JNSA NPO 日本ネットワークセキュリティ協会

Challenge PKI プロジェクトと 公的個人認証サービス

セコム株式会社IS研究所
松本　泰

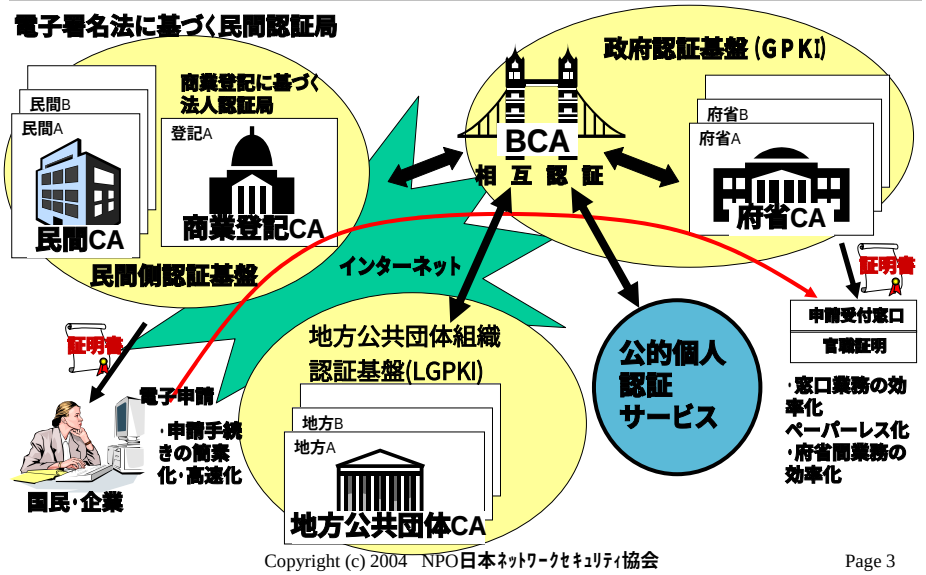
2004 年 4月 27日

Challenge PKI プロジェクトと 公的個人認証サービス

JNSA

- 公的個人認証サービスの技術の概要
  - GPKI,LGPKI,民間認証局も含めてマルチドメインPKIの実装例のひとつ…
  - #JNSA Pressの記事, JESAPの資料….
- GPKI/JPKIに関連した標準化と実装
  - 広い認証ドメインで、ある保証レベルの信頼を確立することは、ありとあらゆる業界で求められている….
- Challenge PKI プロジェクトの展開
  - 何をしようとしているか…..

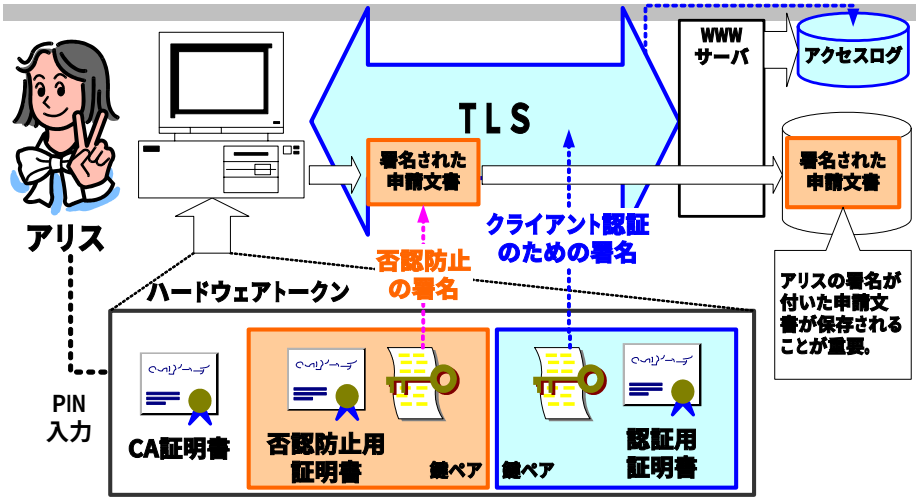
公的個人認証サービスの概要



公的個人認証サービスの概要

- 公的個人認証サービス
  - 自治体が**市民**に配布する証明書
  - 耐タンパ性のあるICカード（住基カードなど）に証明書の鍵を格納
  - 基本的には、**否認防止の署名用**の証明書
- 2002年12月 「電子署名に係る地方公共団体の認証業務に関する法律（公的個人認証法）」2002年12月
- 2003年8月25日 住基カードを配布開始
- 2004年1月29より公的個人認証サービス証明書発行開始
- 2004年2月 東海4県の電子申告の名古屋国税局管内で2004年2月から実施
- 2004年3月下旬 電子パスポート申請
  - 岡山県で開始

認証と否認防止の署名の違い



電子政府などでは、文書に署名され、署名された文書が保存されることが重要。JPKIの証明書は、否認防止の署名用の証明書のみ

公的個人認証サービスと住基カード

- 住基カード
  - 公的個人認証サービスを、ひとつのアプリケーションとして格納することができる。
- 住基カード上の公的個人認証サービスアプリケーションの機能
  - 秘密鍵（私有鍵）のローディン
    - 鍵ペア生成装置で作成した秘密鍵を住基カード上の公的個人認証サービスアプリケーション領域にローディングする。
    - 秘密鍵は、取り出せなくする。
  - 秘密鍵（私有鍵）による署名
  - ユーザ証明書と都道府県CAの自己署名証明書の格納と取り出し。
    - 証明書ユーザの信頼点として「都道府県CAの自己署名証明書」が入るのは非常に重要

公的個人認証サービスの証明書取得

- 住基カードの提出
  - #将来的には住基カード以外もサポートされる可能性がある..
  - 住基カードに「公的個人認証サービスのアプリケーション」をインストール
- 鍵ペアーの生成とローディング
  - 鍵ペア生成装置による鍵ペアの生成と住基カードへのローディング
  - 鍵ペア生成装置は、スタンドアローン
    - 生成された鍵は破棄されているはず….
- 証明書の発行
  - 公開鍵に対して都道府県認証局が署名を行い公的個人認証サービスの証明書が発行される

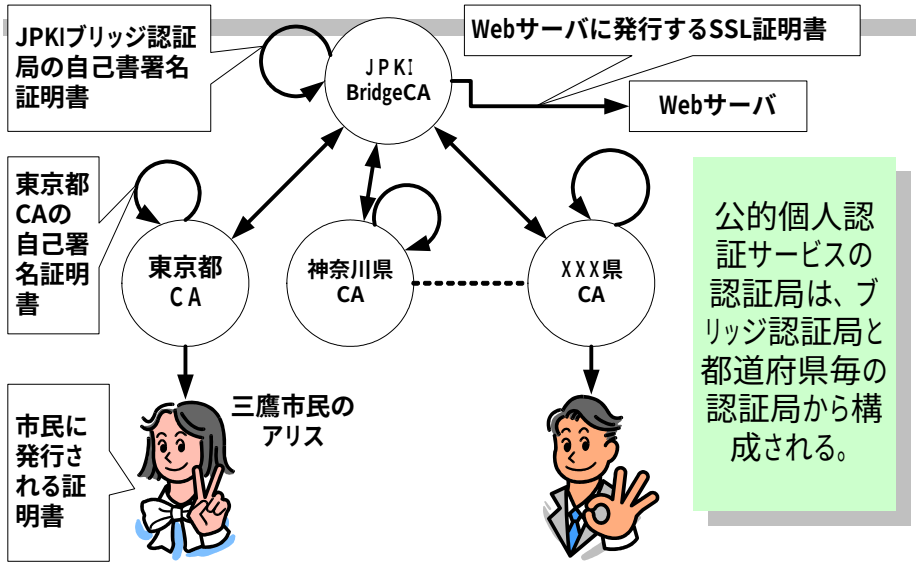
公的個人認証サービスの参考

- 公的個人認証サービスポータルサイト
  - http://www.jpki.go.jp/
- 書籍
  - 公的個人認証サービスのすべて
  - その制度とシステムの全貌
  - ISBN:4324071195
  - 猿渡知之・村松茂
  - ぎょうせい 2003/09出版
  - 21cm 292p
  - [A5 判] NDC分類:317.6 販売価:\2,857(税別)

JPKIの認証局

- 都道府県認証局
  - 市民に証明書を発行する認証局
  - 自己署名証明書を持った独立した認証局となっている
  - JPKIのブリッジ認証局へCA証明書（相互認証証明書）を発行して相互認証を行っている。
- JPKIのブリッジ認証局
  - 通常、ブリッジ認証局は、ユーザの信頼点にはならない（いわゆるroot CAにはならない）。JPKIでは、Webアプリケーションの信頼点となっておりWebサーバへの証明書を発行している。
  - 都道府県認証局へCA証明書（相互認証証明書）を発行して相互認証を行っている。
  - GPKIブリッジ認証局と相互認証を行っている。

JPKIの認証局



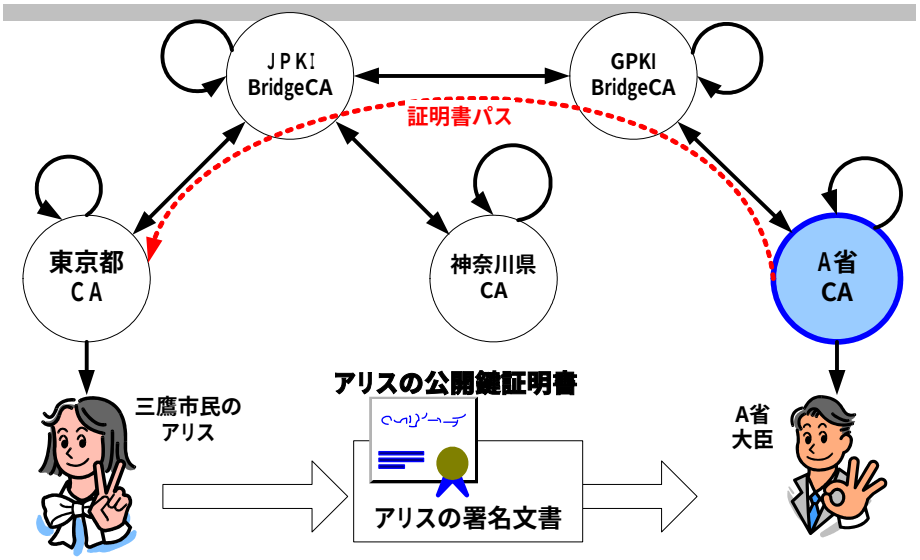
ＪＰＫＩの発行する証明書

証明書の種類	発行認証局	内容
BCA自己署名証明書	JPKI BCA	Webサーバなどの信頼点
相互認証証明書	JPKI BCA	都道府県CAへ発行。JPKIリポジトリに公開される。
相互認証証明書 (GPKI)	JPKI BCA	ＧＰＫＩのBCAへ発行
Webサーバ証明書	JPKI BCA	JPKIドメイン内のWebサーバ
コードサイニング証明書	JPKI BCA	アプレットなどへの証明書
都道府県自己署名証明書	都道府県CA	市民の信頼点。JPKIのICカードに格納される。
相互認証証明書	都道府県CA	JPKI BCAへ発行。JPKIリポジトリに公開される。
OCSPサーバ証明書	都道府県CA	JPKI外から証明書の失効を検証
証明書検証サーバ証明書	都道府県CA	市民が官職の証明書を検証
市民向け証明書	都道府県CA	個人の証明書。JPKIのICカードに格納される。

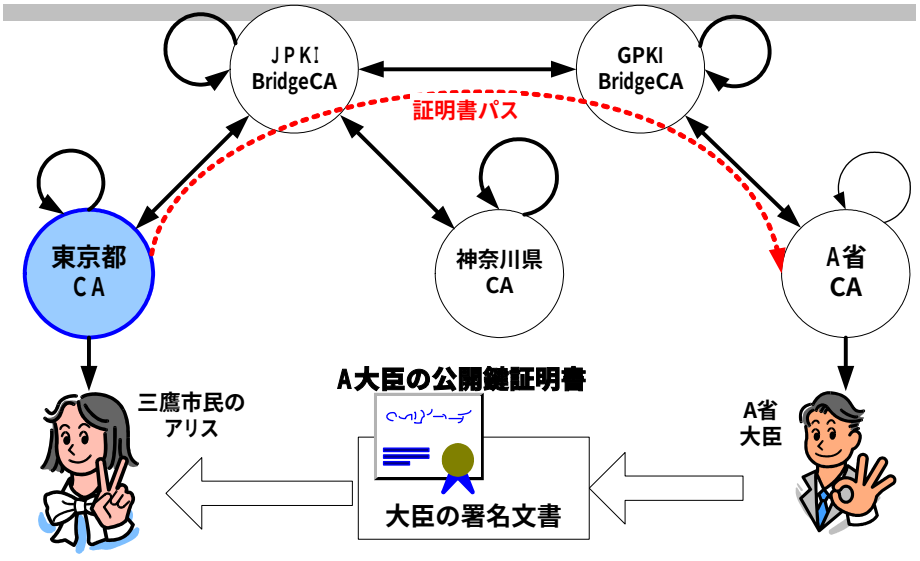
東京都CAから発行されるEE証明書

発行者	OU = the Governor of Tokyo-to　省略
有効期限	2004年1月30日 13:30:29 - **2007年1月29日 23:59:59**
サブジェクト	CN = 2004013xxxxxxxx　#発行年月日+?? L = Mitaka-shi L = Tokyo-to C = JP
サブジェクトの別名	#基本４情報が入る..
証明書ポリシ	[1]Certificate Policy: Policy Identifier=1.2.392.200149.8.5.1.1.**10** 省略
鍵使用方法	Digital Signature, **Non-Repudiation (c0)**
鍵長	**RSA 1024 bit**

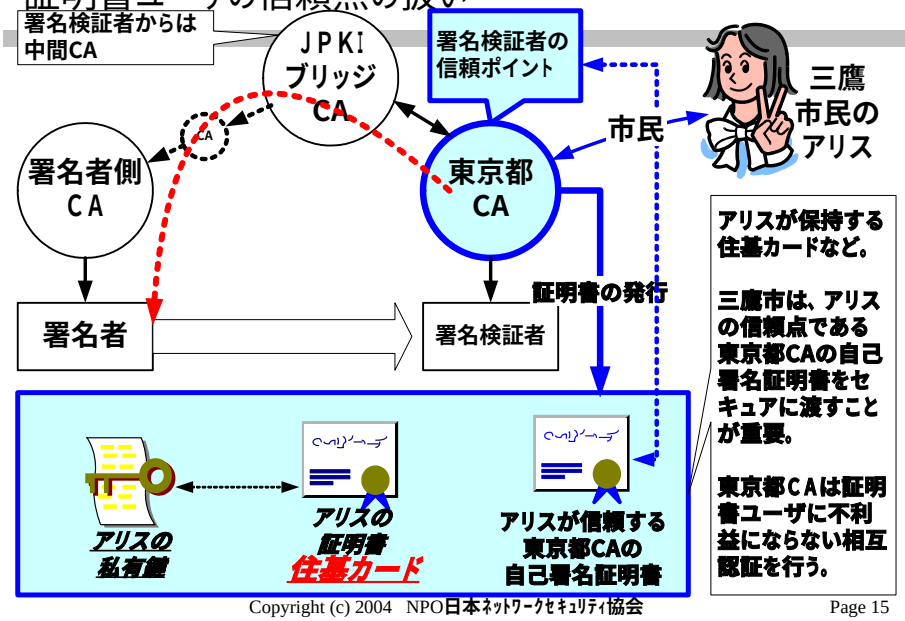
JPKIとGPKI　市民の申請文書の検証



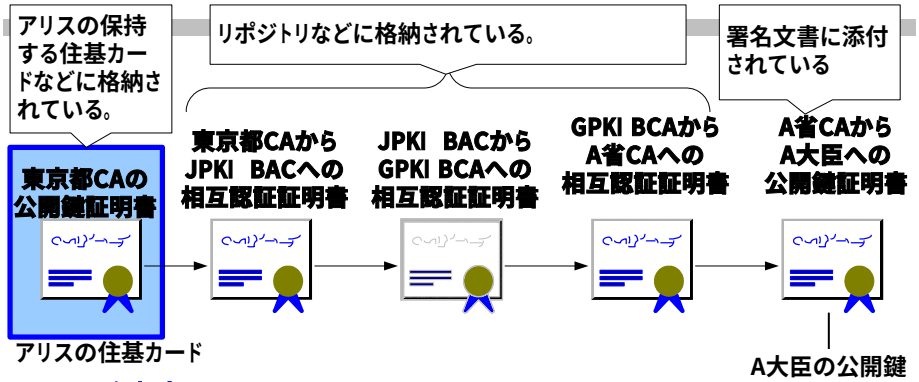
JPKIとGPKI　官職の申請文書の検証



JPKIの信頼点と証明書パス
証明書ユーザの信頼点の扱い



JPKIとGPKI　官職の申請文書の検証　その2



アリスの**信頼点**である東京都CAの公開鍵は、アリスに発行された公開鍵証明書や秘密鍵（私有鍵）と共に住基カードの公的個人認証サービス領域に格納される。
アリスは、この信頼点のみを信頼し証明書パスを検証し、次に、署名文書を検証する。JPKIの場合、（官職）証明書検証サーバが用意されており、実際の証明書検証はこのサーバで行うことができる。しかしこのサーバの応答の署名の検証は行う必要がある。

色々な証明書パス

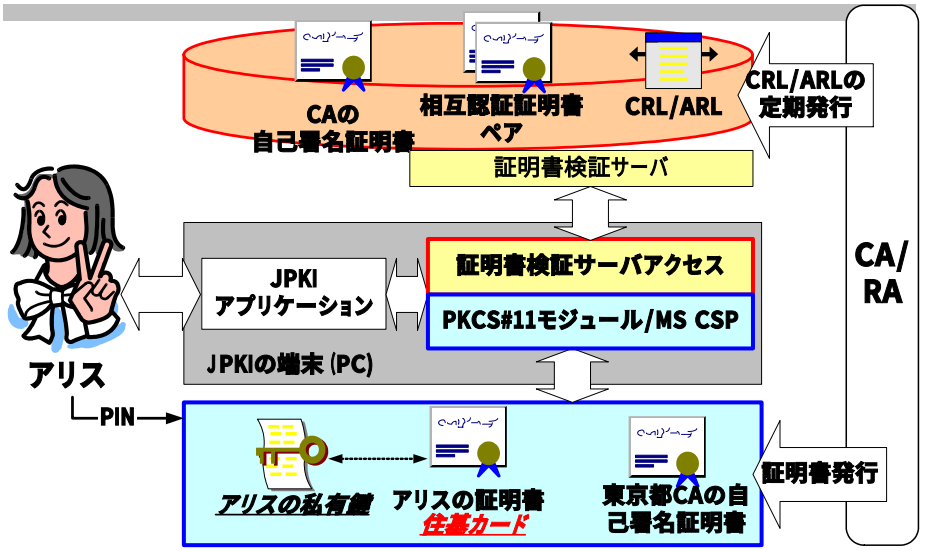
東京都CAからEE証明書の証明書パス

「the Governor of Tokyo-to」は、東京都CAの自己署名証明書

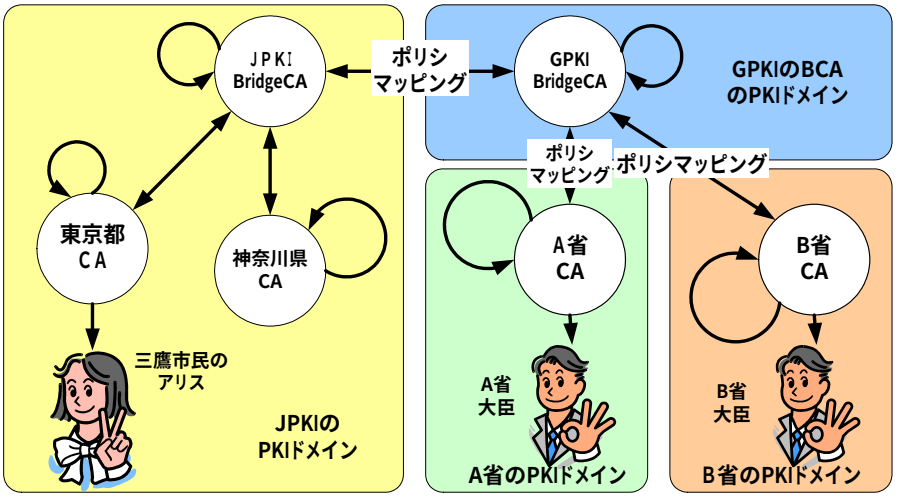
神奈川県CAの自己署名証明書から東京都のEE証明書までの証明書パス。

こうしたC2Cは、公的個人認証サービスではサポートされない

JPKIアプリケーション環境



JPKIのPKIドメイン
JPKIとGPKIのPKIドメイン

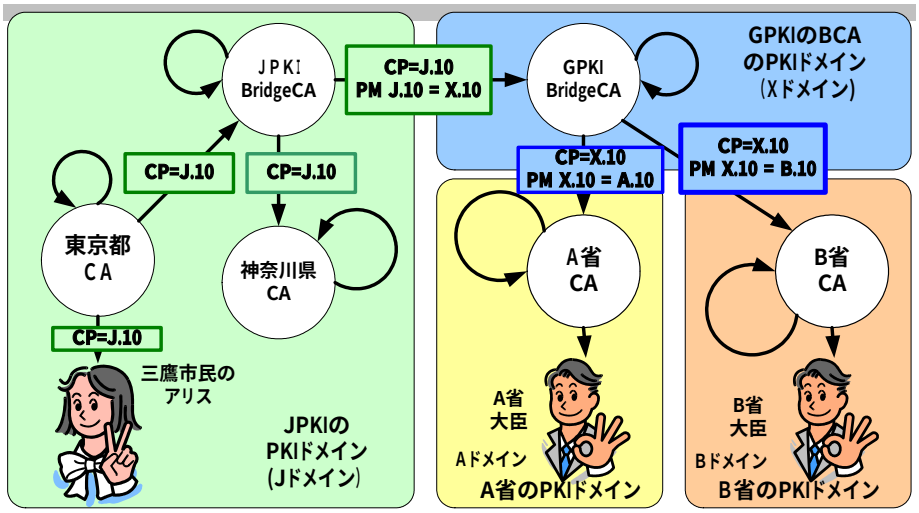


JPKIの証明書ポリシ

証明書の種類	発行認証局	FL	証明書ポリシ OID
相互認証証明書	JPKI BCA	C	1.2.392.200149.8.5.1.1.10
Webサーバ証明書	JPKI BCA		1.2.392.200149.8.5.1.100
コードサイニング証明書	JPKI BCA		1.2.392.200149.8.5.1.400
相互認証証明書	都道府県CA	C	1.2.392.200149.8.5.1.1.10
OCSPサーバ証明書	都道府県CA		1.2.392.200149.8.5.1.300
証明書検証サーバ証明書	都道府県CA		1.2.392.200149.8.5.1.200
市民向け証明書	都道府県CA	C	1.2.392.200149.8.5.1.1.10
相互認証証明書	GPKI BCA	C	0.2.440.100145.8.1.1.1.10
官職証明書	外務省CA	C	1.2.392.100350.8.5.1.1.10
官職証明書	経済産業CA	C	1.2.392.100595.8.5.1.1.10

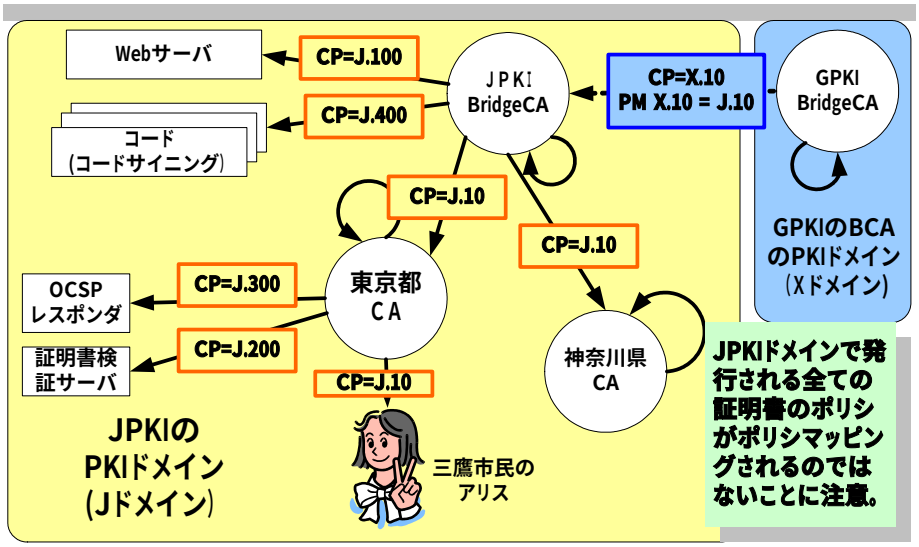
FLは、クリチカルフラグ。「C」はクリチカル。

JPKIのPKIドメイン
証明書ポリシとポリシマッピング



アリスの信頼点である東京都CAからの証明書パスにおける証明書ポリシとポリシマッピング

JPKIのPKIドメイン
証明書ポリシとポリシマッピング



GPKI/JPKIに関連した標準化と実装

- GPKI,JPKIは、マルチドメインＰＫＩ
  - 基本的には、X.509, RC3280から逸脱していない
    - しかし、それだけで相互運用が可能、また、広い展開ができるわけではない
  - マルチドメインＰＫＩの実装は、多くの標準や、現状の実装、これらを把握し、適切な選択を行なう必要がある
  - 適切なプロファイルと足りない部分の標準化
- マルチドメインPKIの困難さ
  - 全ての認証技術はボトムアップ…
  - PKIが難しいのではなく、マルチドメインであることが難しい…
    - ビジネススキーム、地域を越えた法制度、各種のクライテリアの策定状況、現状の実装を踏まえた上での技術を確立することが大変…
  - 広いドメインにおいて、幅広い応用を考えるとき、多くの標準、多くの実装がある中で、何がベストプラクティスであるか判断するのは非常に困難
    - マルチドメイン = マルチポリシ、マルチアーキテクチャ（orハイブリッド）
    - ベストプラクティス。
      - 「日本発の標準」といった派手さがないこともあり重要さが理解されていない面がある….

GPKI/JPKIに関連した標準化と実装

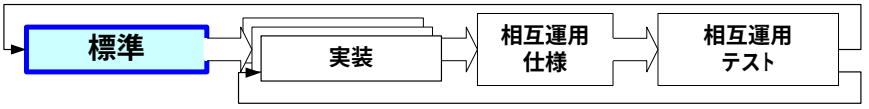
- 大規模なPKIは、世界的に見ても事例は少ない、広く信頼を確立するには、まだ、色々な努力が必要
  - 同じような動きは、北米、ＥＵにある
    - 放っておくと似て非なる相互運用性のないものを作ってしまう..
  - 今後、更に広いドメインでの信頼の確立が必要
    - アジアの中での連携。欧米との連携。業界を超えた連携
- マルチドメインモデルでの色々な業種、応用分野での基盤の確立
  - Webサービスを利用したSSO(SAMLなど)、グリッドコンピューティング、EDI(ebXML)、これらを、ビジネスに展開するためには、本質的に、保証レベルのある信頼関係を必要としている
  - マルチドメインの信頼が確立できないと、上記の技術は、プロトタイプ、実証実験の域を脱することはできない…

Challenge PKI プロジェクトの展開
Challenge PKI プロジェクトの活動

- 標準化活動への参加
  - IETFでの活動
    - 標準自体へのフィードバック
  - 標準・仕様作成と相互運用仕様作成は同時進行であるべき
- PKI相互運用イニシアチブの活動
  - アイディアから仕様へ -> 多くの研究者が行っている
  - 仕様から標準、標準から実装 -> 学術系＆ベンダーなど
  - 標準・実装から展開（相互運用） -> 誰が担うか
    - 標準と呼ばれる文書は山のようにある。しかし相互運用可能なものは極わずか…．これを解決して行かなければならない。
  - 海外との連携
- セキュリティフレームワークやミドルウェア重要性
  - 実際のアプリケーションにおいて、セキュリティ・ミドルウェアが、実行時のネットワーク上の信頼と複雑な相互運用の問題を吸収する

Challenge PKI プロジェクトの展開
標準化から実装、そして相互運用

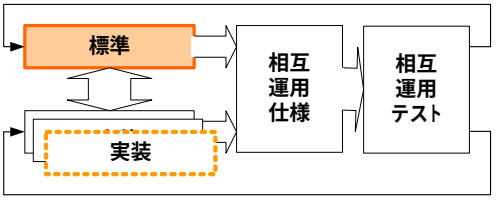
•ISO／IEC、ITUなどの標準化から実装、相互運用



•実装を伴わない現実味のない標準ができる可能性

•長い標準化期間、そして、長いターンアラウンド

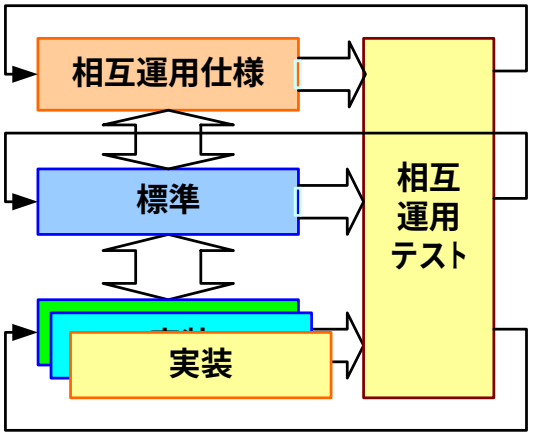
•IETFの標準化から実装、相互運用



IETFの標準化の基本コンセプトは、ラフコンセンサス アンド ランニングコード

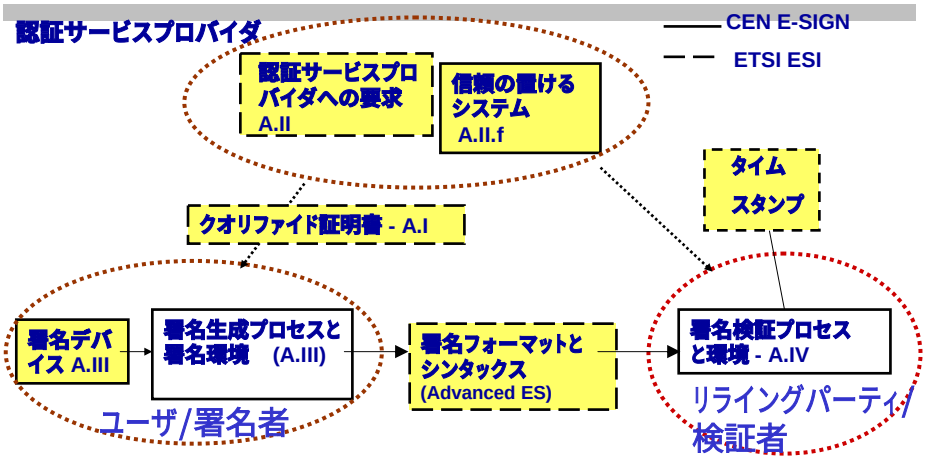
複雑なセキュリティプロトコルに対していい加減な実装が蔓延してしまう…．

Challenge PKI プロジェクトの展開
標準化から実装、そして相互運用の統合



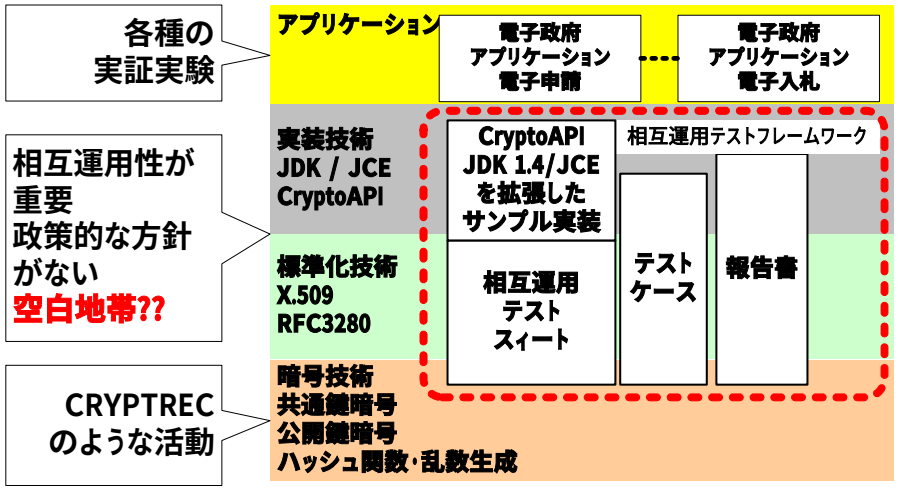
- 標準の作成と相互運用仕様の作成を同時に行う。
- 相互運用テスト（準拠性テスト）を早期に行う
- 相互運用テストスィートなどの開発も考慮する

Challenge PKI プロジェクトの展開
EESSIの認証フレームワーク

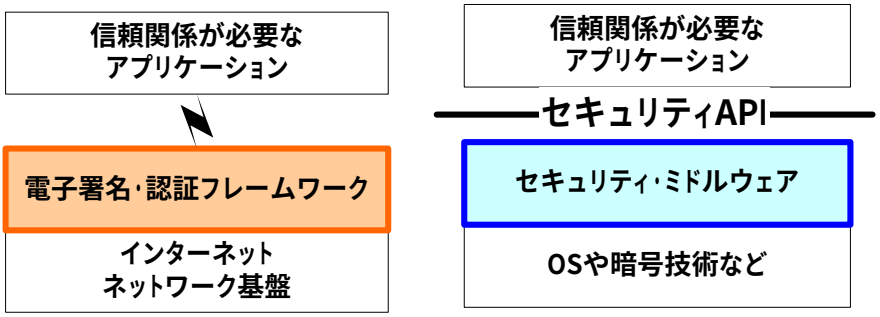


現状の日本の電子政府の認証フレームワークでは、ユーザ/署名者、リライングパーティ/検証者などに対する仕様、ガイドライン、クライテリアなどが決定的に不足している。

Challenge PKI プロジェクトの展開

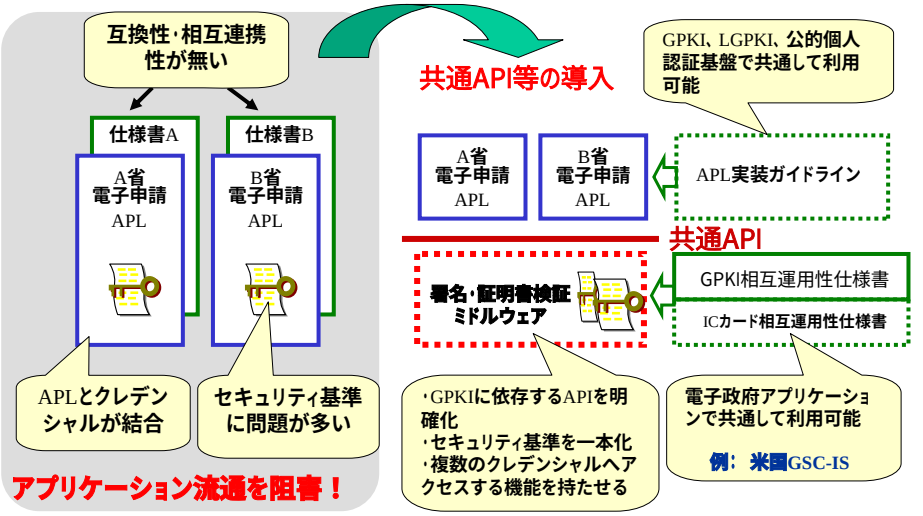


Challenge PKI プロジェクトの展開
セキュリティフレームワークやミドルウェア重要性



実際のアプリケーションにおいて、セキュリティ・ミドルウェアが、実行時のネットワーク上の信頼と複雑な相互運用の問題を吸収する

Challenge PKI プロジェクトの展開
セキュリティフレームワークやミドルウェア重要性



Challenge PKI プロジェクトの展開
Challenge PKI プロジェクトの今後の案

- Memorandum for multi-domain PKI InteroperabilityのRFC化
  - BCP ベストカレントプラクティスの確立に力を注ぐ
- Son of RFC 3280のテストケースの設計
  - UTF8Stringの扱いなど….
- 公的個人認証サービスも含めた電子政府全体のテスト環境
  - テストケースも含め配布できる形態で提供
  - テストサイトの立ち上げ
- デジタルタイムスタンプなどPKIをベースとしてプロトコル類のテストスィートへ
  - #近日中にタイムスタンプのテストサイトを公開予定….
- 米国、EU、アジアでのPKIテストスィート、及び、テストケースの共有
  - 日、韓、台湾の国際相互認証実験などでも利用している…

おしまい