IETFでの活動報告

Challenge PKI プロジェクトとIETFの活動
multi-domain PKIから始まる新WG検討の議論

Challenge PKI プロジェクト
島岡　政基
<shimaoka@secom.ne.jp>

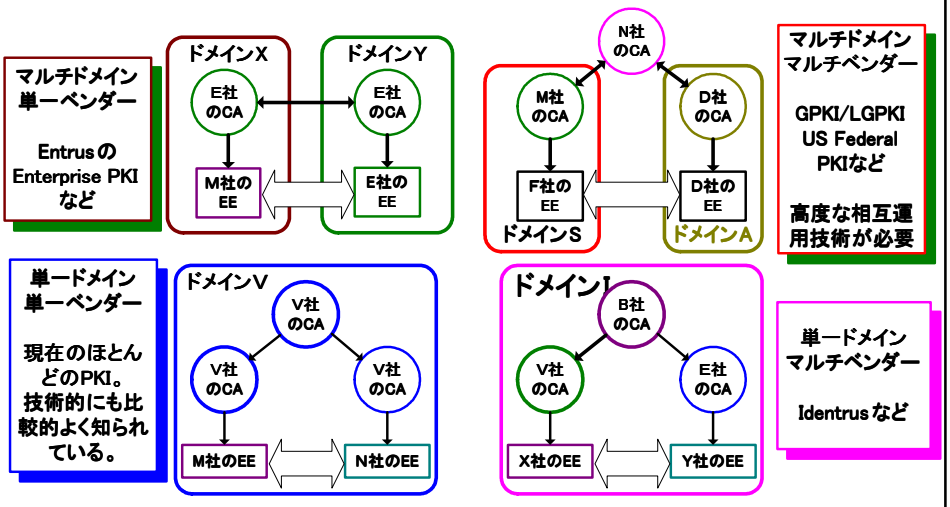
Challenge PKI プロジェクトの概要

Challenge PKI活動概要

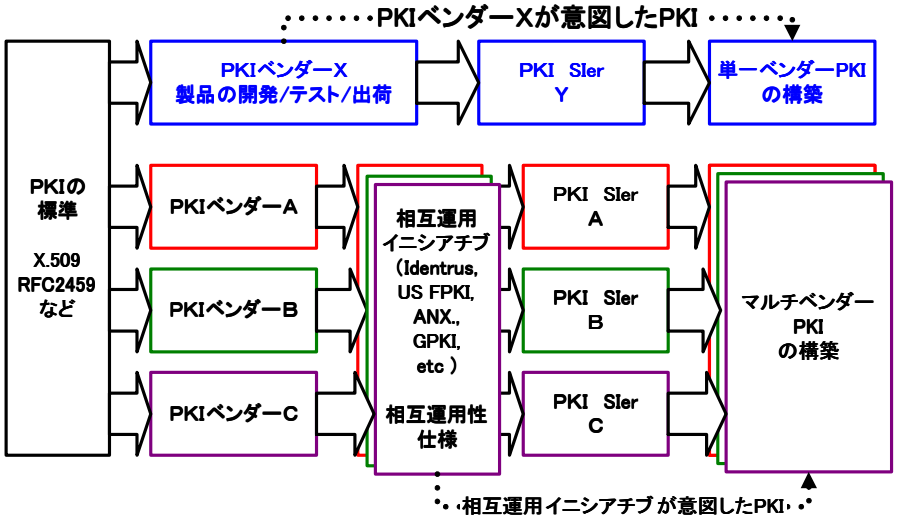
Challenge PKI 2001	- 9つのCAが参加を得て行ったマルチドメイン、マルチベンダーのPKI相互運用実験 - 課題はCA間の相互接続	**マルチドメイン、マルチベンダー環境下でのPKI相互運用フレームワークの確立**
Challenge PKI 2002	- 相互運用テストスィートの開発など - よりPKIアプリケーションよりのPKI相互運用の課題に挑戦 - GPKIのようなマルチドメイン、マルチベンダーのPKI開発を容易にする	
Challenge PKI 2003	- 「セキュリティAPI」「タイムスタンプ」 etc. - RFCの提案	**標準技術の調査、フィードバック**

- 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
- いずれも情報処理振興事業協会（IPA）の委託を受けて実施

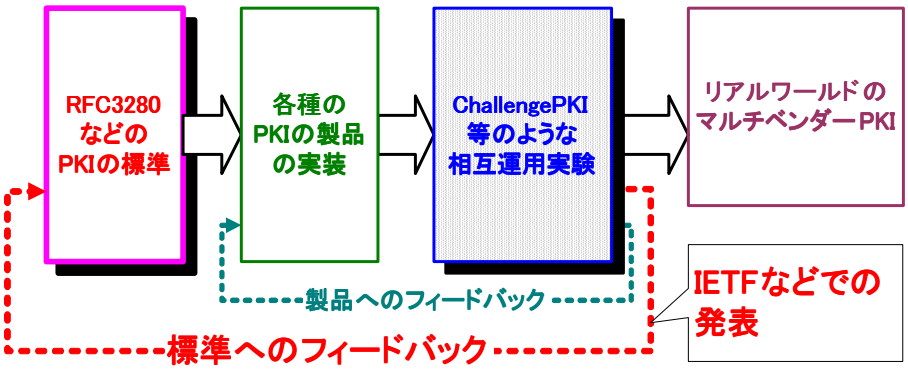
マルチベンダPKI、マルチドメインPKI



相互運用実験の必然性

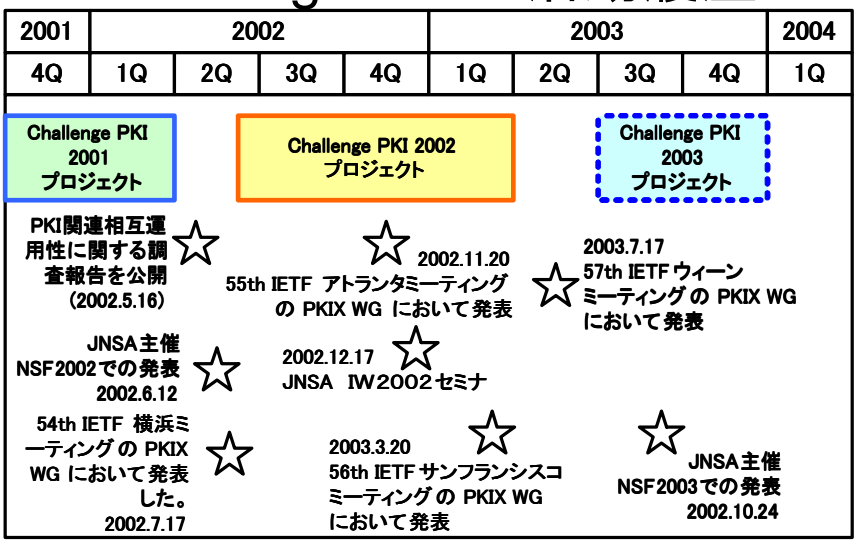


相互運用技術と標準技術との関係



実験を行い、相互運用性の問題点を明らかにすることにより、
実際に利用可能なマルチベンダーPKI、マルチドメインPKIを実現する。

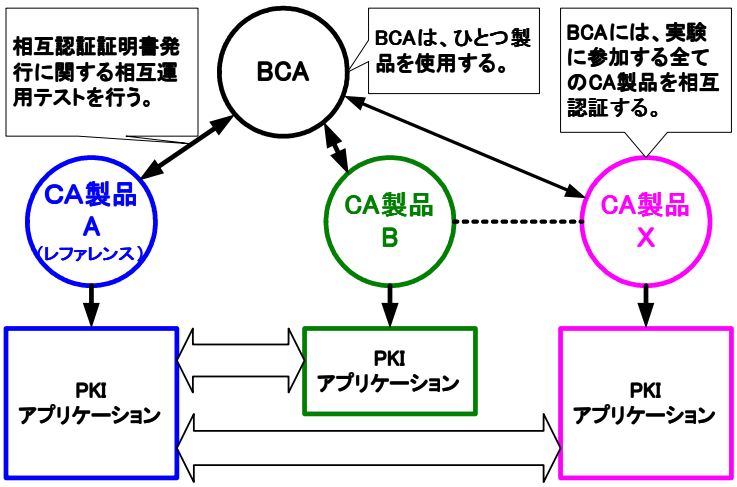
Challenge PKIの活動履歴



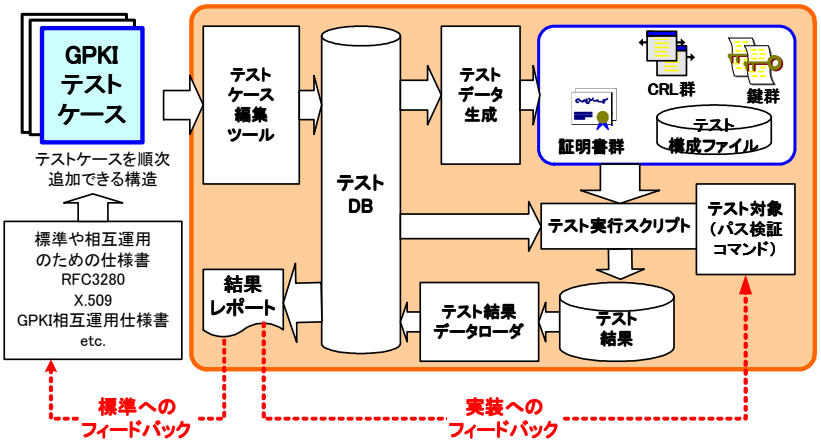
関連するPKI相互運用実験

- 日本(および関係国)
  - GPKI先行3省実証実験 (2001)
    - ブリッジ認証局、先行3省認証局、商業登記認証局により、各認証局間の相互運用性を確認
    - 認証パスの構築・検証等のプリミティブなテスト
    - 業務アプリケーションを用いた連携テスト
  - PKI-J(日本PKIフォーラム)国際間相互接続実証実験 (2001-)
    - 韓国・シンガポール・台北・香港・タイ・日本によるCA間相互認証の実証実験
    - その他証明パス検証ガイドライン、PKCS#11ライブラリ共通インタフェースに関する実証実験
- 海外
  - EEMA pki Challange (2001-2003)
    - EUによるマルチベンダPKI相互運用実験
    - 4つのテストプラン(相互認証、階層CA、証明書発行、証明書検証)
  - NIST PKITS (?～)
    - PKIクライアントPP (Protection Profile)のためのリファレンス
    - 認証パス検証モジュールのためのテストケースとテスト条件を設計

Challenge PKI 2001
ブリッジモデルと参加CAの関係

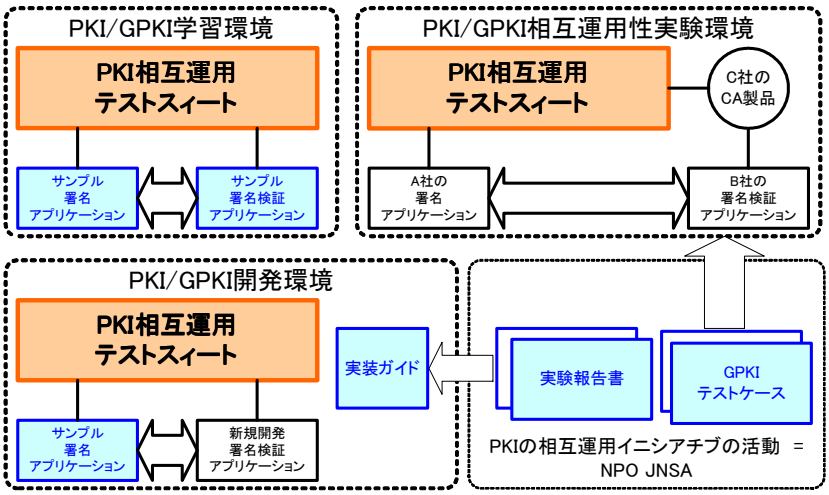


Challenge PKI 2002
相互運用テストスィート



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
相互運用テストスィートの利用イメージ



IETFとの関わり

IETF/PKIXとの関わり

- きっかけ
  - 横浜で開催された54th IETF meeting
  - PKIX WGで活動内容をPR
  - WG後、非公式BoFでマルチドメインPKIに関する問題を提起 → 57thIETF
- その後
  - 以後、55th, 56th, 57th各IETF meetingのPKIX WGで発表
  - 57th@ViennaではmPKI I-Dを提案
  - 59th@Seoulで新WG設立是非について議論

54th IETF@Yokohama

- PKIX WG
  - 初めてChallenge PKIの活動紹介を行った。(富士ゼロックス 稲田氏)
  - http://www.jnsa.org/mpki/ChallengPKI2001-IETF-PKIX.pdf
  - Challenge PKI 2001の成果として、PKIXの仕様だけでは解決できない相互運用性問題があることを報告した。
- 非公式BoF
  - PKIX WGでの発表後、マルチドメインPKIの相互運用性に関する問題提起を行った。(セコムトラストネット 島岡)
  - http://www.jnsa.org/mpki/Interoperability_mPKI.pdf
  - 後のmPKI I-Dは、これをベースとしている。

55th IETF@Atlanta

- PKIX WG
  - Challenge PKI 2002の活動方針説明を行った。(富士ゼロックス 稲田氏)
  - http://www.ietf.org/proceedings/02nov/slides/pkix-5.pdf
  - 2001から得られた知見をもとにPKI相互運用テストスィートを設計
    - 模擬CA、模擬CA
    - 様々なテストケース
    - Java, C++によるクライアントのサンプル実装
  - 今後の開発スケジュールなど

56th IETF@SanFrancisco

- PKIX WG
  - 開発したPKI相互運用テストスィートの解説を行った。(富士ゼロックス 稲田氏)
  - http://www.ipa.go.jp/security/fy14/development/pki/pkix-2.pdf
  - Java, C++によるサンプル実装とCryptoAPIによる相互運用テスト結果の比較
  - テスト結果から標準へのフィードバックの提案
  - デモンストレーション
- その他
  - mPKI I-Dを提案したらPKIX WG DraftとできるかPKIX WGのChairであるTim Polkに口頭で打診。(富士ゼロックス 稲田氏、セコムトラストネット 島岡)
  - 「読まないとわからないが、多分PKIXのScopeには該当するので、WG Draftにできるだろう」との回答。

57th IETF@Vienna

- PKIX WG
  - 初めてmPKI I-Dについて発表を行った。(セコムトラストネット 島岡)
  - http://www.ietf.org/proceedings/03jul/slides/pkix-9/index.html
    - 直前に初版(-00)をリリース。
  - 文書構成、各章の概要、今後の作業などについて説明。
  - WG ChairのTim PolkはじめInternet2のBob Morgan(ワシントン大)や、認証パス構築に関するI-Dの著者の一人であるMatt Cooper(Orion Security)らから支持を受けた。
- その他
  - PKIX WG中で担当ADのRuss Housleyから、PKIX WGはおおよそのミッションを達成したので、現在抱えているI-DをRFC化して終息方向へ向かう、という事実上のクローズ宣言がなされた。

mPKI I-Dの紹介

mPKI I-D(略称)

- Memorandum for multi-domain PKI Interoperability
  - <draft-shimaoka-multidomain-pki-02.txt>
  - 57th IETF/PKIX発表資料
    - http://www.ietf.org/proceedings/03jul/slides/pkix-9/index.html
- 概要
  - マルチドメインPKIの曖昧な点を明確化
  - PKIドメイン間で相互運用性について議論する際の共通認識を持つためのガイドライン
  - 各メンバのから生まれた共通認識
- 経緯
  - 認証パス検証ガイドラインがリファレンス
    - 2002年度PKI-J 国際間相互接続実証実験 成果物
  - Challenge PKIでの知見を盛り込み文書化
- 目的
  - マルチドメインPKIにおける信頼モデル、PKIドメインを定義

I-Dの目的と範囲

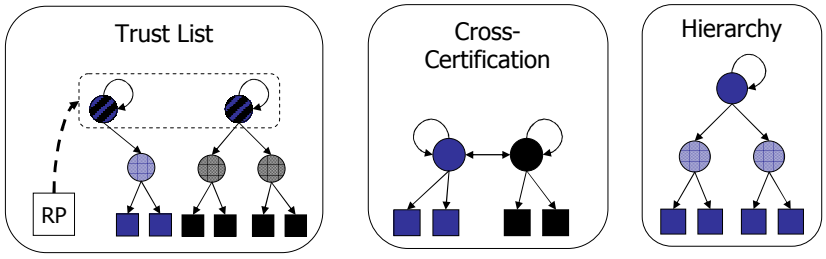
- 目的
  - マルチドメインPKIの相互運用を実現する
    - 現状では「標準」が存在しない
  - 不正な信頼モデルを抑止する
    - 相互運用性のないPKIと相互接続しない
- 範囲
  - PKIドメインの認証基準を確立する
    - CA-CA間の信頼関係
    - マルチドメインPKIにおける信頼モデル
  - 標準ではなく、Best Current Practiceを目指す。

文書構成

1. イントロダクション
2. 語句の定義
3. (CA-CA間の)信頼関係
4. PKIドメイン(の定義)
5. シングルドメインPKI
   - PKIドメインのモデル定義
6. マルチドメインPKI
   - マルチトラストポイントモデル
   - シングルトラストポイントモデル
7. セキュリティ考察
8. 参考文献

3章 (CA-CA間の)信頼関係

- 個々のCA-CA間(peer)の関係を定義

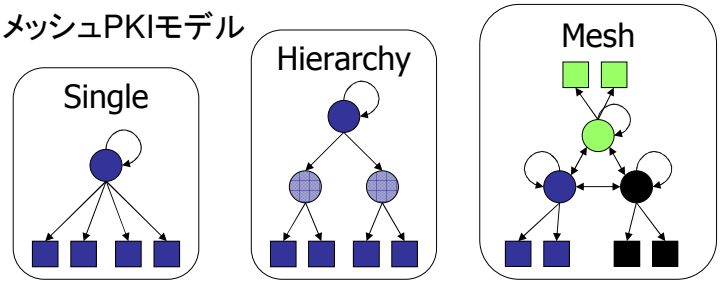


4章 PKIドメインの定義

- 信頼の範囲を示すPKIドメインを定義
  - 同じ証明書ポリシを共有できる範囲
- 相互運用性のないPKIドメインの問題
- PKIドメインの相互運用要件

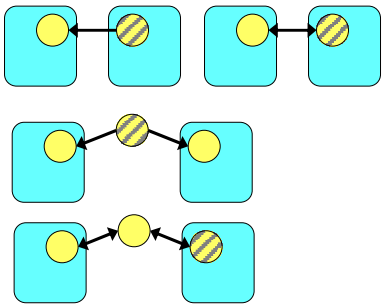
5章 シングルドメインPKI

- シングルドメインを形成する典型的なPKIモデルを定義
  - シングルPKIモデル
  - 階層PKIモデル
  - メッシュPKIモデル



6章 マルチドメインPKI

- マルチトラストポイントモデル
  - トラストリストモデル
- シングルトラストポイントモデル
  - ピアツーピアモデル
    - 片方向相互認証
    - 双方向相互認証
  - ユニファイドドメインモデル
  - ブリッジモデル

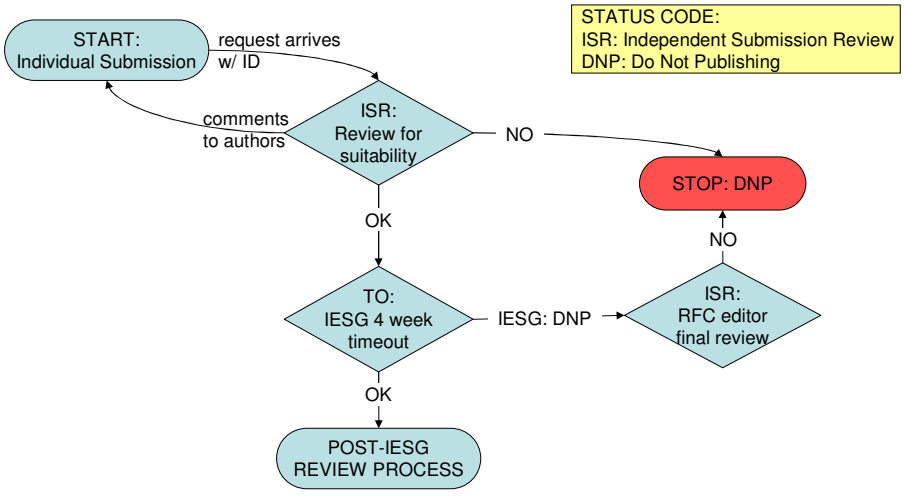


新WG検討の議論

新WGの検討@59th Seoul

- Before 59th IETF@Seoul
  - mPKI I-D 第3版(-02)をリリース
  - PKIX WGへエキスパートレビュを依頼
    - WG Chair他数名から、PKIXとはScopeが異なる(広すぎる)ので別WGを新設して検討すべきでは、とのコメント。
    - D.Pinkas, P.Hesseら実質的なWG主要メンバからのコメントがいくつか寄せられた。
- At 59th IETF@Seoul
  - WG新設のニーズ、可能性等についてAD/WG Chairらと検討

RFC Editor Process (RFC 2026)



WG新設プロセス (RFC 2418)

- WG新設要件
  - ADの承認
  - 明確なゴールとマイルストーン →WG憲章
  - 少なくとも4,5人のアクティブメンバと1,2ダースのML参加者
  - 必要に応じて新設前にBoFを開催
  - 決定すべきアイテム
    - WG名 (8文字以内)、概要
    - WG Chair (2名以内)と担当AD
    - オープンなメーリングリストとアーカイブ
    - WG憲章
    - ゴールとマイルストーン
- BoF (Birds of A Feather)
  - 目的
    - WGゴールの明確化、WG憲章の作成
    - WG新設可能性の確認
  - AD(Area Director)承認が必要
  - 原則として1回。
    - 2回目の開催は極めて例外的(要AD承認)
    - 3回目はない。

新WGの検討

- WGの目的と範囲
  - PKIの相互運用性維持が大きなテーマ
    - 相互運用なので、範囲を明確化することが難しい
  - 範囲を議論すべきBoFで、議論が発散する可能性がある
    - BoFの開催回数には制限がある。
- WGメンバの確保
  - 興味を持っている人間がどの程度いるか?
  - アクティブメンバのリクルート
- WG運営上の課題
  - 既存PKIとの整合性、関連WGとの連携
  - National PKI等に対する政治的な調整

Power Dinner @ 59thSeoul (1)

- 参加メンバ
  - Area Director: Russ Housley, Steve Bellovin
  - WG Chair: Stephen Kent
  - Observer: Jim Schaad
  - JNSA/IPA: 宮川(IPA)、安田(JNSA)、松本(セコム)、稲田(富士ゼロックス)、島岡(セコムトラストネット)


Power Dinner @ 59thSeoul (2)

- 議題
  1. WG新設のニーズ
  2. 新WG運営のフィージビリティ
  3. mPKI I-DのRFC化
- 結論
  1. 新WG運営には非技術面での問題解決も不可欠
     - ことPKIは国によっては政策的側面もあるため、エンジニアだけでは調整が困難。
  2. WG設立を望む同志がいれば協力は可能。
  3. IESGレビュの前にPKIX以外の関連WG(S/MIME, TLS, pki4ipsecなど)のエキスパートレビュも不可欠

今後の作業

- I-Dの改訂
  - 第4版(-03)のリリース
  - 当初より作業が遅れているが、5/中を目標に。
- 関係WGへのアナウンス
  - smime WG, pki4ipsec WGなど
  - 議論、レビュへの参加の呼びかけ
- mPKIサイトを公開、誘導
  - 議論用のMLを立ち上げ
  - MLアーカイブの公開 (ドキュメントステータスのオープン)
  - 関連資料の公開 (一部公開済)
- Co-authorのリクルート
  - 視点を偏らせないために不可欠。
  - 識者へのアピールという点からもNISTなど権威ある機関のメンバが好ましい。
- 60th@SanDiegoで非公式BoF
  - 識者を獲得しやすい環境でオフラインレビュを実施
  - 事前のアナウンスの仕方が重要

関連資料

- Challenge PKI project ホームページ
  - http://www.jnsa.org/mpki/
  - http://www.jnsa.org/mpki/index_j.html
- 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
- 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
  - 開発: GPKI アプリケーション サンプル実装
- 2003年度 情報セキュリティ関連の調査 (CPKI2003)
  - セキュリティAPIに関する技術調査 (サンプルコードあり)
  - http://www.ipa.go.jp/security/fy15/reports/sec_api/index.html
  - タイムスタンプ・プロトコルに関する技術調査
  - http://www.ipa.go.jp/security/fy15/reports/tsp/index.html

セミナ資料

- JNSA NSF(Network Security Forum) 2002
  - 「PKI相互運用実験　Challenge PKI 2001」
  - http://www.jnsa.org/nsf2002/r_12_b1.html
  - http://www.jnsa.org/nsf2002/pdf/B1.pdf
- JNSA NSF 2003 Spring
  - 「PKIアプリケーションの相互運用を促進するChallenge PKI 2002」
  - http://www.jnsa.org/nsf2003spring/pdf/b4.pdf
  - 「IETFでのPKI関連技術動向」
  - http://www.jnsa.org/nsf2003spring/pdf/b5.pdf
- INTAP インターネット技術シンポジウム 2002
  - http://www.net.intap.or.jp/INTAP/information/2002/its2002/material/09.pdf
  - PKIの相互運用実験 Challenge PKI2001とIETF/PKIX