている
  - PKIアプリケーションに関して議論するBOF/WGが出来るかも?

最近のPKIX-WGでの話題

- **証明書検証に関して**
  - RFC 337: DPD(Delegated Path Discovery)/DPV(Delegated Path Verification)
  - EEでのパス検証が重過ぎるのでサーバサイドでの検証モデルの確立
  - 56th IETF PKIX-WGでSCVPを使うことに合意
- **新しい暗号アルゴリズムの追加**
- Proxy Certificate
  - **権限代行/権限委譲の一モデル**
- Qualified Certificate
  - **身分証明書として使える証明書の形式とは?**
- PKI**利用の新アプリケーション**
  - TAP
- **他組織とのアライアンス**
  - OASIS/W3C/EESSI/JNSA

JNSAのIETFにおける活動

- 第54回@横浜
  - PKIX-WGでChallenge PKI 2001の報告
- 第55回@Atlanta
  - PKIX-WGでChallenge PKI 2002の中間報告
- 第56回@San Francisco
  - PKIX-WGでChallenge PKI 2002の最終報告およびデモンストレーション

56th IETFのトピック

- Security Area Directorの変更

–MITのJeffrey I. Schiller氏が退任

–Russell Housley氏(Virgil Security社)が新任

- 元RSA Laboratories.
- RFC2459/3280の著者の一人
- S/MIME WGの元チェア

56th IETF PKIX-WGでの議論

- **参加**: 76**人**
- Chairs: Stephen Kent(BBN), Tim Polk(NIST)
- 19**本の**Internet-Drafts(I-Ds)
  - **近々**Last Call
    - SCVP, Proxy Cert
  - Expire**を待たずに廃棄される**Draft**もある。**
  - Area Director**からのコメント待ち**
    - Repository Locator Service


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

Agenda

- DPD/DPV standard selection process
- SCVP Discussion
- Proxy Certificates
- Signature Algorithms & Key Usage
- Trusted Archive Protocol
- Qualified Certificates Profile
- *LDAP/X.500 alignment*
- Subject Identification Method
- *EESSI*
- *JNSA ChallengePKI 2002*
- LDAP PKI Issues

Liaison

NPO 日本ネットワークセキュリティー協会
Japan Network Security Association

DPV/DPD Strawpoll – Tim Polk(NIST)

- RFC3379に対応するプロトコルを絞り込む。
  - SCVP, CVP, DVCS, OCSPv2
- 要件をあげたMatrixを作成
  - 各プロトコルはMatrixを埋めMLに送付
  - Matrixをもとに、PKIXのML上で投票が行われた。

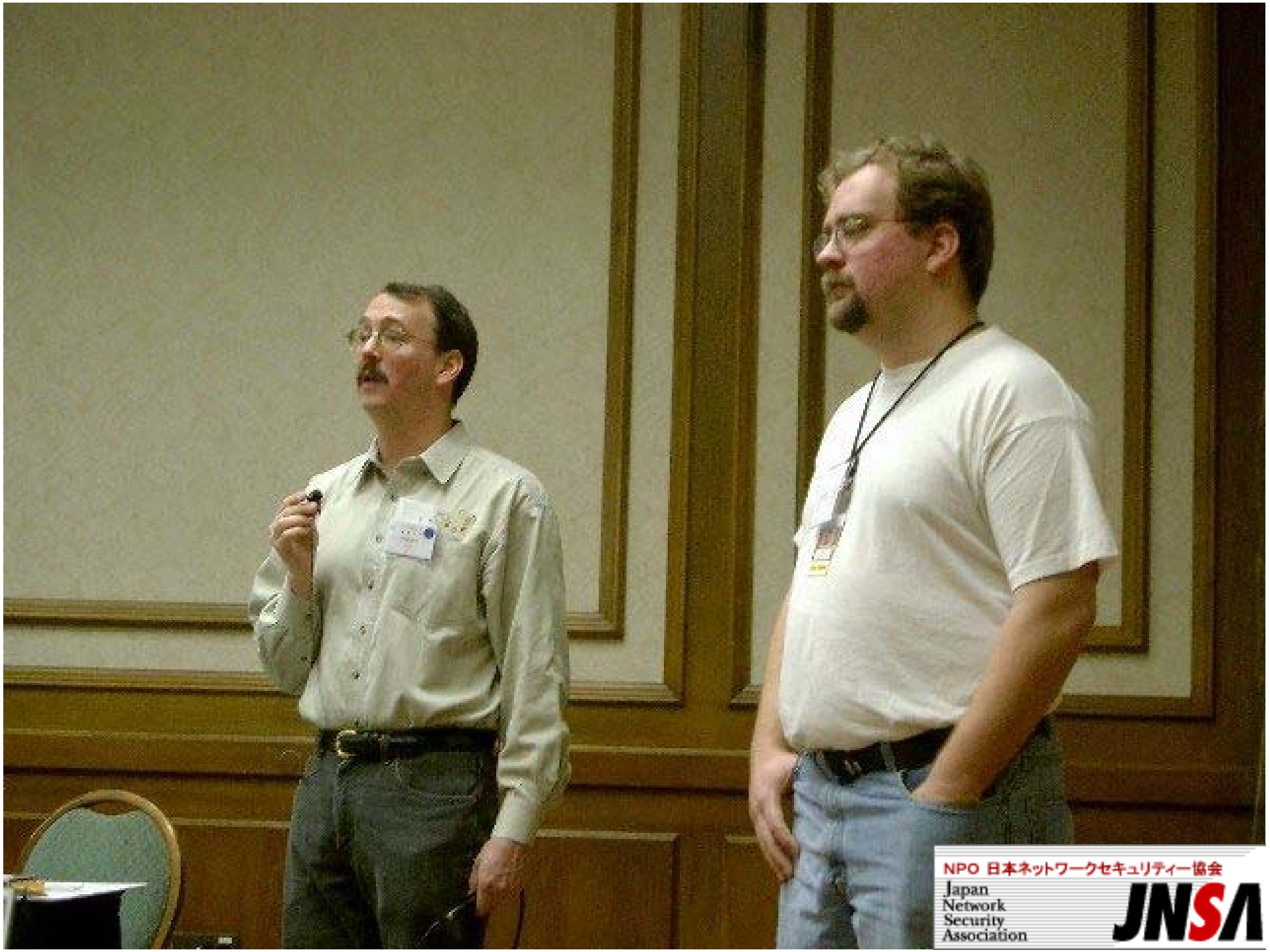
- SCVPが、投票の過半数を得、最小限の修正でRFC3379を満たすと判断された。

SCVP - Trevor Freemen (Microsoft)

- **投票の結果を踏まえ**
  - 5**月末にドラフトを更新予定。**
  - 57th@Vienna**までに**LastCall**の予定。**
- MAC**認証機能を追加する。**
  - RFC3379**要件なのか**?
- **いくつかの**ValidationPolicy**を明文化する。**
  - **アプリケーション毎に要求されるものを選別**
    - S/MIME, IPsec, TLS**など**
- **現時点では、標準を意識した仕様ではなく、製品仕様を文書化したもののように見える。**
  - **標準仕様として必要な機能と、そうでないものを、これからふるいにかける予定らしい。**

Proxy Cert - Von Welch (Argonne Labs)

- EEが権限の委任目的で(他の)EE証明書を発行可能とする仕組み
  - issuerがEEとなる。
  - ProxyCertificateであることが明確になるようにcritical拡張として明記
- ProxyCertに関してのパス検証方法について追記
  - 通常のパス検証ではProxyCertは、検証できない
- WGのLast Call待ち。


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

Signature Algorithms & Key Usage – Jim Schaad (Soaring Hawk Consulting)

- PKCS#1のPSS/OAEPやDH/DSAの違いがkeyUsageに与える影響を明確にしよう、という試みに見えた。
  - algorythmIDを新たに定義すべき、との話も出ていた
- 中心メンバが割と興味を持って聞いていた。
  - Russ, Steve Kent, Timなど


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

Trusted Archive Protocol – Carl Wallace (Cygnacom)

- (長期保存データ)のアーカイブのデータ構造や、アーカイブ方法を定義したもの。
  - Data Validation: Evidence verification
  - Path Processing: Evidence Collection
- TSP messageにはCMSが使われる。
- www.openevidence.orgでサーバを公開している。
  - DVCSとの違いは何か?
- WG Draftにはならなかった。
  - 最近MLでTAP支持者が増えている。
    - DVCSの著者Peter Sylvesterが支持してた。
  - PKIXEXTとかPKIXAPPSとかのWGを立ち上げよう、と言っている人たちもいる。


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

QC Profile - Stefan Santesson (RetroSpekt)

- Scopeを明確化した。
  - 今までは単なるプロファイルセットだった。
  - For identify certs issued to physical persons
  - # Legal Regurationsに従うものでなければならない?
- DNに関する要件をいくつか修正
  - issuerのサブツリーでなければならないとか。
  - RFC3280にはない属性を導入した。
- keyUsageに関する要件を修正
  - nonRepudiationに限定しない。
  - 個々のセキュリティポリシや法制度に委ねる。


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

LDAP/X.500 alignment – Skip Slone (Lockheed-Martin)

- X.500 5th が2005年までにリリースされる。
- ";binary"
- enhanced Matching
- nonRepudiation → contentCommitment

Subject Identification Method - Park Jong-Wook (KISA)

- **プライバシ保護のために、**non-public**な** peronsl ID**が必要。**
  - sensitive ID: national Id**など**
  - protection ID: national Id**のハッシュなど**
- **修正の反映など作業報告のみ。**
- 3**月末に上記事項を**revise**予定。**


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

EESSI– Riccardo Genghini

- European Electronic Signature Standardization Initiative
- EU**電子署名標準のレビュ状況などの説明**
- 57th Vienna**の後に**PKIX/EESSI**のジョイントを提案**


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

JNSA ChallengePKI2002

- JNSAが行ったChallenge PKI 2002の説明とデモンストレーションを行った。

- 報告書の英訳とソースコードの公開を約束

NPO 日本ネットワークセキュリティー協会
Japan Network Security Association


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

LDAP PKI Issues – David Chadwick (Univ of Salford)

- subjectDN**以外の属性からも、証明書や**CRL**を探したい。**
  - component matching
    - **クライアントの対応が必要**
  - Attribute Extraction
    - **証明書の属性を解析するフロントエンドを用意する。**
    - CA/RA**からの登録時のみ、このフロントエンド経由で**LDAP**へアクセス。**
    - **通常は、単なる**LDAP**アクセスでよい。**
- **投票の結果**ComponentMatching**を採用することに。**
  - **投票者は少なかった模様**


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA


NPO 日本ネットワークセキュリティー協会
Japan
Network
Security
Association
JNSA

Multi Domain PKI Test Suite

-- Result of JNSA Challenge PKI 2002 --

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

As representative of

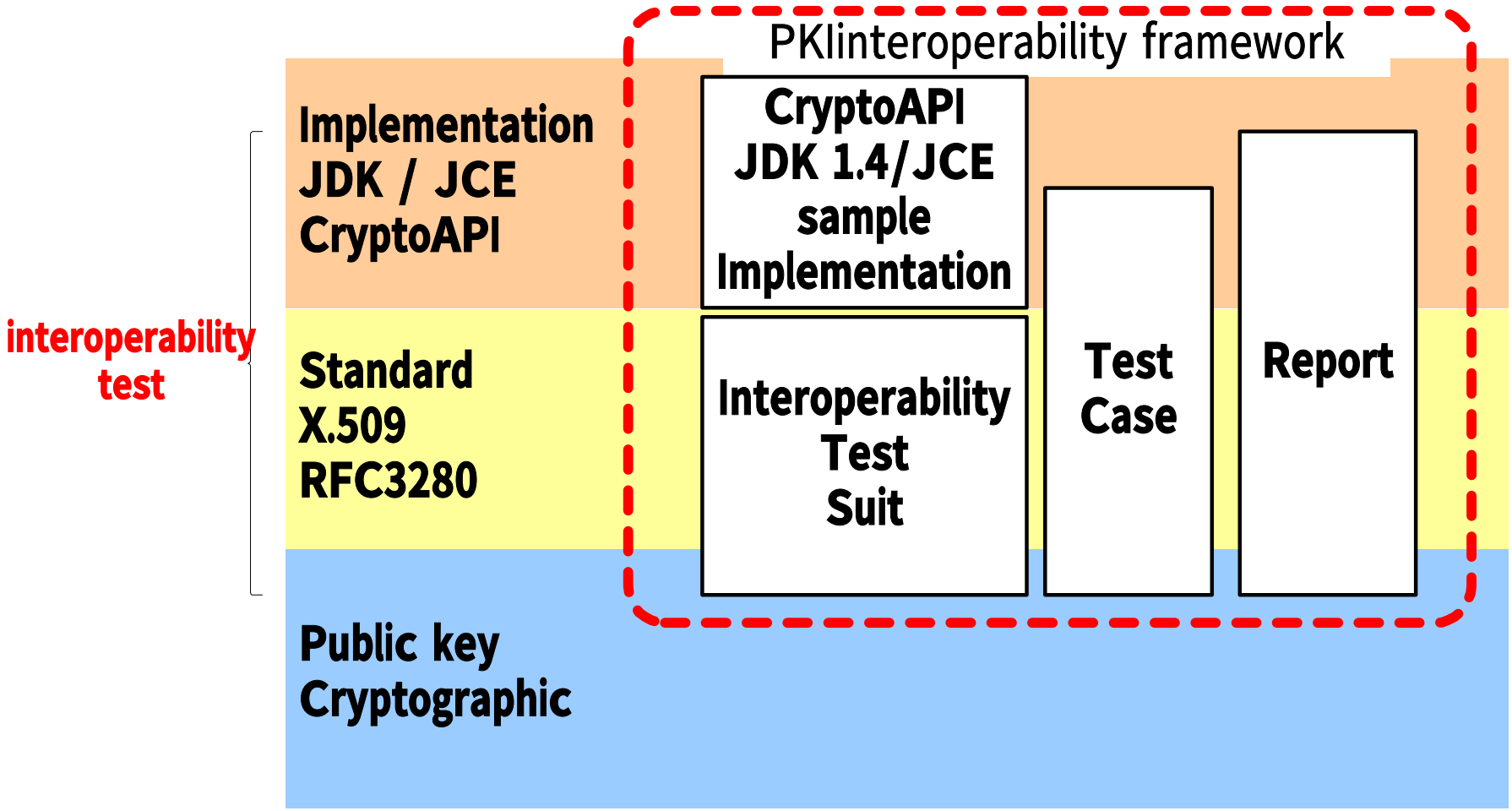
NPO **J**apan **N**etwork **S**ecurity **A**ssociation

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

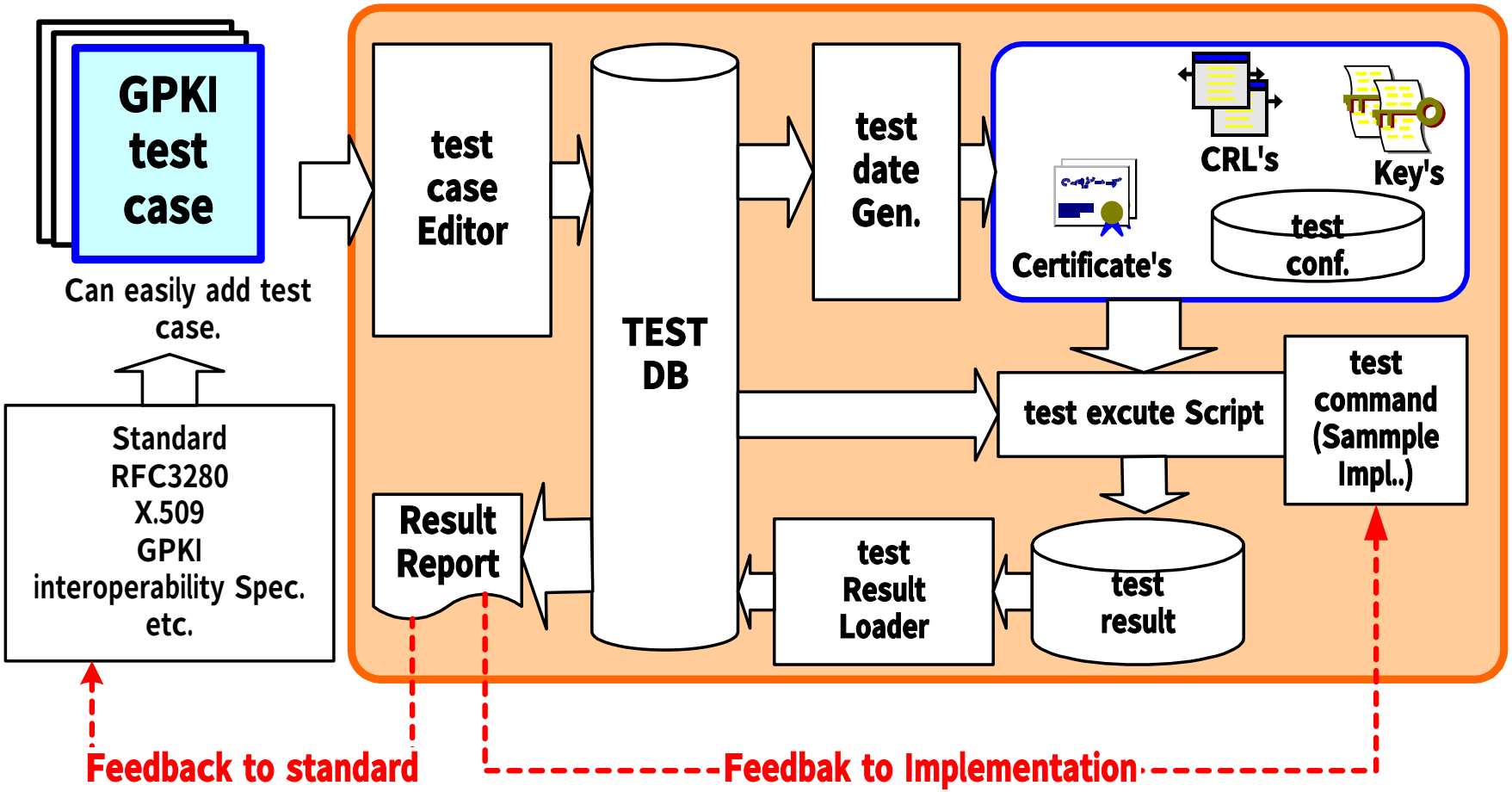
JNSA Challenge PKI 2002

- 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

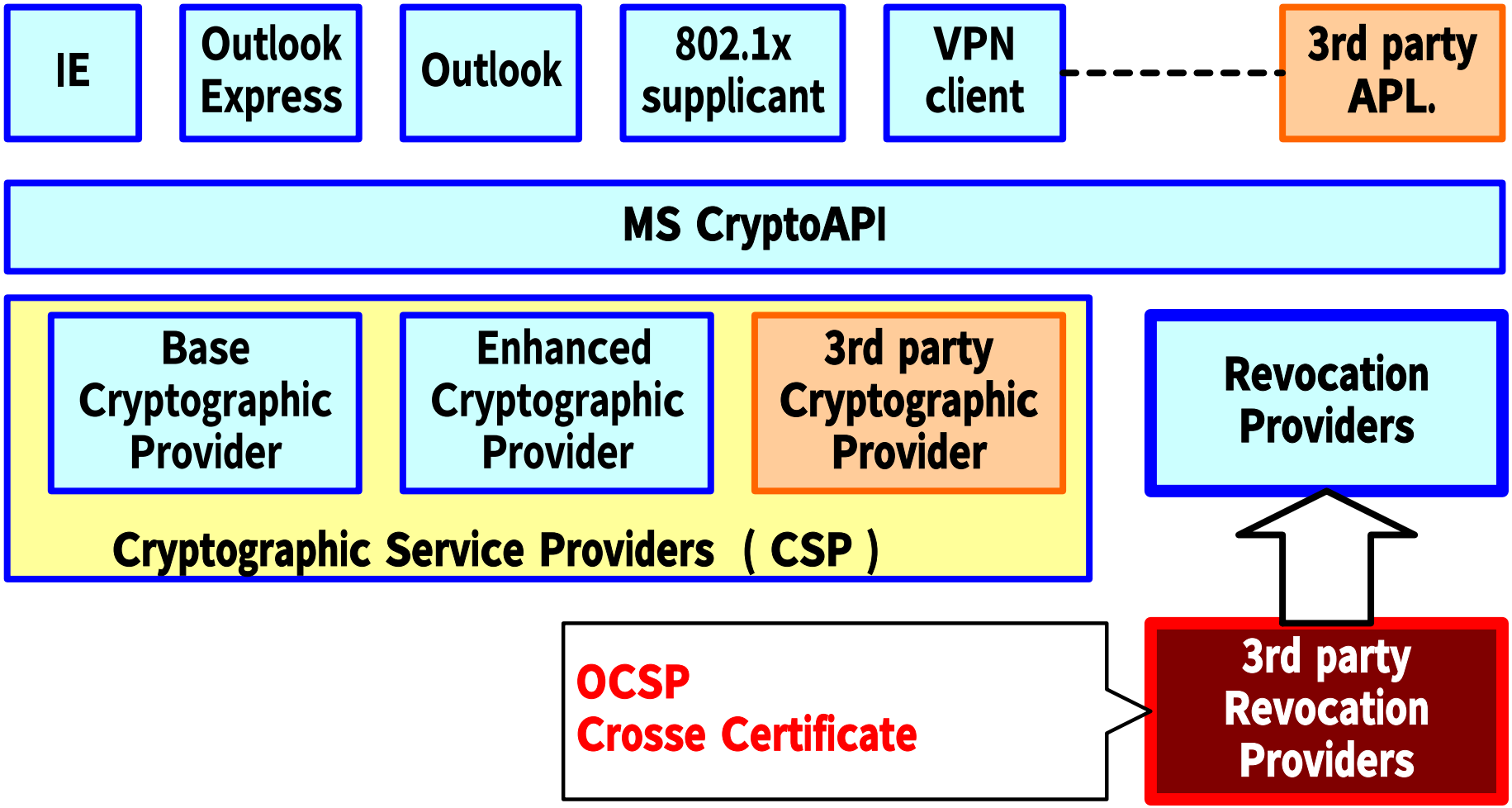
- In Java
  - Worked on JDK 1.4
    - Based on Path Discovery/Path Validation API which provided from reference implementation.
    - And additional Path Discovery/Path Validation logic which concerned multi domain PKI environment.
- In C++
  - Worked on Microsoft Crypto API.
    - Using Windows original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

Requirement of GPKI and implementations

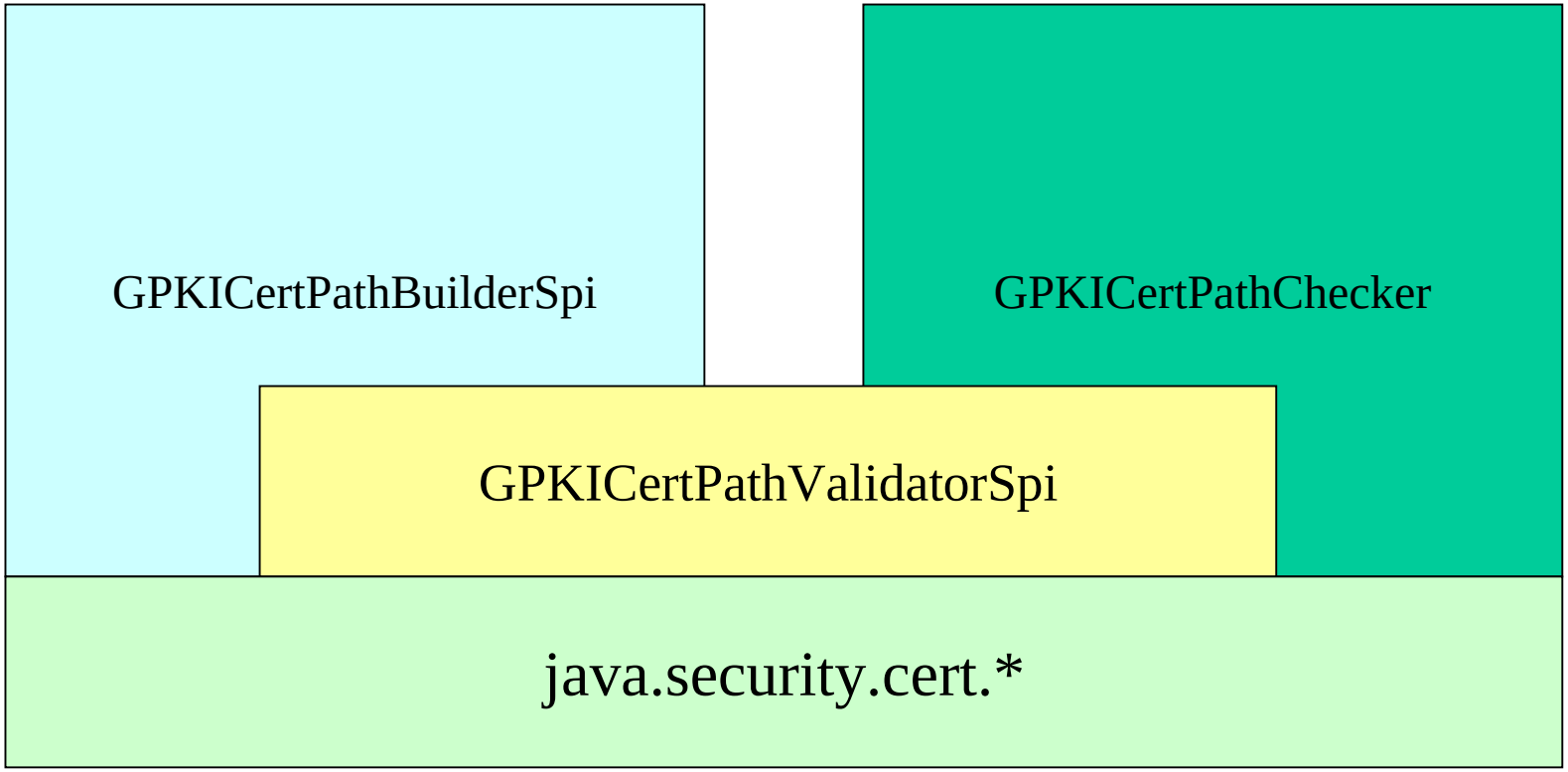
	Microsoft CryptoAPI Win-2000	Microsoft CryptoAPI Win-XP	JDK1.4 Cert. Path lib.	Sample Impl.	Requirement of GPKI
Basic Constrain	○	○	○	○	MUST
Policy Constraints	×	○	○	○	MUST
policy mapping	×	○	○	○	MUST
Name Constrain	×	○	○	○	MUST
AIA / OCSP	×	×	×	○	MUST
Path Construction	×	△	○	○	MUST
CRL IDP *1	×	○	×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

***1 CRL IDP (issuing distribution point)**

Sample implementation for CryptoAPI



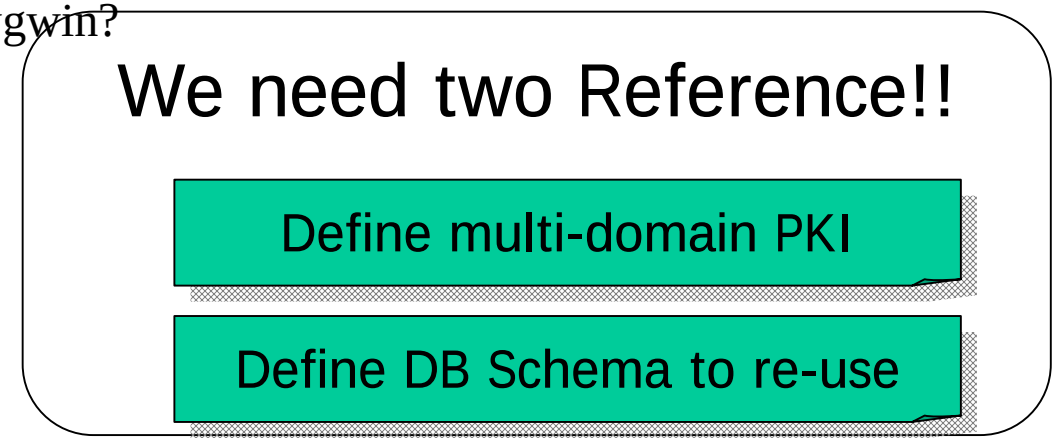
Sample implementation for JAVA



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?



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