U.S. Department of the Treasury

Public Key Infrastructure Architecture and Personal Identity Verification Integration

Donna Canode
Enterprise Solutions
PKI Program Management Office

April 11, 2006

Objectives

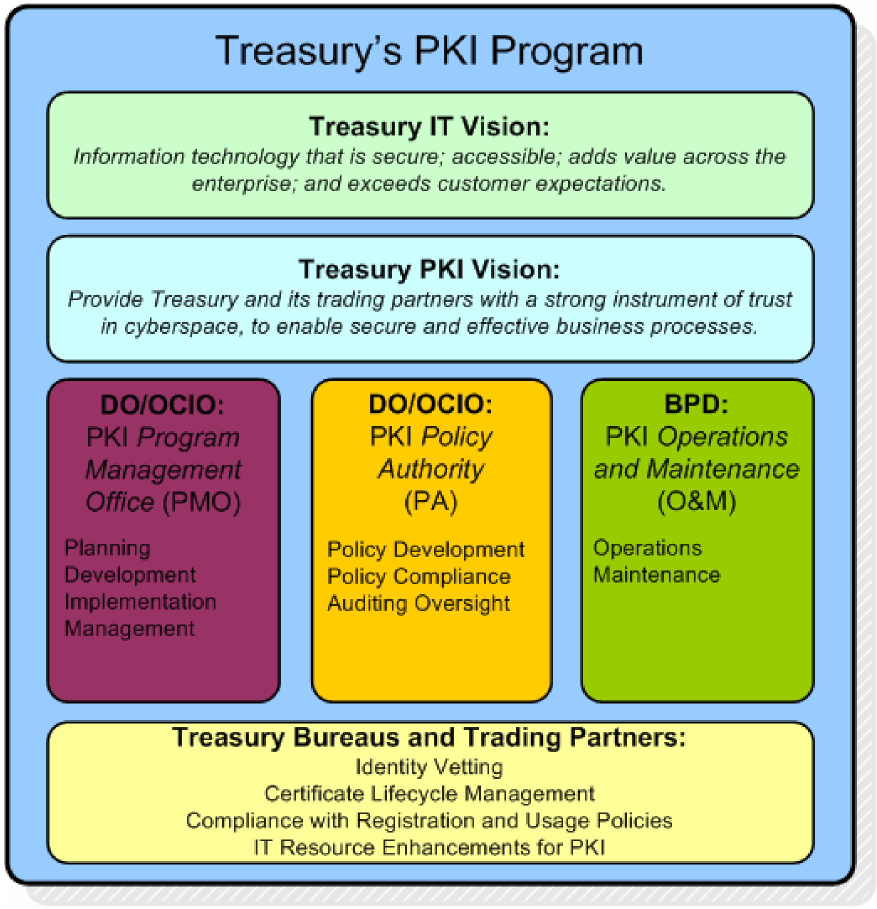
1. Achieve greater understanding of current “as is” PKI architecture
2. Examine Treasury’s reuse of past PKI investments to meet PIV goals
3. Share upcoming PIV related integration activities in PKI program
4. Achieve understanding of PIV integration focus areas that will require attention

Treasury PKI Governance

- **Treasury PMO** provides oversight, responsible for communicating with Treasury Bureaus on current and future PKI activities and initiatives.

- **Treasury PA** develops and provides policy guidance to PKI operations and oversight, and to Bureaus in utilizing public key services.

- **Treasury O&M** provides operations and maintenance of critical PKI components (CAs). Responsible for performing technical activities to reconfigure PKI components to support current and future PKI activities and initiatives.



Treasury's PKI Program

Treasury IT Vision:
Information technology that is secure; accessible; adds value across the enterprise; and exceeds customer expectations.

Treasury PKI Vision:
Provide Treasury and its trading partners with a strong instrument of trust in cyberspace, to enable secure and effective business processes.

DO/OCIO:
PKI *Program Management Office* (PMO)
Planning
Development
Implementation
Management

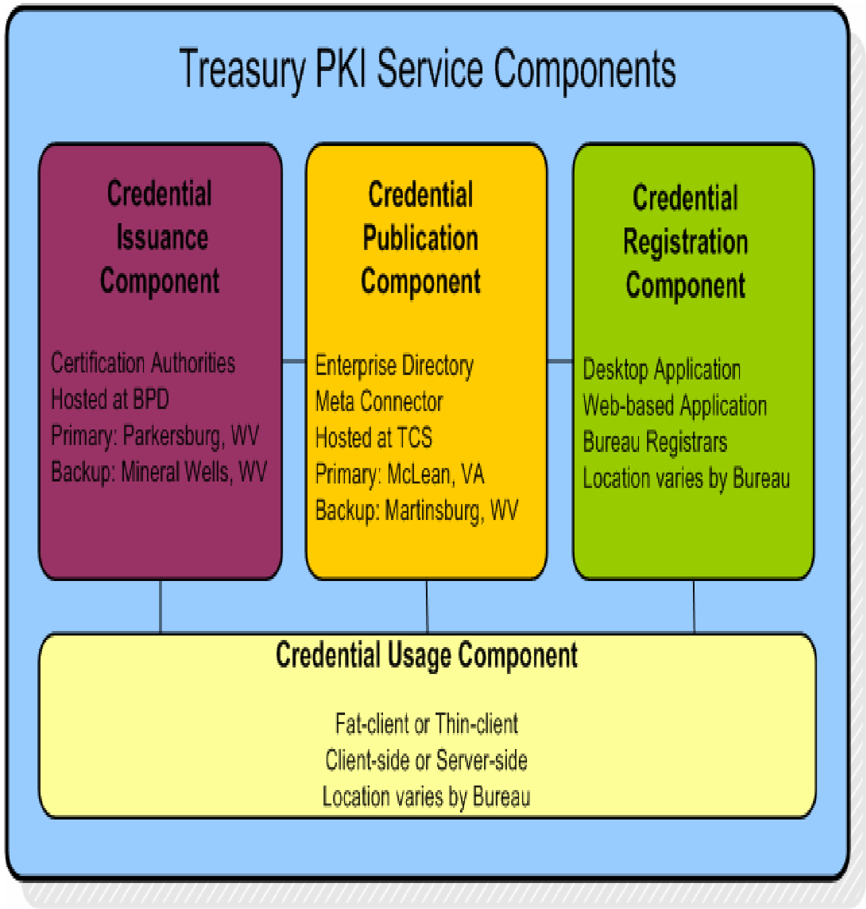
DO/OCIO:
PKI *Policy Authority* (PA)
Policy Development
Policy Compliance
Auditing Oversight

BPD:
PKI *Operations and Maintenance* (O&M)
Operations
Maintenance

Treasury Bureaus and Trading Partners:
Identity Vetting
Certificate Lifecycle Management
Compliance with Registration and Usage Policies
IT Resource Enhancements for PKI

Treasury PKI Component View

- **Issuance** component involves CAs hosted at BPD that provide digital credentials to the PKI user community.
- **Publication** component provides repository services (TEDS) to ensure availability of personnel data to registrars, and credential / revocation data to relying parties.
- **Registration** component provides credential lifecycle management functions for certificate subscribers.
- **Usage** component provides a means to employ PKI services for authentication, integrity, confidentiality and non-repudiation.



Treasury PKI Service Components

Credential Issuance Component

Certification Authorities
Hosted at BPD
Primary: Parkersburg, WV
Backup: Mineral Wells, WV

Credential Publication Component

Enterprise Directory
Meta Connector
Hosted at TCS
Primary: McLean, VA
Backup: Martinsburg, WV

Credential Registration Component

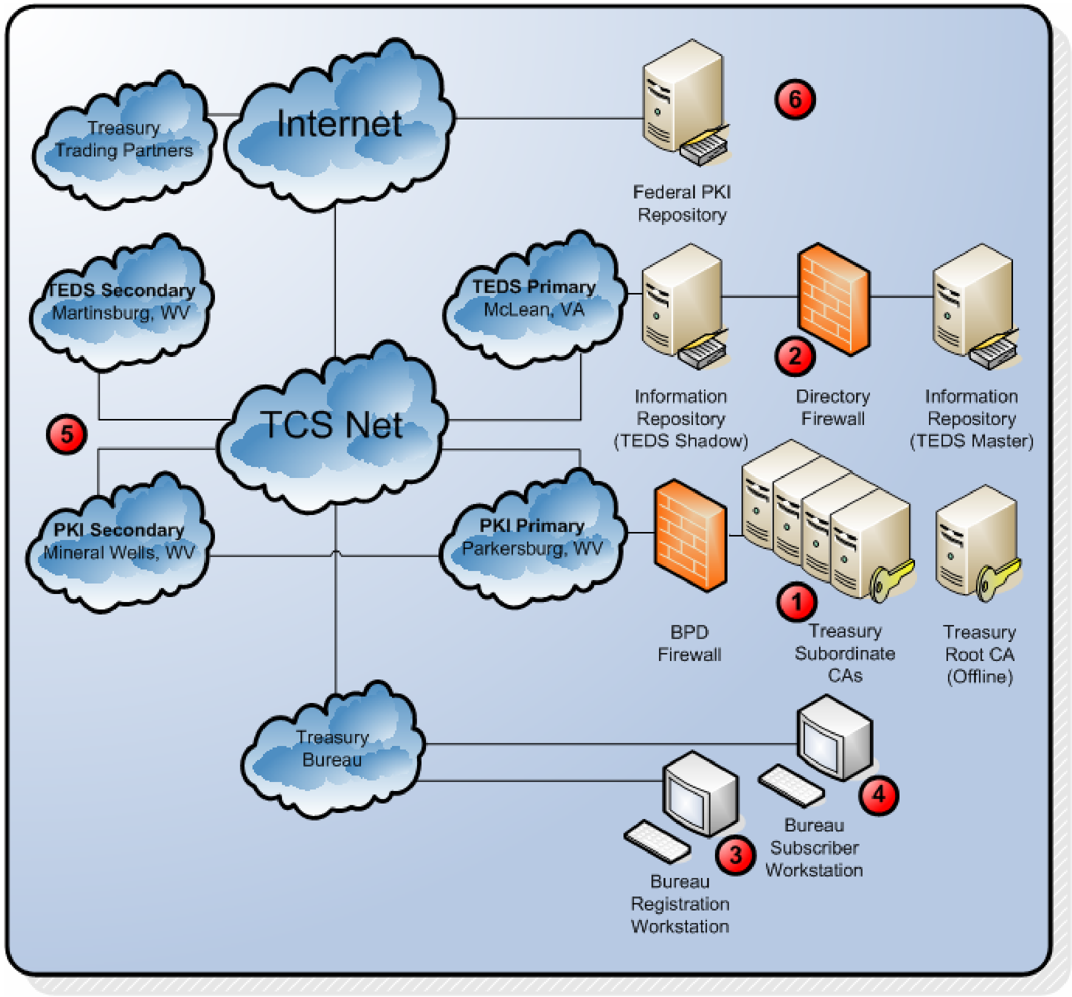
Desktop Application
Web-based Application
Bureau Registrars
Location varies by Bureau

Credential Usage Component

Fat-client or Thin-client
Client-side or Server-side
Location varies by Bureau

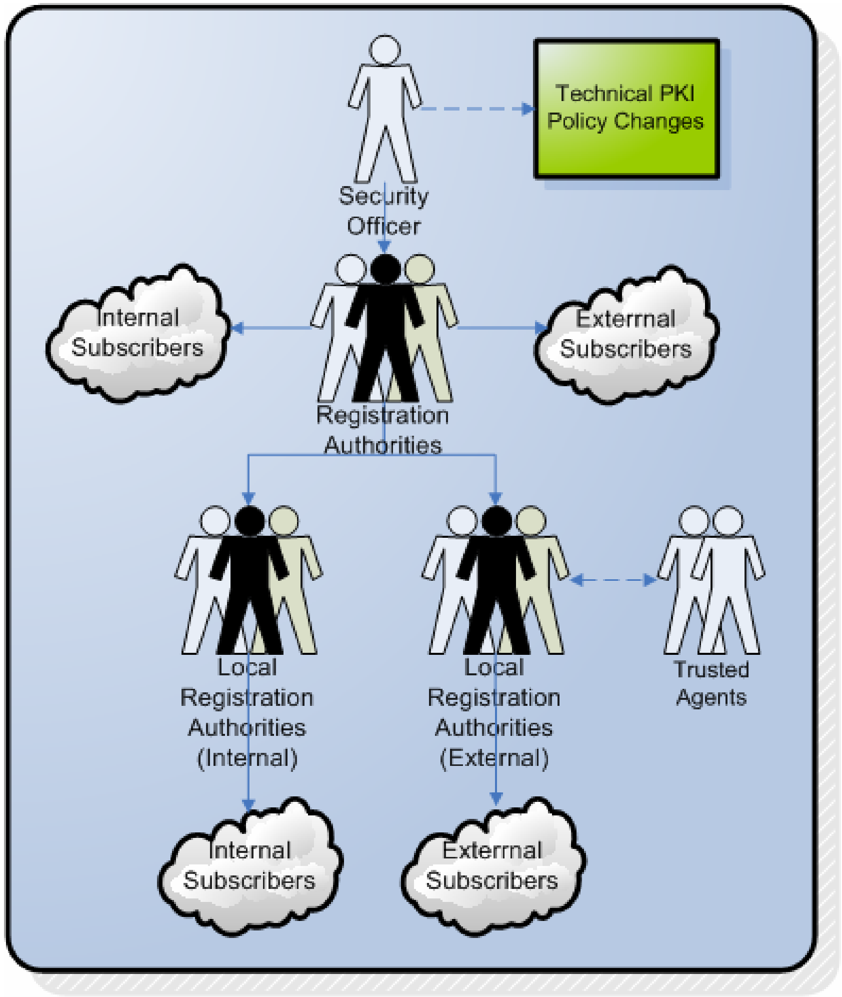
Treasury PKI High-Level Network View

1. **Issuance** network area (*enterprise*) includes all Treasury CAs.
2. **Publication** network area (*enterprise*) provides TEDS master, shadows, meta connectors for PKI data publication and retrieval.
3. **Registration** network area (*local*) includes workstations that issue and manage PKI credentials.
4. **Usage** network area (*local*) includes workstations that use PKI credentials.
5. **Disaster Recovery** network area (*enterprise*) provides fully redundant hosts for issuance and publication components.
6. **External** network area (*enterprise*) provides access to Federal PKI repository for trust interoperability.

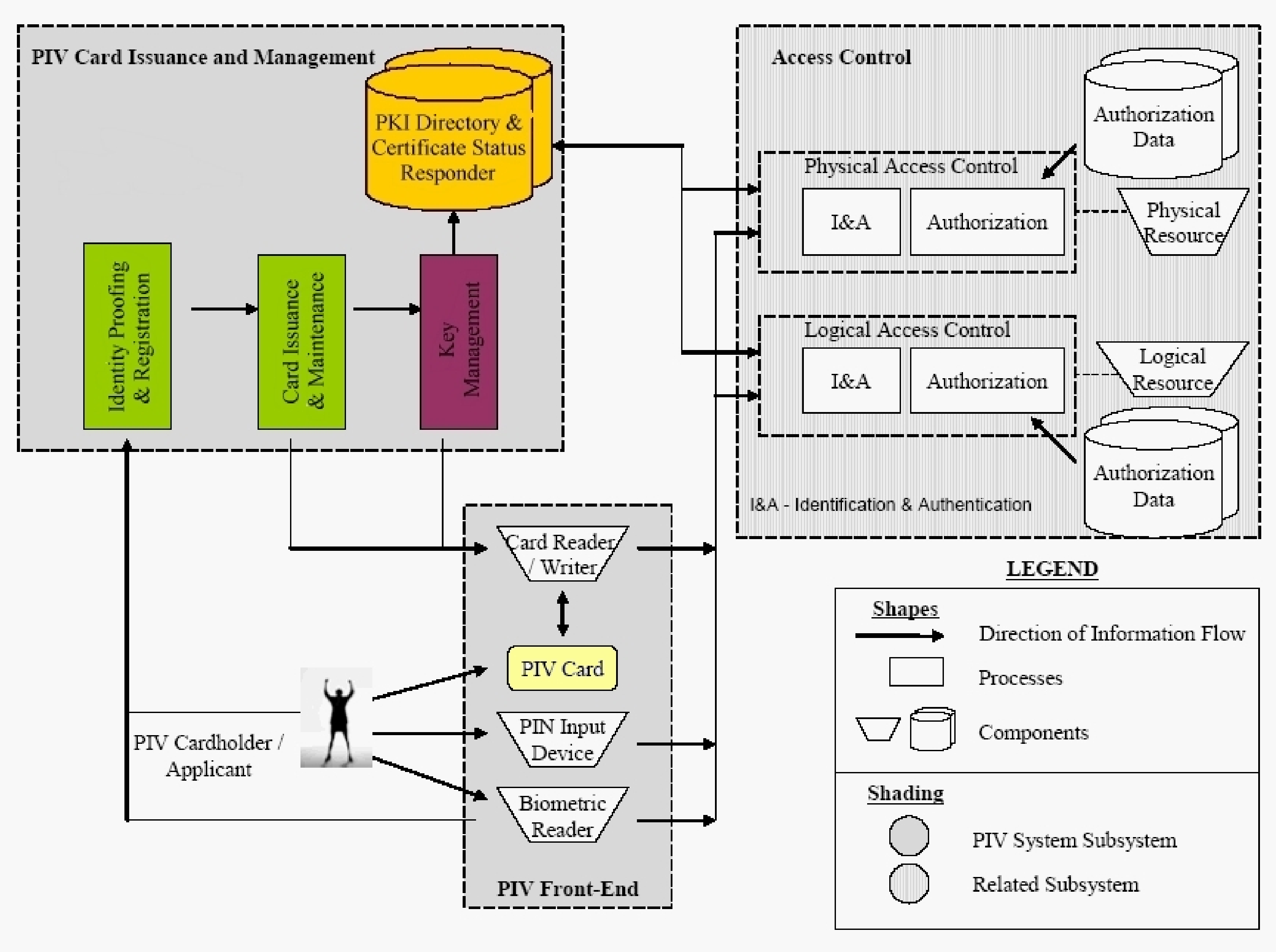

Treasury Trading Partners
Internet
6
Federal PKI Repository
TEDS Secondary Martinsburg, WV
TEDS Primary McLean, VA
2
Information Repository (TEDS Shadow)
Directory Firewall
Information Repository (TEDS Master)
5
TCS Net
PKI Secondary Mineral Wells, WV
PKI Primary Parkersburg, WV
1
BPD Firewall
Treasury Subordinate CAs
Treasury Root CA (Offline)
Treasury Bureau
4
Bureau Subscriber Workstation
3
Bureau Registration Workstation

Treasury PKI Registration Process

- **Security Officers (SOs)** perform PKI policy changes and delegate Subscriber credential management responsibilities to registration authorities. SOs use fat-client management software.
- **Registration Authorities (RAs)** perform credential management functions for internal and external Subscribers, and (in some cases) delegate credential management responsibilities to local registration authorities. RAs use fat-client management software.
- **Local Registration Authorities (LRAs)** perform credential management functions for internal and external Subscribers. LRAs use fat- or thin-client management software.
- **Trusted Agents (TAs)** provide identity proofing functions for Subscribers, and work with LRAs to perform credential management functions for Subscribers. TAs use no software.



PKI Integration with PIV Components



Reusable PKI Components

Treasury will leverage its current PKI investment to the best extent possible.

- Leverage current PKI certificate licensing agreement
- Utilize established Treasury PKI Policies
  - Cross-certified with Federal PKI architecture
  - *Mostly* compliant with Common Policy CP
- Use current *Treasury Operational Certification Authority* (TOCA)
  - Currently providing certificates to internal Treasury community as an enterprise service
  - Best target host within current infrastructure for PIV credential issuance
  - Uses industry-standard PKI software that provides simple interface to external PIV components (CMS, IDMS)
- Adopt Registration Process
  - Integrate with Treasury's currently established PIV-I registration process
  - PIV *Issuing Authorities* (IAs) will inherit RA/LRA responsibilities

Upcoming PKI PIV Integration Activities

Treasury will accomplish the following technical activities to address PIV requirements.

- Modify *Treasury Root Certification Authority* (TRCA)
  - *Online Certificate Status Protocol-* (OCSP-) related certificate extensions
  - Planned to occur simultaneously with TRCA re-key event
- Modify *Treasury Operational Certification Authority* (TOCA)
  - TOCA is subordinate to the TRCA
  - *Online Certificate Status Protocol-* (OCSP-) related certificate extensions
  - PIV Authentication Key certificate
  - Common Policy *Object Identifiers* (OIDs)
  - 18-hour CRL publication
- Establish OCSP responder to assist in credential verification process
  - *Hypertext Transfer Protocol-* (HTTP-) based access
  - Utilize current revocation data using CA or TEDS database source

Focus Areas

Treasury is taking action to address various PIV requirements that require attention

- Key and Certificate Creation
  - PIV Authentication Key certificate contents
  - Other optional keys/certificates?
- Certification Authority Updates
  - Ensure business process continuity
- Policy Activities
  - Alignment of Treasury X.509 CP with Common Policy
- OCSP Responder Establishment
  - Service level agreement with Bureaus for OCSP availability
- Technical alignment with other PIV components
  - IDMS: for credential publication, location, and name form
  - CMS: to handle certificate requests

Future Considerations

Treasury will need to address future Common Policy Requirements

- Common Policy Object Identifier (OID) Assertions
- PIV Authentication Key Size must be increased to RSA 2048-bit length
- Digital Signature / Key Management Key Size must be increased to RSA 2048-bit length
- Secure Hash Algorithm 256 (SHA-256) must be considered
- Treasury may consider use of elliptic curve algorithms where computational efficiency is a factor

Contact Information

For further information on Treasury's PKI, please contact:

• Program Management Office:	Jimmy Atta jimmy.atta@do.treas.gov 202.622.9438
• Policy Management Authority:	Jim Schminky james.schminky@do.treas.gov 202.622.2446
• Operations & Maintenance:	Joe Gribble joe.gribble@bpd.treas.gov 304.480.7608