PKIアプリケーションの相互運用を促進する Challenge PKI 2002

NPO 日本ネットワークセキュリティ協会
／セコム株式会社IS研究所
松本　泰
yas-matsumoto@secom.co.jp

2003 年 6月 4日

PKIアプリケーションの相互運用を促進する Challenge PKI 2002

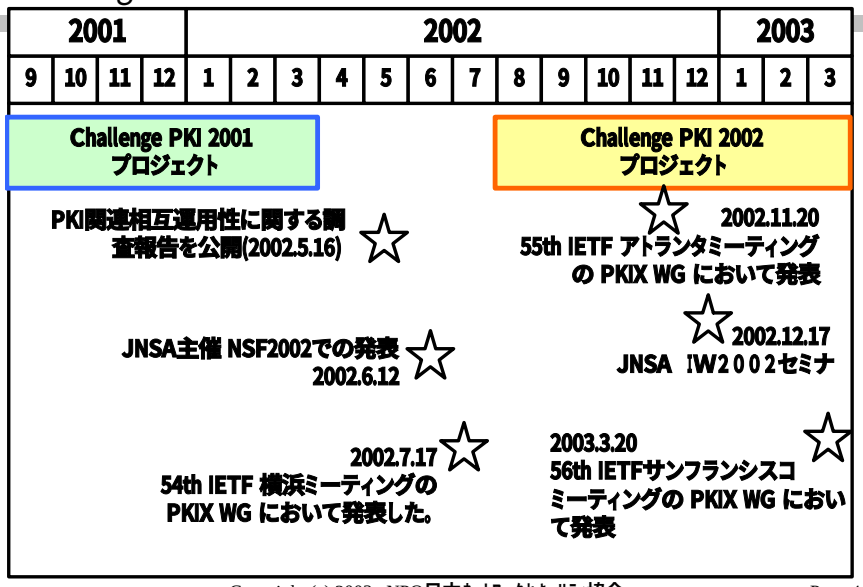
JNSA

- Challenge PKI 2002は、 GPKI/LGPKI/公的個人認証基盤などのPKIアプリケーションの相互運用性の確保を支援するためのフレームワークの確立を目指したプロジェクトである。プロジェクトの成果は、54th-IETF横浜、55th-IETFアトランタ、55th-IETFサンフランシスコで発表しており、今後は、これまでの成果を生かしたRFCの作成も検討している。本講演では、Challenge PKI 2002の内容と今後の展望を説明する。

NPO JNSAにおけるPKI相互運用関連の活動

- Challenge PKI 2001
  - 情報処理振興事業協会 (IPA) の委託を受けて実施
  - 9つのCAが参加を得て行ったマルチドメインPKI、マルチベンダーPKIのPKI相互運用実験
- Challenge PKI 2002
  - 情報処理振興事業協会 (IPA) の委託を受けて開発
  - 昨年度のプロジェクト。相互運用テストスィートの開発など
  - よりPKIアプリケーションよりのPKI相互運用の課題に挑戦
  - GPKIのようなマルチドメインPKI、マルチベンダーPKIの開発を容易にする
- Challenge PKI 2001とChallenge PKI 2002の目標
  - マルチドメインPKI、マルチベンダーＰＫＩ環境下でのPKI相互運用フレームワークの確立
- その他のPKIに関連した活動
  - IPsec相互接続実験、無線LAN相互接続実験などでのPKIの認証
- NPO JNSAのモチベーション
  - PKIのインフラとしての必要性を社会にアピール
  - ネックとなるPKI相互運用性の問題などを自ら解決していく

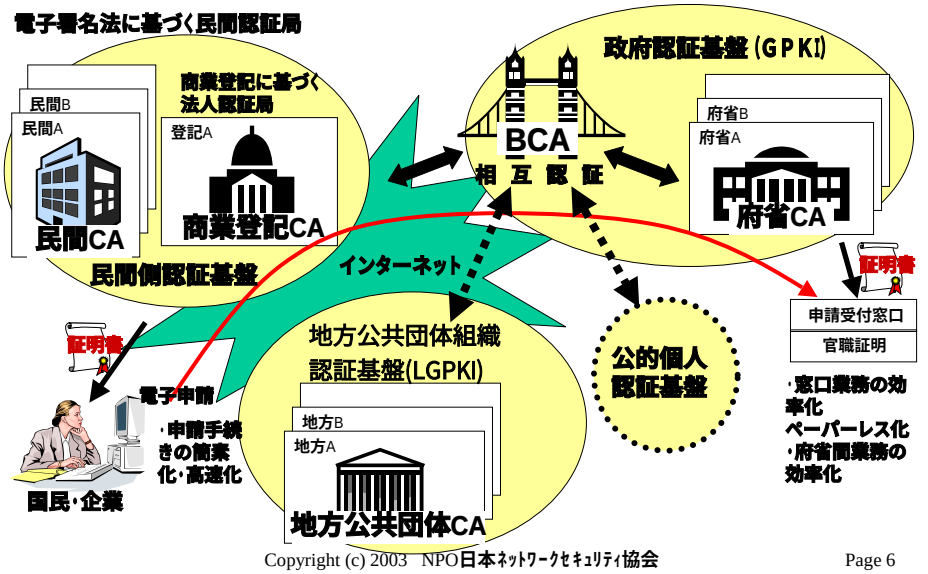
NPO JNSAにおけるPKI相互運用関連の活動 Challenge PKI 2001&2002



Challenge PKI 2002 - プロジェクトの背景

- 電子政府の成功の鍵のひとつ - アプリケーションの流通
  - 使いやすくセキュアなPKI/GPKI・電子政府対応アプリケーションの流通
    - 相互運用性が確保されたPKI/GPKI対応電子政府APLの流通
    - COTS (Commercial Off-The-Shelf) の流通も必要
  - しかし、現実は
    - GPKI Readyなアプリケーションを開発するための、参考がない、テスト環境、開発環境がない、テストの方法が分からない etc….
  - これらを解決することは、PKIを基盤とした広範囲なセキュリティを適正なコストで実現することにつながる。
- 標準化の問題点
  - IETFなどのセキュリティ関連の標準化が必ずしも成功していない
    - ラフコンセンサス アンド ランニングコードで成功したIETFの標準も、セキュリティ関連の標準化は必ずしも成功していない
    - 標準といわれるRFCに対して色々な実装 (コード) が出てくるが、どこまで実装されているか？その実装が正しいか誰もわからなくなりつつある。
  - GPKIの仕様や実装もこの不安定な? RFCなど準拠している
    - どのように実装してテストすればよいかわからない….
    - 仕様 (GPKI相互運用性仕様書) はあっても準拠性がわからない

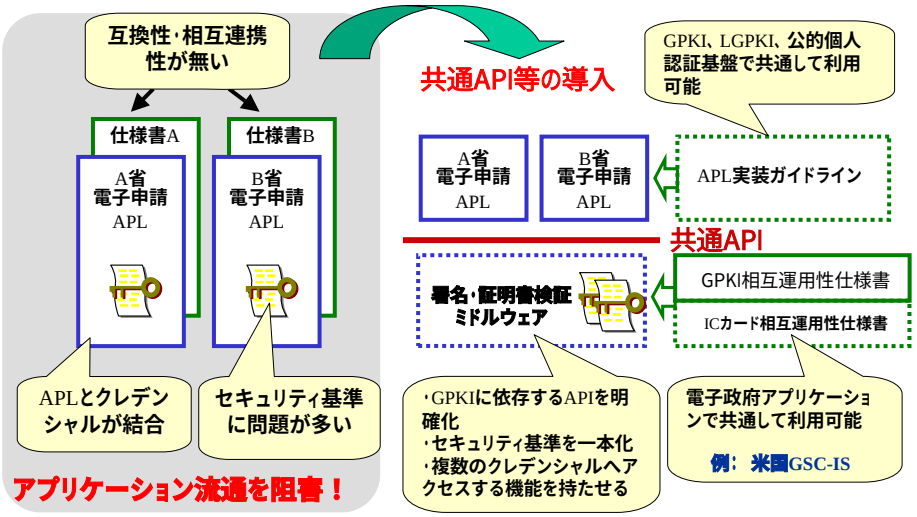
Challenge PKI 2002 - プロジェクトの背景
GPKI、LGPKI、公的個人認証基盤



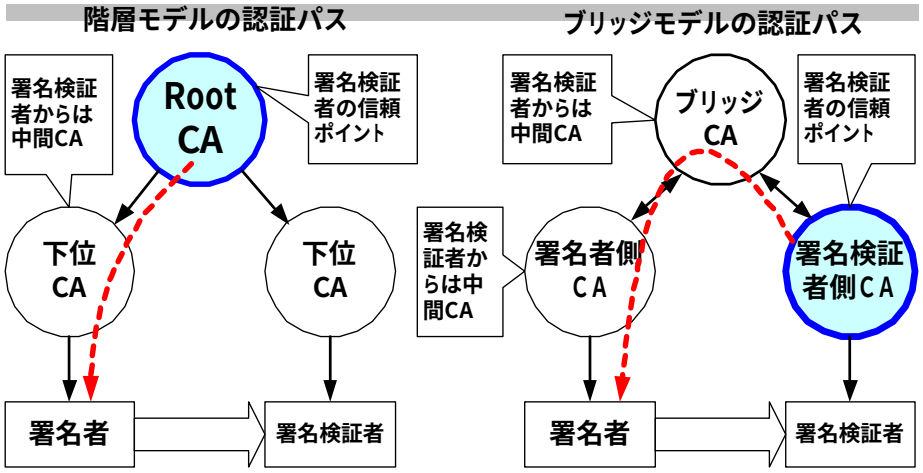
Challenge PKI 2002 - プロジェクトの背景
電子政府アプリケーションの相互運用性の課題

- 電子政府の認証基盤のモデル - マルチドメインPKIと複数アプリケーションのモデル
  - 色々なPKIドメインの認証局が発行した証明書が、色々な電子政府アプリケーションで利用可能なモデル。
  - 成功すれば効果が大きいが、敷居も高い。
  - 特に相互運用性に課題が大きい
- 署名側の課題
  - 署名環境のセキュリティ関する指針が存在しない
  - 1枚の証明書が色々な電子政府アプリケーションに対応するためのフレームワークが不在
- 署名検証側の課題
  - GPKI,LGPKI、公的個人認証基盤、民間認証局、海外へと広がる認証基盤に対応する署名検証のメカニズムの対応が重要
  - Challenge PKI 2002が注目している課題

Challenge PKI 2002 - プロジェクトの背景
電子政府アプリケーションの構成

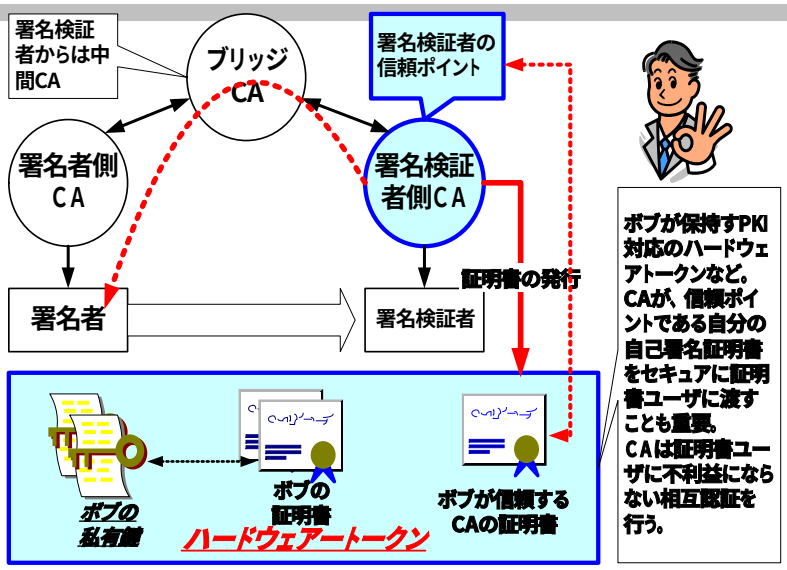


Challenge PKI 2002 - プロジェクトの背景
階層モデルとブリッジモデルの認証パス

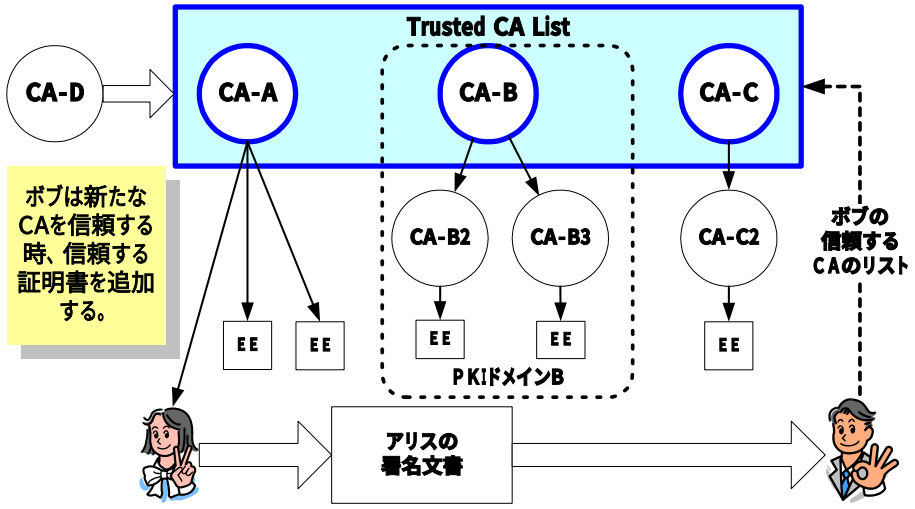


RFC3280などに記述されている認証パス検証は、信頼モデルに依存しない。しかし、ブリッジモデルでは、その性格から、RFC3280の仕様の多くの部分の実装が要求され、高度なPKI相互運用技術が要求される。

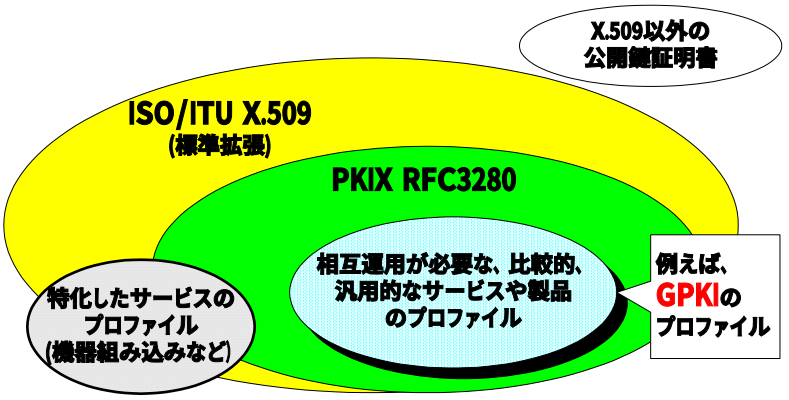
Challenge PKI 2002 - プロジェクトの背景
ブリッジモデルにおける信頼ポイントの扱い



Challenge PKI 2002 - プロジェクトの背景
証明書信頼リストによる方法 (Webモデル)



Challenge PKI 2002 - プロジェクトの背景
証明書のプロファイルの関係



- RFC3280 (RFC2459) 準拠の意味するもの
  - **証明書発行そのものよりも、そのプロファイルを解釈するアプリケーションの実装が格段に難しい。アプリケーションにおいて、100% RFC3280サポートは、まずない。**

Challenge PKI 2002 - プロジェクトの背景
GPKIの要求とパス検証の実装

	Microsoft CryptoAPI Win-2000	Micosoft CryptoAPI Win-XP	JDK1.4 Cert. Path lib.	サンプル実装(*1)	GPKIの要求 (パス構築、パス検証)
基本制約拡張	○	○	○	○	必須
ポリシ制約拡張	×	○	○	○	必須
ポリシマッピング拡張	×	○	○	○	必須
名前拡張	×	○	○	○	必須
AIA拡張 / OCSP	×	×	×	○	必須(官側のみ)
動的パス構築	×	△	○	○	必須
CRL IDP *2	×	○	×	○	必須

*1 Challenge PKI 2002プロジェクトで開発したサンプル実装

*2 CRL IDP (issuing distribution point)

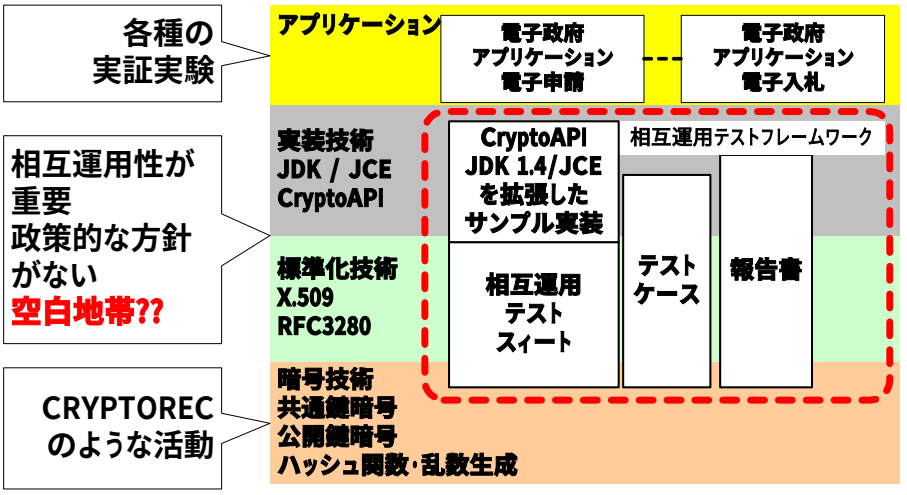
Challenge PKI 2002の目標 - その1

マルチドメインPKIの問題点	解説	Challenge PKI 2002の目標
標準の曖昧さ	マルチドメインPKIなどの場合、新しい標準を参照しており、その曖昧さが問題になる。	実装、実験を通じ曖昧な部分を明確にしてIETF/PKIXなどにフィードバックする。 54thIETF横浜、55th アトランタ、56th サンフランシスコなどでの発表
テスト・クライテリア	マルチドメインPKIに対応した実装があってもテストケースが少なく標準への準拠性が分からない	主にGPKIに対応したテストケースを設計し提供する。また、テストケースを容易に拡張できるものを提供しGPKI以外でもテストを可能にする。
テスト環境	マルチドメインPKIのテスト環境を構築することは非常に困難。	マルチドメインPKIをターゲットにしたPKI相互運用テストスィートを開発し提供する。1台のLinuxマシンで多くのCA環境をシミュレート。

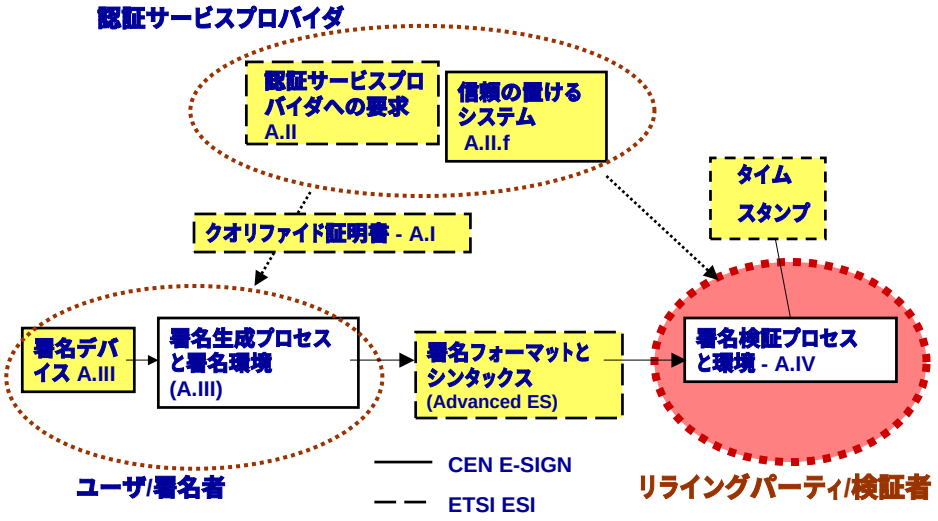
Challenge PKI 2002の目標 - その2

マルチドメインPKIの問題点	解説	Challenge PKI 2002の目標
レファレンス実装	ブリッジモデル(GPKIなど) で必要とされる証明書検証の実装が分かりづらい	Microsoftのプラットホームと Javaの環境でレファレンスとなるサンプル実装を提供する。また、テストを行いその結果を報告書に記述する。
分かり易い解説書	標準、テスト、実装、そして将来の方向性の関係が分かりづらい	X.509、RFC3280などの標準、色々なテストケース、実装を解説した報告書を作成する。
共通のテストプラットホーム	マルチドメインPKIのテスト環境の難しさは日本に限ったことではない。世界で共通で使用できるテストプラットホームが必要。	テストスィートなどを海外へも配布できることを検討。また、IETFなどでもテストの標準化などを提言し、マルチドメインPKIの定義やテストスィーマなどのRFC化なども検討。

Challenge PKI 2002-プロジェクトの範囲



Challenge PKI 2002-プロジェクトの範囲
EESSIの認証フレームワーク



Challenge PKI 2002 - プロジェクトの成果物

- PKI相互運用テストスィート
  - PKI相互運用テストを行うための道具
  - 世界中で汎用的に使用できることが目標
- GPKIテストケース
  - PKI/GPKIのパス検証のテストケース
  - 実装に対して、どこまで実装できているか？何が正しいか？
- サンプル実装
  - パス検証の実際に動作するコード
    - RFC3280/GPKI相互運用性仕様書に準拠した実装（ランニングコード）
- 実装ガイド調査報告書

Challenge PKI 2002-プロジェクトの成果物
相互運用フレームワークの構成

相互運用テストフレームワーク

◆GPKIテストケース設計書

◇GPKI模擬環境テストケース
◇DoD/FPKIパス検証テストスィート
◇オリジナルテストケース

◆GPKIアプリケーションサンプル実装の開発

◇ Javaによるサンプル実装
◇ CryptoAPIによるサンプル実装
◇ 証明書検証サーバのクライアント

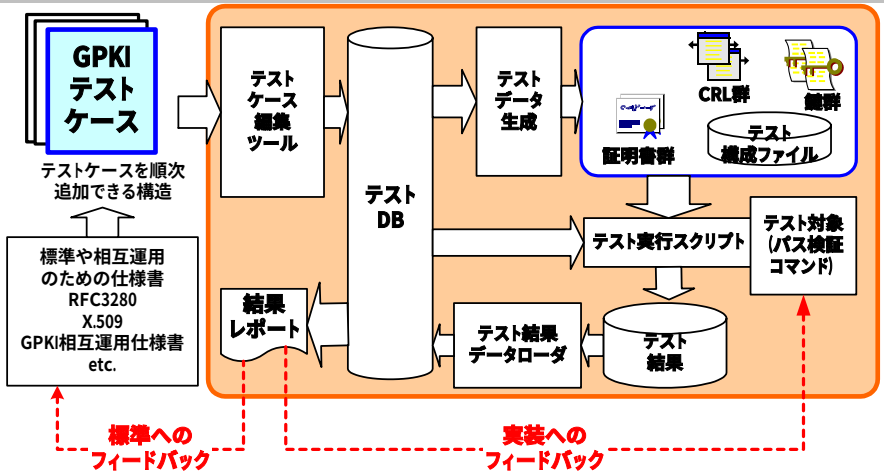
◆GPKIアプリケーション実装ガイド報告書

◇証明書パス検証の標準や仕様の説明
◇証明書パス検証サーバなどの新しいモデルの説明
◇証明書パス検証のテストクライテリアの動向
◇各種の実装の説明
◇Javaによる実装の説明
◇CryptoAPIによる実装の説明
◇まとめ

◆相互運用テストスィートの開発

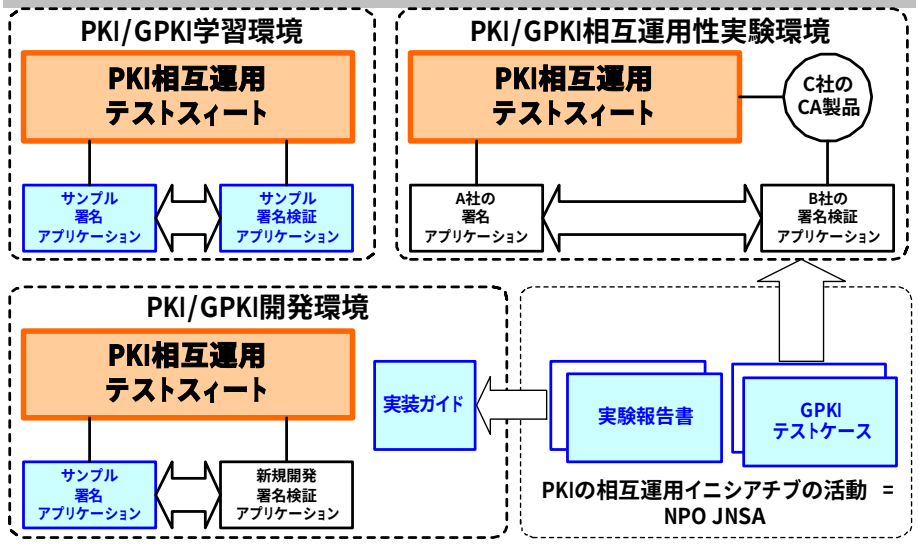
◇テストデータベース
◇テストデータ生成ツール
◇テスト実行環境
◇各種DBツール
◇リポジトリ
◇OCSPレスポンダシミュレータ
◇証明書検証サーバシミュレータ
◇インストーラ

Challenge PKI 2002-プロジェクトの成果物
相互運用テストスィート

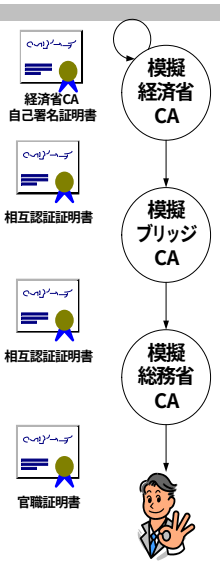


テストデータ生成のための暗号プリミティブには、名古屋工業大学岩田研究室が開発したAICryptoを使用

Challenge PKI 2002-プロジェクトの成果物
PKI相互運用テストスィートの利用イメージ



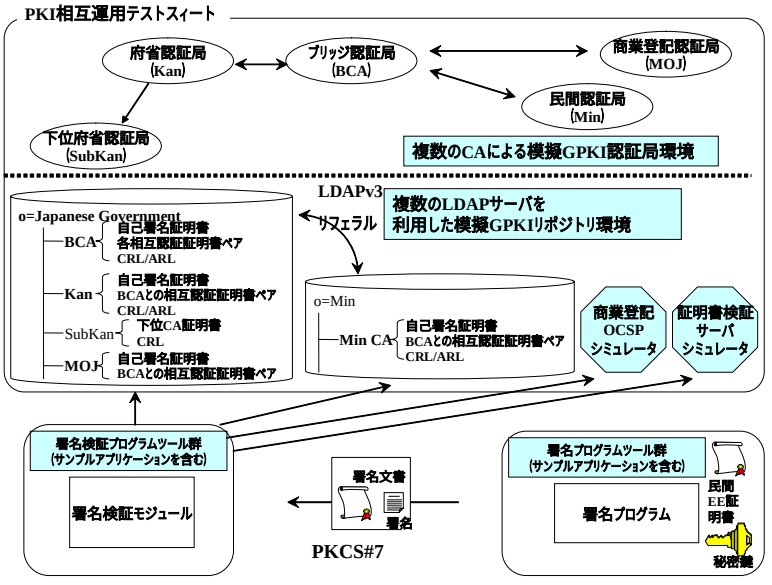
PKI相互運用テストスィートの画面
証明書パスの編集画面



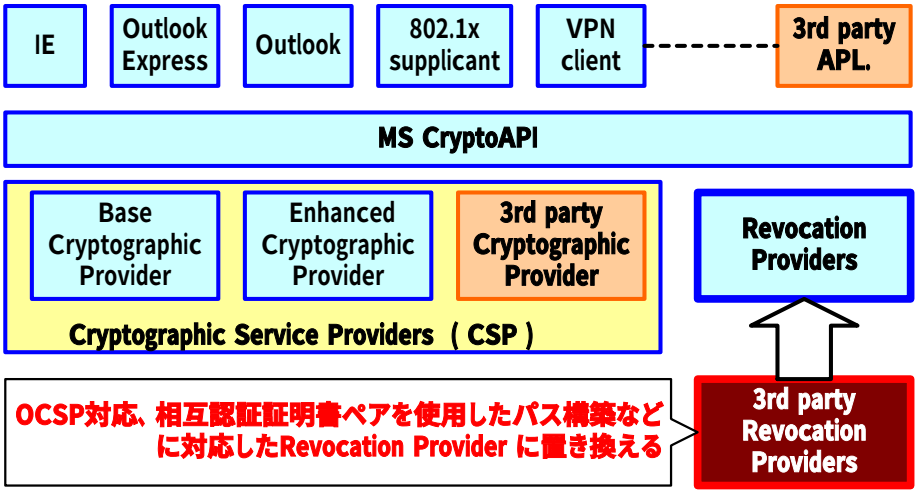
Challenge PKI 2002-プロジェクトの成果物
GPKIテストケース

- テストケース設計の目標
  - ブリッジモデルで要求されるX.509v3証明書拡張に関する証明書拡張を網羅する。
  - GPKI/LGPKI/公的個人認証基盤などのテストクライテリアとなるものを目指している
- 既存のGPKI環境の模擬環境　-　81ケース
  - GPKIブリッジ認証局、商業登記CA、民間認証局、既存の府省認証局などのプロファイルを証明書、CRL/ARLの模擬
- X.509のパス検証　-　130ケース
  - X.509 Path Validation Test Suite, Version 1.07
  - http://csrc.nist.gov/pki/testing/x509paths.html
  - 130ケース
- GPKI相互運用性仕様書から作成 -　45ケース
  - X.509 Path Validation Test Suite, Version 1.07に含まれないオリジナルのテストケース
  - 鍵更新のテストケース、PrintableとUTF8の混在、OCSPとCRLの混在、ポリシマッピングなど

Challenge PKI 2002-プロジェクトの成果物
相互運用テストスィート+テストケース = ＧＰＫＩ模擬環境

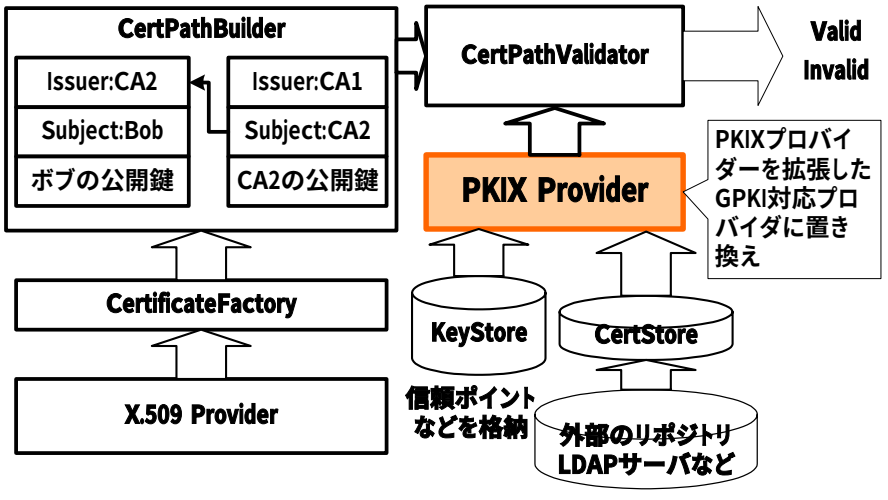


Challenge PKI 2002-プロジェクトの成果物
CryptoAPIによるサンプル実装

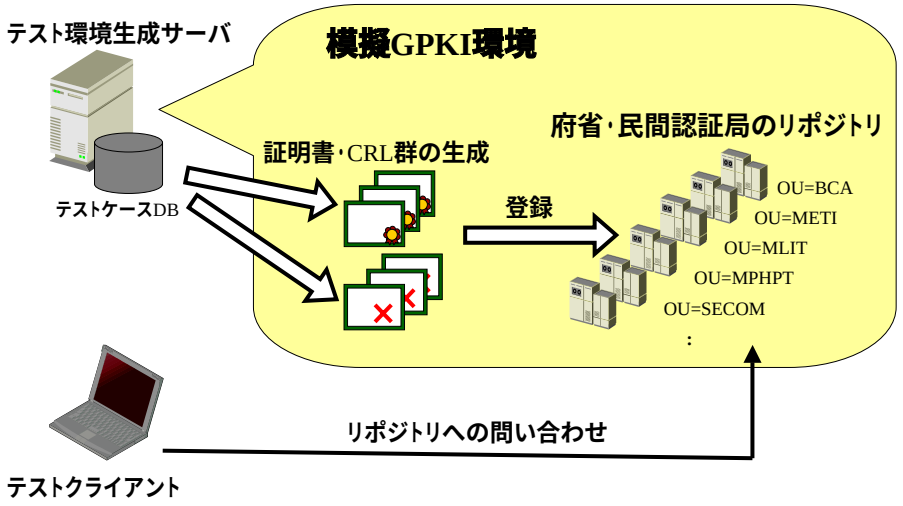


Challenge PKI 2002-プロジェクトの成果物
Javaによるサンプル実装

JDK1.4のCertification Path API を拡張し、OCSPなどに対応



テストの実行環境



テストの実行と結果

- 5つの実装をテスト
  - CryptoAPIとJavaのふたつのサンプル実装と既存の3つの実装をテスト
  - テストの結果は、報告書に記述
- 256のテストケースの実行をデータ生成を含め20分程度で行える

Challenge PKI 2002-プロジェクトの成果物
実装ガイド調査報告書

- 実装ガイド調査報告書
  - IPAのサイトで公開されている
  - 英訳の報告書も作成中（ 近日公開予定 ）
- 認証パス構築・パス検証の標準や仕様の説明
  - X.509 4thEdition、RFC3280、RFC2560などの説明
- 証明書パス構築・パス検証サーバなどの新しいモデルの説明
  - RFC3379(DVD&DVPプロトコル要求)、SCVP(Simple Certificate Validation Protocol)、GPKI証明書検証サーバプロトコルなどの説明
- 証明書パス構築・パス検証のテストクライテリアの動向
  - 世界で行われているChallenge PKI 2002類似プロジェクトの動向
- Javaによる証明書パス構築・パス検証の実装の説明
  - JDK 1.4のCertificate Path Libraryを基にした実装
- CryptoAPIによる証明書パス構築・パス検証の実装の説明
  - Microsoft CryptoAPIに組み込んだ実装

IETF PKIX WGでの発表

- **54th IETF 横浜での発表**
  - **2002年7月**
  - **ChallengePKI2001の成果の発表**
- **55th IETF アトランタでの発表**
  - **2002年11月17日のIETF/PKIX WGにて活動を発表**
  - **昨年度行ったChallenge PKI 2001で明らかになった問題点など報告**
  - **ChallengePKI2002の紹介**
    - **開発するマルチドメインPKIにおけるテストスィートの開発やテストケースの設計等を紹介**
  - **WGの議長であるTim Polk氏からも励まし??のお言葉**
- **56th IETF サンフランシスコでの発表**
  - **2003年3月20日のIETF/PKIX WGにて活動を発表**
  - **今年度行っているChallengePKI2002の成果の発表**
    - **相互運用テストスィート、サンプル実装、テストケース**
  - **開発した相互運用テストスィートのデモ**
- **今後の予定**
  - **テストフレームワークのRFC化**

次の課題

- IETFでのRFC draft の作成
  - マルチドメインPKIの定義
    - プロトコルやデータフォマットの仕様だけでは説明ができない
  - テストフレームワーク＆テストデータベーススキーマ
    - IETFの範疇か??
      - もはや、テストフレームワークがなければ標準化自体が進まない
- 署名者側の相互運用性
  - 本人認証の現状に関する調査報告書
- その他検討中
  - 署名の長期保存、XMLセキュリティ対応、etc….

Challenge PKI 2001&2002の参考

- **電子政府情報セキュリティ相互運用支援技術の開発 (CPKI2002)**
  - **http://www.ipa.go.jp/security/fy14/development/pki/interop.html**
  - **GPKI アプリケーション実装ガイド**
  - **http://www.ipa.go.jp/security/fy14/development/pki/implementation.pdf**
  - **開発：PKI 相互運用テストスィート（2003/5/26現在 準備中）**
  - **開発：GPKI アプリケーション サンプル実装（2003/5/26現在 準備中）**
- **PKI 関連相互運用性に関する調査報告(CPKI2001)**
  - **PKI の相互運用性に関する現状**
  - **http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.html**
  - **http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.pdf**
- **JNSA Network Security Forum 2002でのセミナー Challenge PKI 2001の資料**
  - **http://www.jnsa.org/nsf2002/r_12_b1.html**
  - **http://www.jnsa.org/nsf2002/pdf/B1.pdf**
- **Internet WeekでのJNSAのセミナーChallenge PKI 2002 とマルチドメインPKI**
  - **http://www.jnsa.org/seminar_20021217.html**
  - **http://www.jnsa.org/seminar/active/CPKI2002.pdf**

その他参考

- The report of Challenge PKI in IETF Atlanta
  - http://www.ietf.org/proceedings/02nov/slides/pkix-5.pdf
- Multi Domain PKI Test Suite in IETF San Francisco
  - http://www.ietf.org/proceedings/03mar/slides/pkix-2.pdf
- IPA「本人認証の現状に関する調査報告書」
  - http://www.ipa.go.jp/security/fy14/reports/authentication/index.html
  - PKI、ICカード、バイオメトリクスを中心に、電子政府における本人認証技術の提言を行っている。
- Internet Week 2002 チュートリアルプレゼンテーション
  - PKI～技術概要と利用の実際～
  - 富士ゼロックスの稲田氏と松本が講師を務めたIWのPKIチュートリアル
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/T9-1.pdf
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/T9-2.pdf

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

End