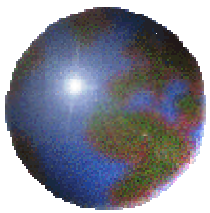
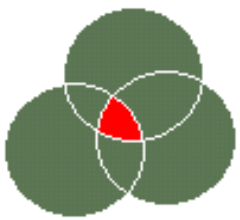


日本発の
PKI国際標準を目指して



Challenge PKI Project

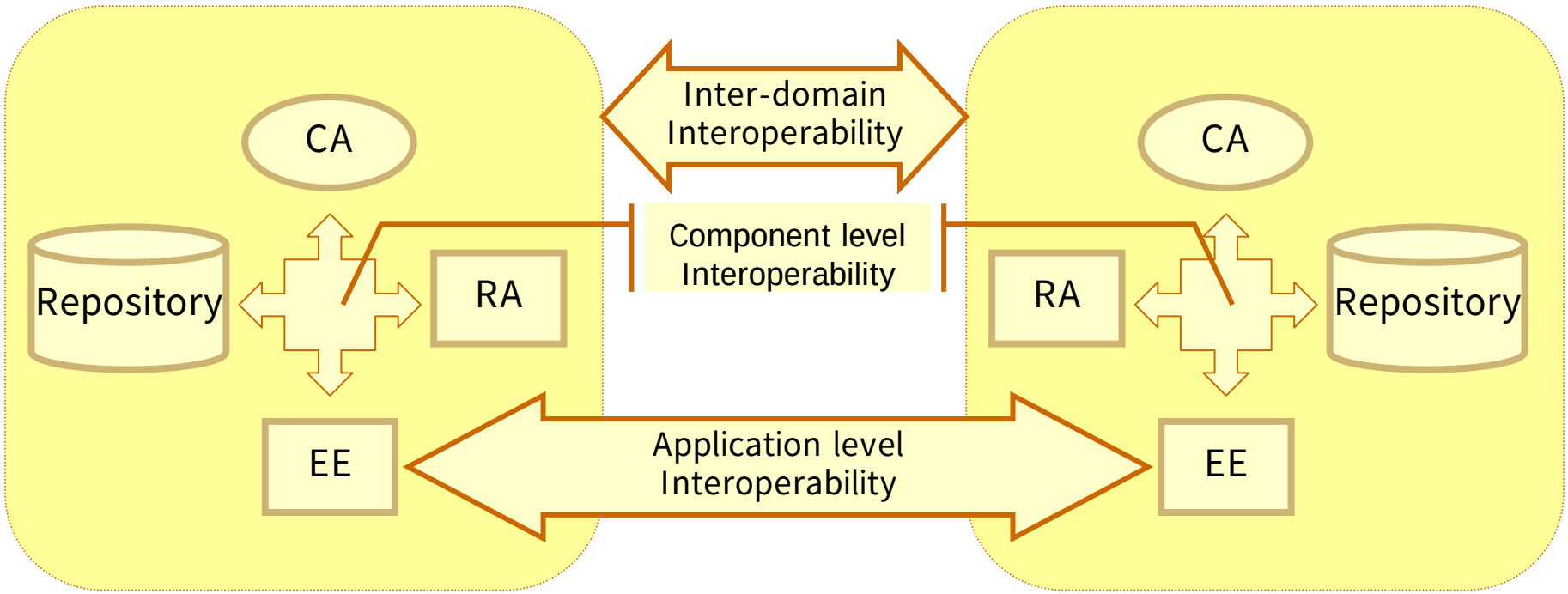
The Multidomain PKI Interoperability Framework

セコム IS研究所
島岡　政基
<m-shimaoka@secom.co.jp>

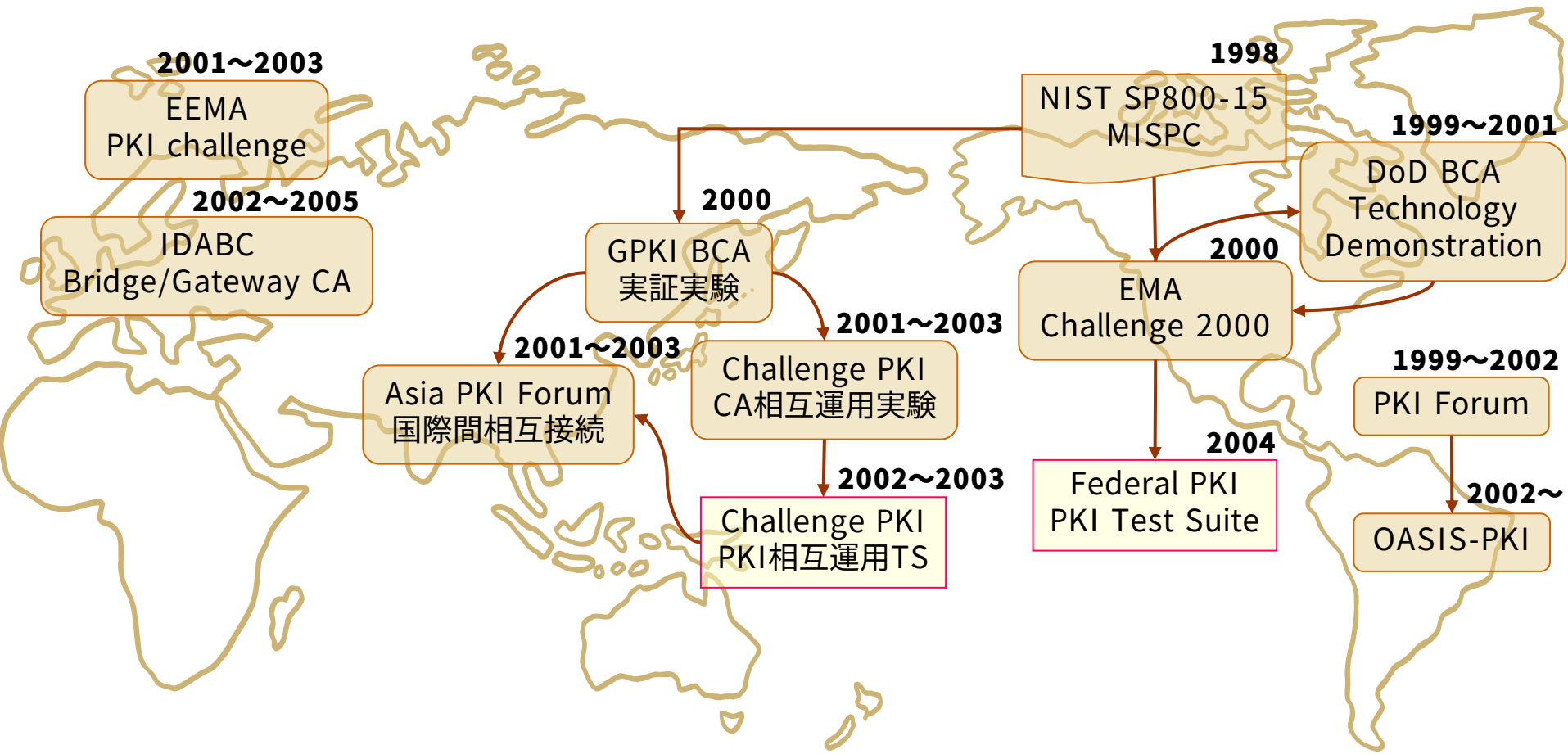
PKIの相互運用って何?

- NIST: SP800-15 MISPC (1998)
  - “Minimal Interoperability Specification for PKI Component”
  - Component Specifications
    - CA, ORA, 証明書所有者, クライアント
  - Data Formats
    - Certificate, CRL, パス検証、メッセージフォーマット、通信プロトコル
- GPKI:相互運用性仕様書(2001)
  - PKIコンポーネント仕様
  - アプリケーション間相互運用性
  - 異なるPKIドメイン間の相互運用性
  - PKIドメイン内仕様
  - 証明書検証サーバの利用
  - プロファイル
- PKI Forum: PKI Interoperability Framework(2001)
  - コンポーネントレベル相互運用性
  - アプリケーションレベル相互運用性
  - ドメイン間相互運用性

3つの相互運用性

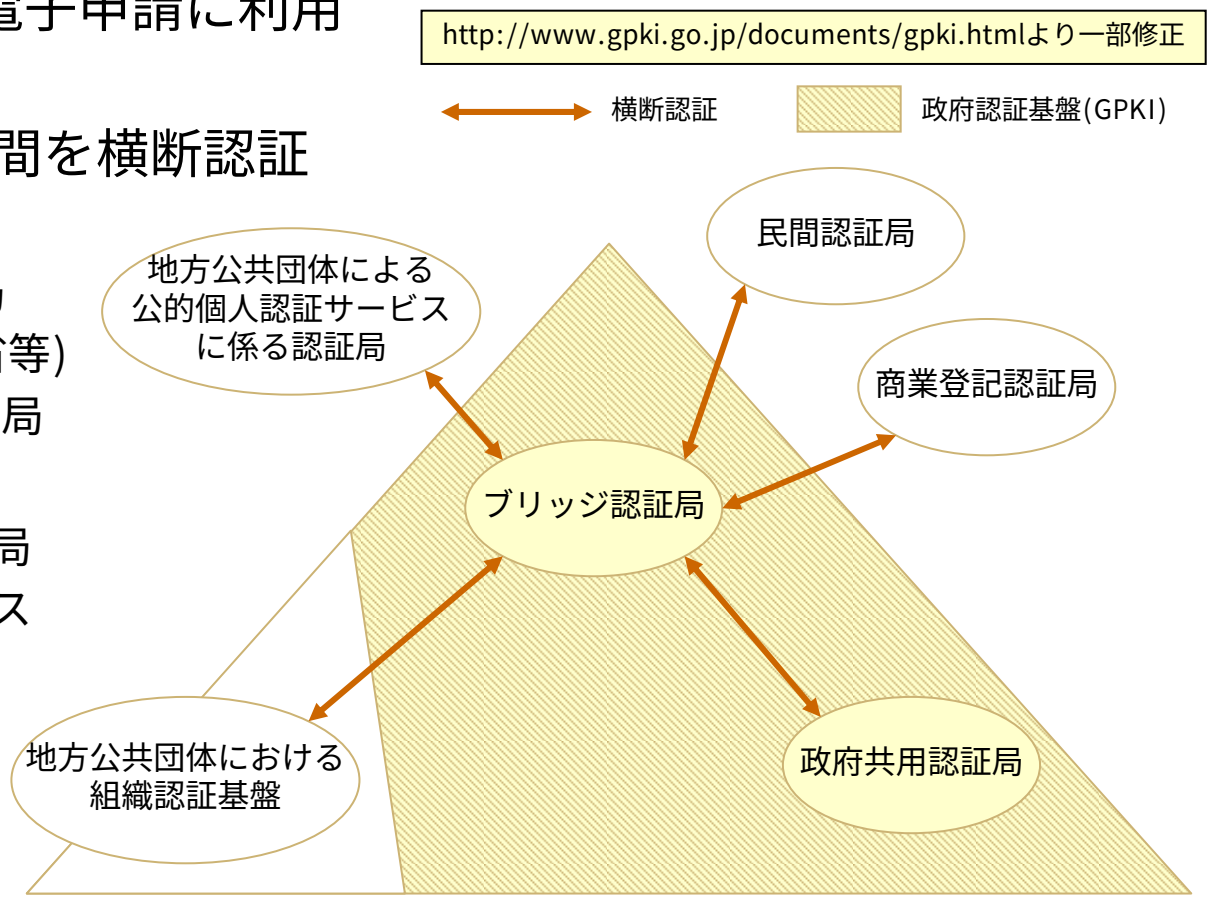

Inter-domain
Interoperability
CA
CA
Component level
Interoperability
Repository
RA
RA
Repository
EE
Application level
Interoperability
EE

日欧米のPKI相互運用に対する取り組み

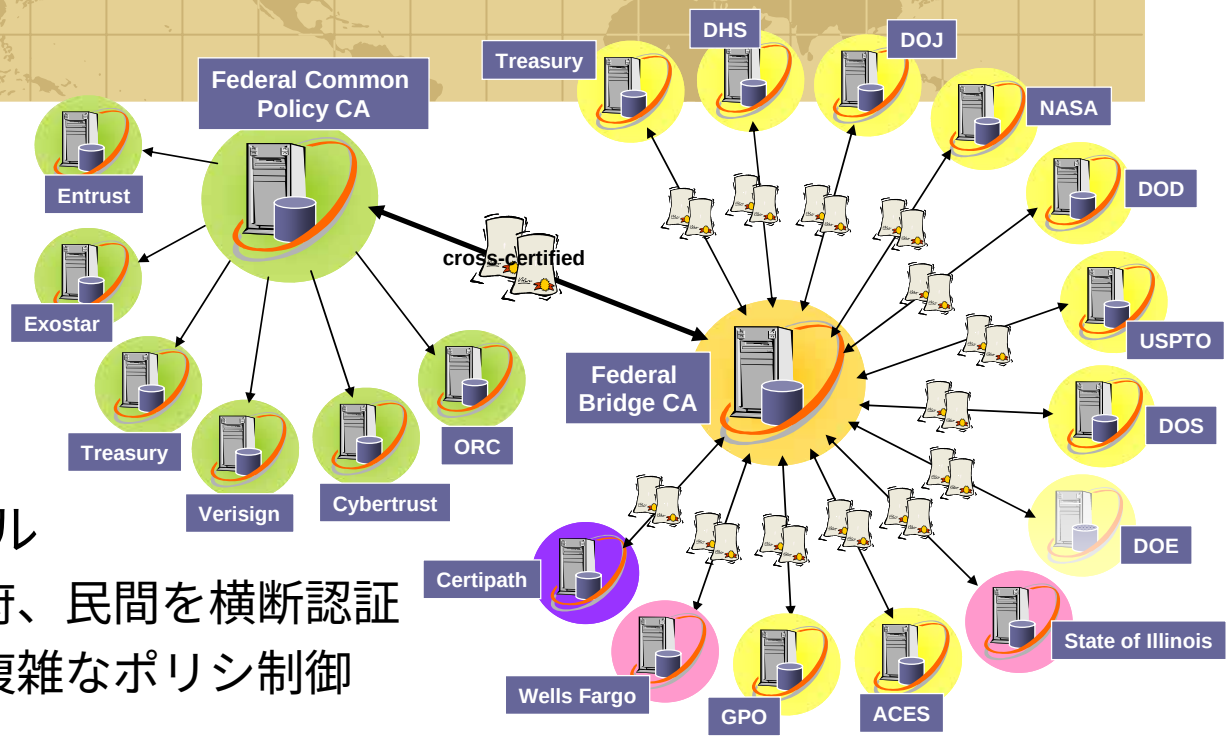


GPKI: 政府認証基盤

- 国民から行政機関への電子申請に利用
  - 本人確認、改ざん検知
- ブリッジCAで府省と民間を横断認証
  - 官職ドメイン
    - GPKIブリッジ認証局
    - 政府共用認証局(府省等)
    - LGPKI ブリッジ認証局
  - 申請者ドメイン
    - 電子署名法特定認証局
    - 公的個人認証サービス
    - 商業登記認証局



Federal PKI



"Federal Identity Credentialing", 6th PKI R&D Workshop より
http://middleware.internet2.edu/pki07/proceedings/

- 米連邦政府のPKI
- 大規模なブリッジモデル
  - 連邦政府省庁、州政府、民間を横断認証
  - 複雑な認証パスと、複雑なポリシ制御
- コモンポリシの整備
  - 4レベルのポリシクライテリア
    - High, Medium, Basic, Rudimentary
  - 各CAのポリシをいずれかにマッピング
- コモンポリシにもとづく共用CAサービスの提供
  - Shared Service Provider
  - C4CA(Citizen and Commerce Class Common CA)

これまでのPKI相互運用アクティビティ

- PKI相互運用アクティビティの成果物の多くは、、、
  - 自らのアクティビティで実装を動かす、あるいは自らのアクティビティ運用に必要な資料
  - 実装ガイドライン、技術仕様、参加手続、規程類など

マルチドメインPKIに**参加**するには
どうすればよいか

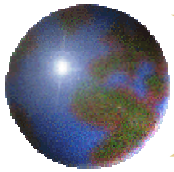
は、あるが、

マルチドメインPKIを**設計・構築**するには
どうすればよいか

が、なかった。

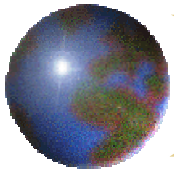
マルチドメインPKIの相互運用性確保

- 相互運用可能なマルチドメインPKIを設計・構築するためのノウハウが必要
  - それぞれ異なるポリシを持つPKIドメインが相互運用する。
  - 他のPKIドメインと相互運用するためには何が必要なのか?
  - PKIドメイン同士が相互運用するにはどんな構成や手法がよいのか?



マルチドメインPKIの相互運用性確保の提案

- PKIドメインの定義
  - マルチドメインPKIの構成要素
- PKIドメイン要件
  - 他PKIドメインと信頼関係を築く要件
- PKIドメイン間の信頼関係
  - トラストポイント統合(統合CA)
  - トラストポイント独立(ブリッジCA)
- トラストリスト
  - PKIドメインとリライングパーティの信頼関係



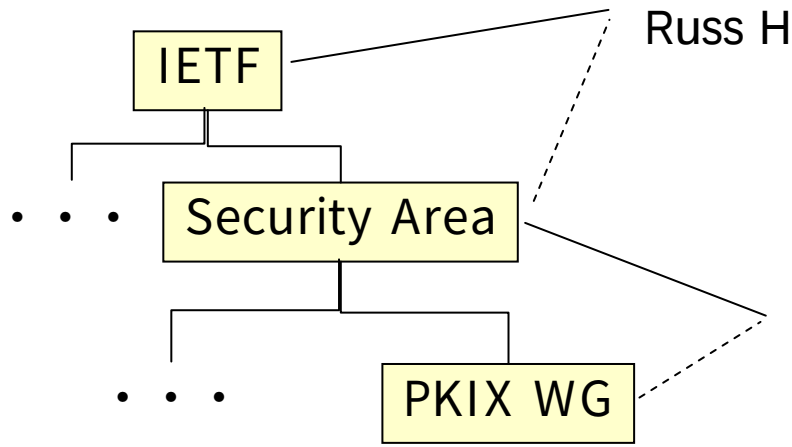
提案の進め方

- IETFへの提案ってどうすればいいの?
  - PKIX WGの有識者と継続的に協議
  - 一定の関心があることがわかった。
- まずはInternet-Draftを書いてみる
  - これを書かないことには始まらない
  - 走りながら考える(セコムのお家芸)
- 一定の賛同を得るには、専門家の支持が必要
  - 特に関心のあるFederal PKI方面から共著者をスカウト
  - WG Draftではないので、Area Directorの支持が不可欠
- マルチドメインPKIって難しすぎる！
  - PKIX WGと別に新たなWGを作らないか、というオファーもあった
  - PKIドメイン毎に曖昧だった用語や信頼関係のモデルを整理することにフォーカス

IETFにおけるPKI技術のキーパーソン

Russ Housley

- PKIX WGのRFCの約1/3を執筆。
- Security Area Director (2003/03～2007/03)
- IETF Chair (2007/03～)

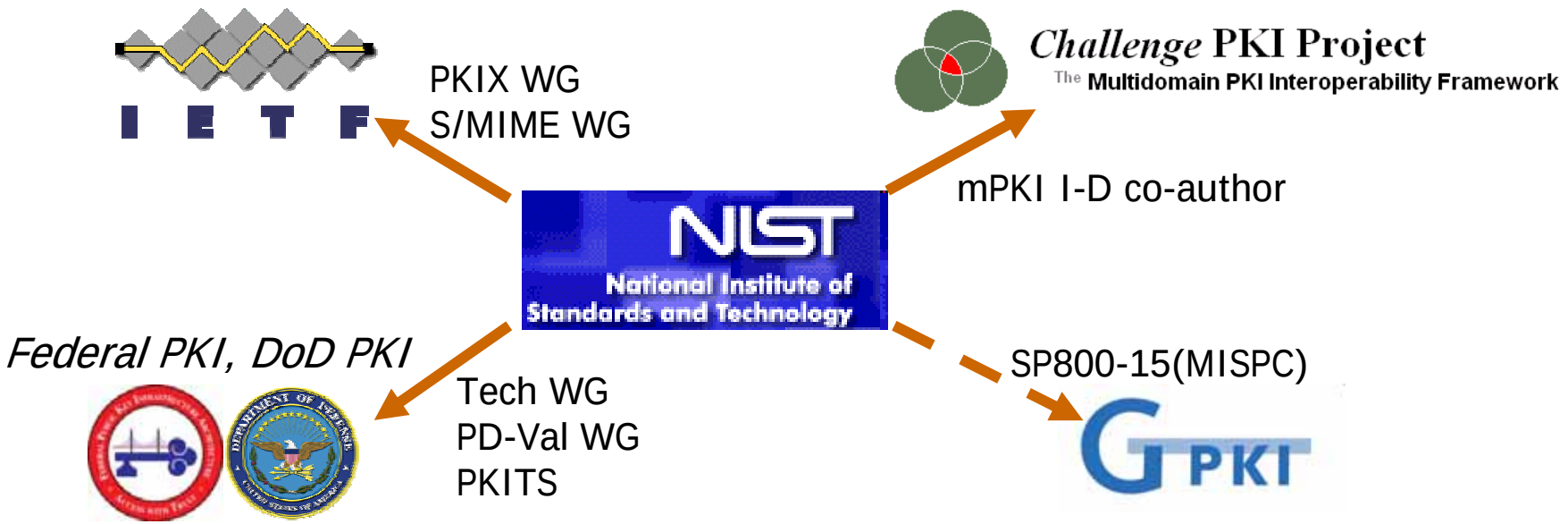


Tim Polk

- NISTの主戦力としてPKIX WGおよびFederal PKIの主要な仕様を執筆。
- PKIX WG co-chair (2000/08～2006/04)
- Security Area Director (2007/03～)

PKIにおけるNISTの存在

マルチドメインPKIの相互運用性確保に長く取り組んでおり、かつ運用ノウハウを持つ世界的にも数少ない組織



標準化までの道のり

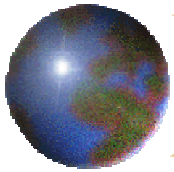
2003/06 I-D Submission
2007/02 WG Draft? → Shepherding AD
2007/05 WG Last Call ← Expert Review
2007/08 AD Evaluation
2007/12 IETF Last Call
2008/04 IESG Evaluation → Do Not Publish
2008/06 RFC-Ed Review
06/24 AUTH48
2008/07? Publish

2003/07 57th IETF/PKIX WGにて発表
2004/09 新co-author Nelson Hastings
2005/07 Security ADらと会談
2006/01 新co-author Rebecca Nielsen
2006/04 co-author会談@NIST
2007/01 構成変更・大幅改訂

あと一息！

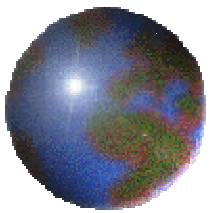
Nelson Hastings
(NIST)
Federal PKI設計に従事

Rebecca Nielsen
(Booz Allen Hamilton)
DoD PKIおよびFederal PKI設計に従事



標準化から学んだ難しさ

- そもそも「マルチドメインPKIの相互運用性」はスコープが広すぎる
  - ある意味マジックワード、まだまだ整理が足りない
  - もっと経験を積んで、個別の課題に落とし込む必要あり
- Individual Draftの標準化プロセス
  - WGで仕様策定して標準化するのが基本
  - Individualに対するプロセスは曖昧な部分が多かった
  - 2006年ぐらいから徐々にプロセスが整備されてきた
- 英語の壁。。。
  - 島岡自身の語学力は言うまでもなく…
  - IETF特有の、キャラクタ(英数字)だけで説明することの難しさ
  - 細かな言葉遣い(複数形や定冠詞など)が、非常に重要な違いに直結



ありがとうございました

JNSA Challenge PKIプロジェクト
セコム IS研究所
島岡　政基 <m-shimaoka@secom.co.jp>