Implementing SSP PKI

NIST PKI Implementation Workshop
April 10, 2006

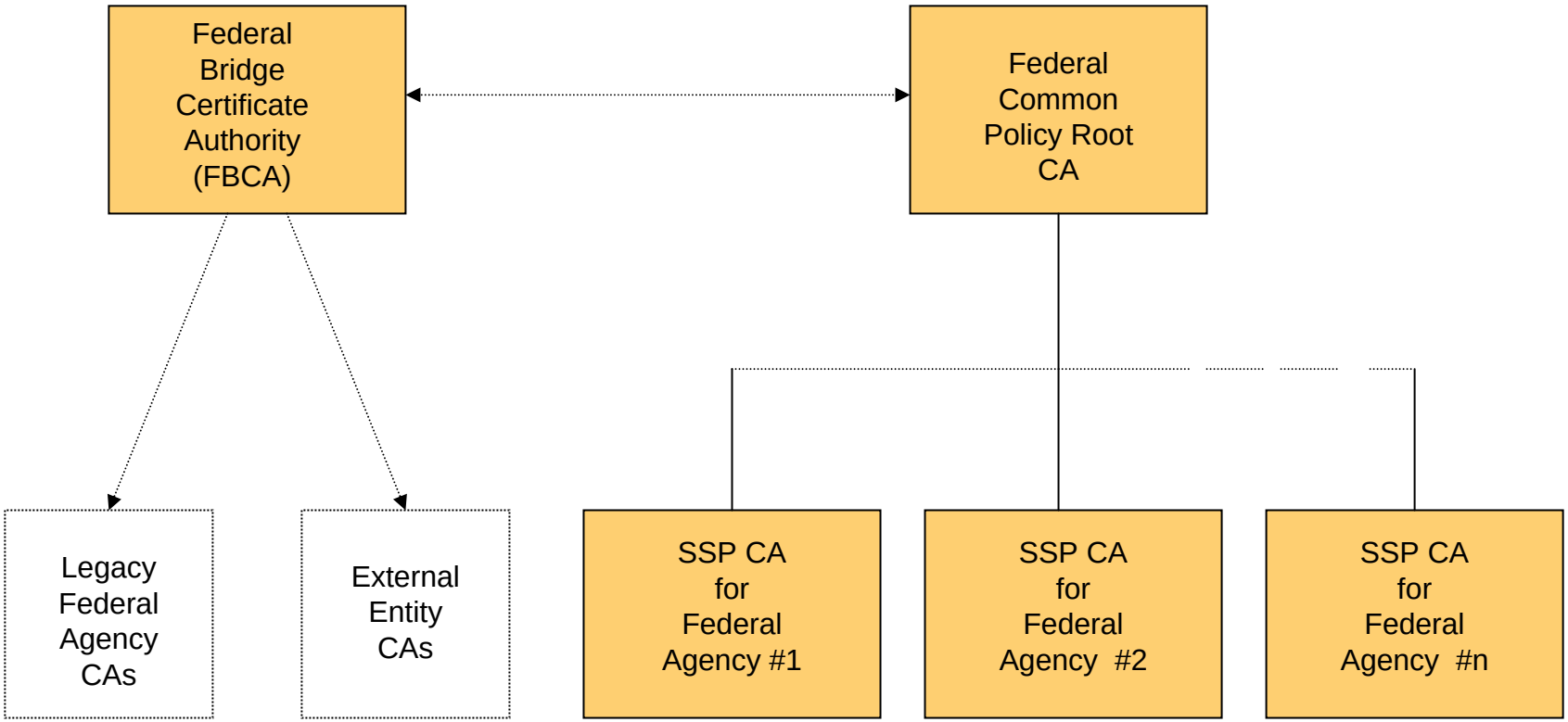
Nick Piazzola
npiazzola@verisign.com
410-691-2100

©2004 VeriSign Inc.

What is Shared Service Provider (SSP)

- In Feb 2004 the Federal Identity Credentialing Committee (FICC) established requirements and a process for the certification of vendors to provide PKI and smart-card issuing services for Federal Agencies. The first approved vendor list was published in Jul 2004
- The FICC specified a common identity credential to be used by Federal employees for both physical and logical access to Federal facilities and IT systems and a hierarchical PKI with Federal Agency CAs operated by approved SSPs.
- SSP CAs chain to the Federal Common Policy Root CA and must comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.
- The Common Policy Framework CP has been updated to comply with NIST FIPS 201
- OMB requires that beginning 1 Jan 2006, Federal agencies acquiring PKI must meet their needs by purchasing services from an approved SSP.

The Federal SSP PKI Hierarchy



Notes:
1. All SSP CAs chain to the Federal Common Policy Root CA.
2. All SSP CAs must comply with the Federal Common Policy Framework CP.
3. All end-entity client certificates issued by SSP CAs are interoperable without the need for special software for path discovery and validation.
4. The Federal Common Policy Root CA is cross-certified with the FBCA.

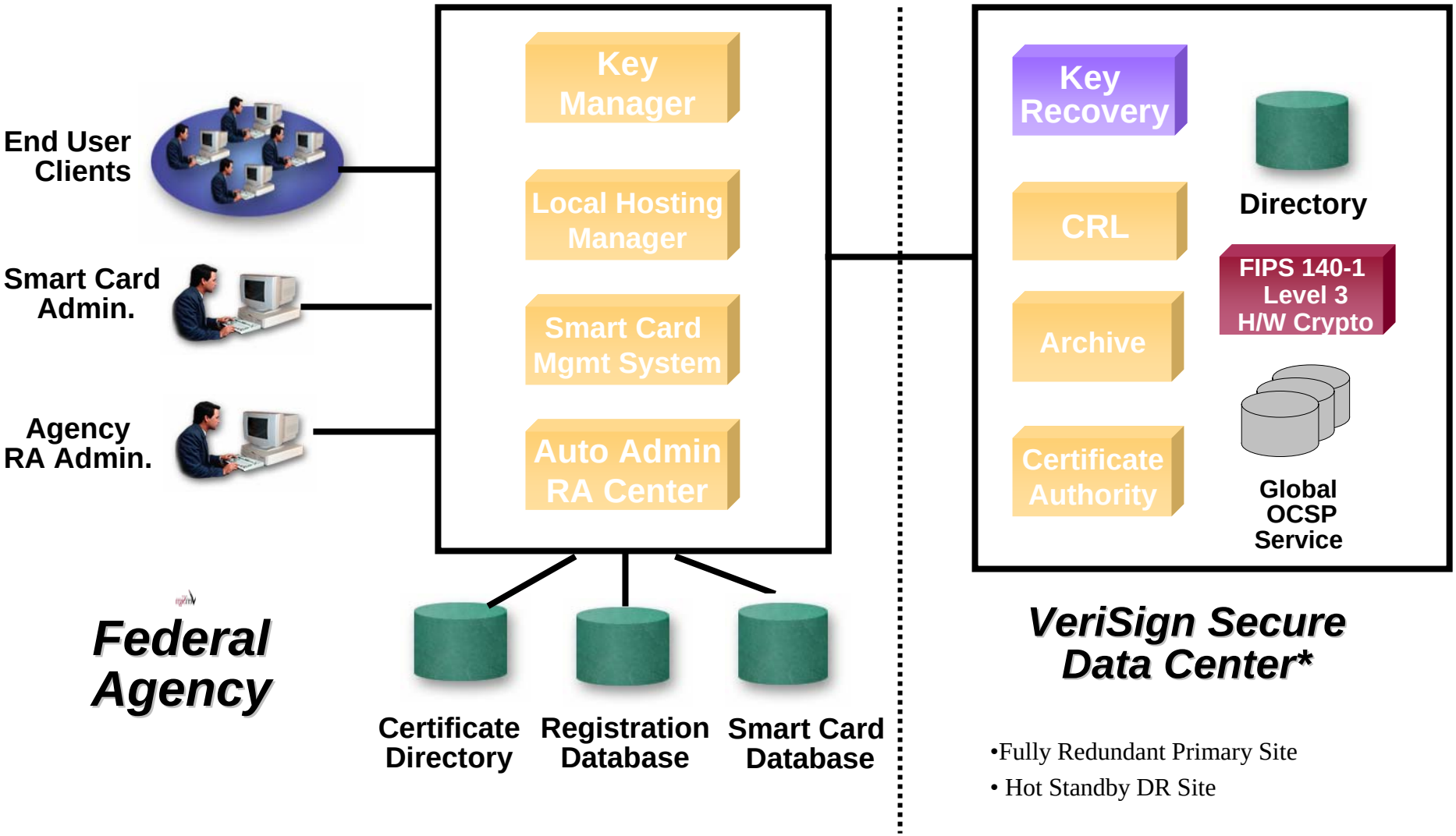
SSP Requirements

- SSP must provide the following capabilities:
  - Certification Authority
  - Registration Authority
  - Repository
  - Archive
  - Smart Card Management System
- SSP offering must meet the following requirements:
  - Certificate Practice Statement (CPS) which maps to the Federal Common Policy Framework Certificate Policy
  - Registration Authority Requirements and Registration Authority Practices Statement (RPS) for components deployed at the Federal agency
  - SSP Repository Service Requirements
- SSP qualifications include the following
  - Annual External Audit
  - Certification and Accreditation (by Federal Agency)

VeriSign Shared Service Provider/HSPD-12 Offering

- VeriSign SSP offering includes a complete Federal agency identity credentialing system
  - Compliant with the Federal Common Policy (approved SSP CPS and C&A).
  - Managed Certificate Authority subordinate to Federal Common Policy Root
  - Integrated Registration Authority and CMS (ActivCard and VeriSign CMS) for issuing smart cards for both physical and logical access.
  - VeriSign Directory Service, VeriSign Certificate Validation Service (TGV)
  - Guaranteed High Availability with Disaster Recovery (East and West Coast Data Centers, Redundant CAs w/auto failover, Dual ISPs, battery backup, diesel generators)
  - All professional services needed for deployment planning, installation and setup, integration with Agency databases.

VeriSign HSPD-12/SSP Managed PKI Service



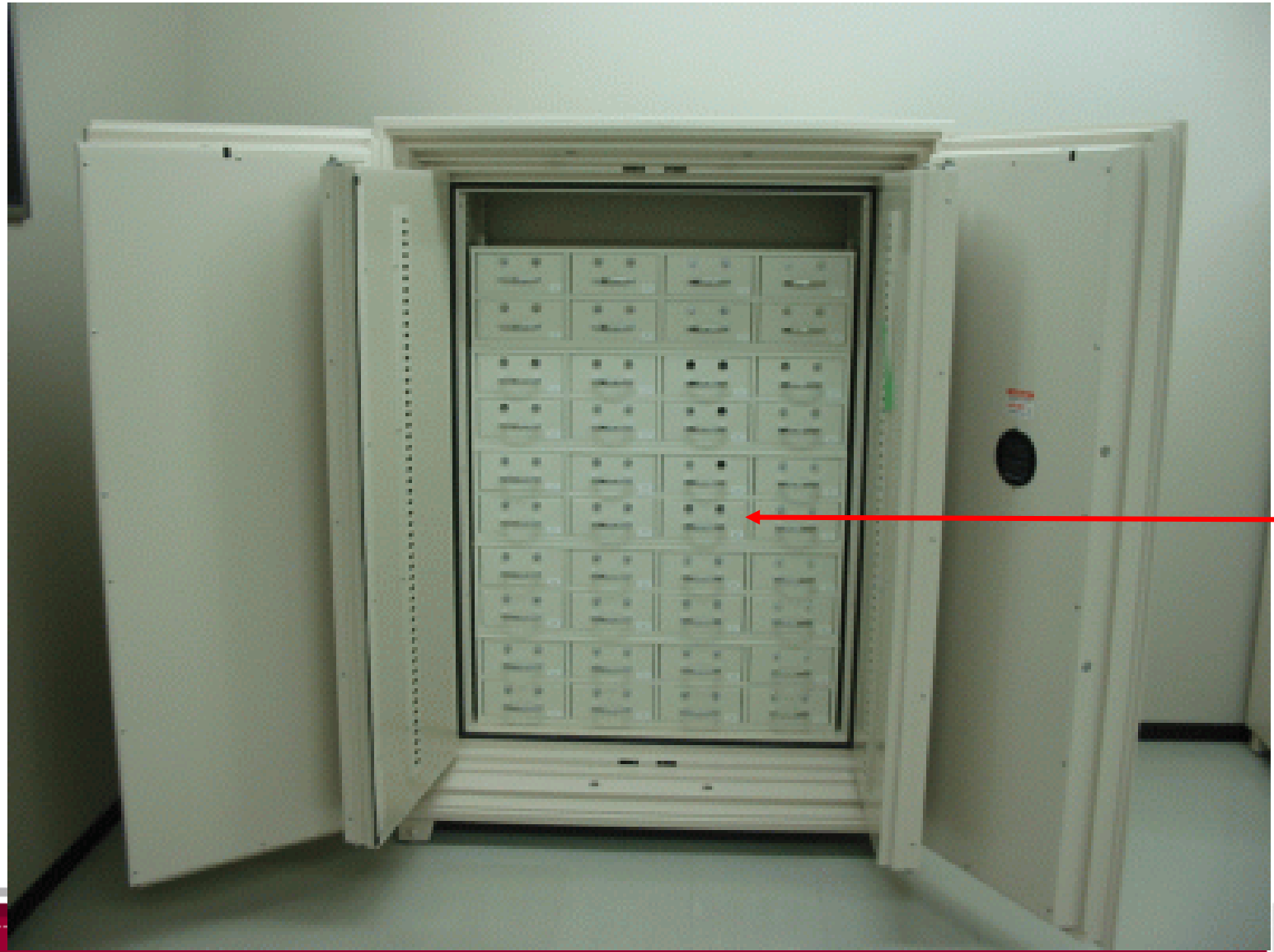
VeriSign Certificate Validation Services

- VeriSign developed a high availability, global certificate validation service
  - Solve the growing problem of large CRLs in PKI deployments
  - Provides real-time validation of code-signing and web server certificates.
- TGV is designed to scale to hundreds of millions of relying parties
  - Next-generation Microsoft operating system will turn on certificate validation by default.
- TGV uses same platform (ATLAS) and infrastructure (13 global sites) used by VeriSign to deliver DNS services for .com and .net.
  - Each of the redundant 13 TGV sites can deliver 50,000 OCSP responses per second.
- VeriSign TGV can propagate a certificate status change globally to the 13 sites in 1 to 2 minutes.
- VeriSign TGV service is bundled at no additional cost with the VeriSign SSP offering.

VeriSign Trusted Global Validation (TGV)

+ Trusted Global Validation (TGV) is based on VeriSign ATLAS Technology used for the .com and .net Internet domain name service
  - ✓ High-Volume (18B queries a day)
  - ✓ Highly-Available (99.999+)
  - ✓ Highly Distributed (global)

Offline Tier 7 Cryptographic Key Storage



Safe Deposit Boxes (at least 16)

Practical Considerations for SSP Implementation

- SSP PKI is a mission-critical system.
- All SSPs are FICC-certified, but not all SSPs are equal.
- Some factors to carefully consider in choosing an SSP:
  - Experience in delivering mission critical systems
  - Experience in delivering managed PKI services (including depth and breadth of experienced personnel and number of PKIs being maintained)
  - Reliability and availability of SSP offering (ability to withstand power failures, internet outages, denial of service attacks, disasters)
  - Ability to deliver 24x7x365 service and willingness to provide SLAs.
  - Security of physical infrastructure and strength of procedures for handing cryptographic keying material including key ceremonies and on/offline protection of private keys. (How many people required to access/activate a private key)
  - Availability of both internal and external validation services
  - Financial stability

VeriSign®