Interagency Advisory Board

Meeting Agenda, January 27, 2010

1. **Opening Remarks**
2. **Digital Signature Lessons Learned** *(John Landwehr, Adobe)*
3. **Challenges of IdM for the Virtual Lifetime Electronic Record (VLER)** *(Doug Felton, DoD/VA Program Office*
4. **Global Threat Intelligence** *(Phyllis Schneck, McAfee*
5. **New Initiative- Joint IAB/SCA Meetings** *(Randy Vanderhoof, Smart Card Alliance)*
6. **The Value of PKI** *(Judy Spencer, GSA)*
7. **Closing Remarks**

Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

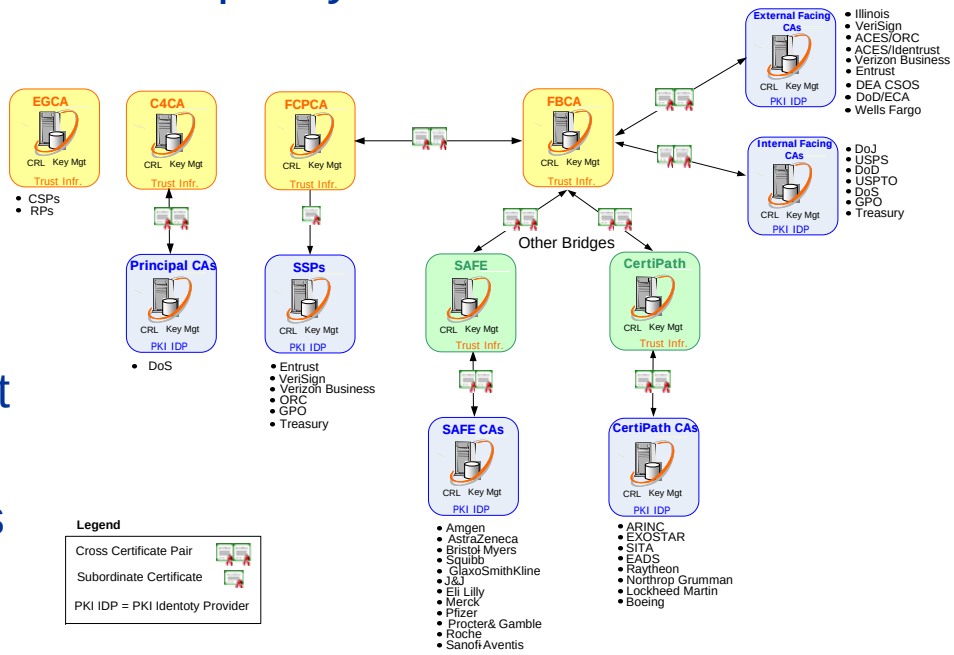
www.idmanagement.gov

The Realized Value of Federal PKI

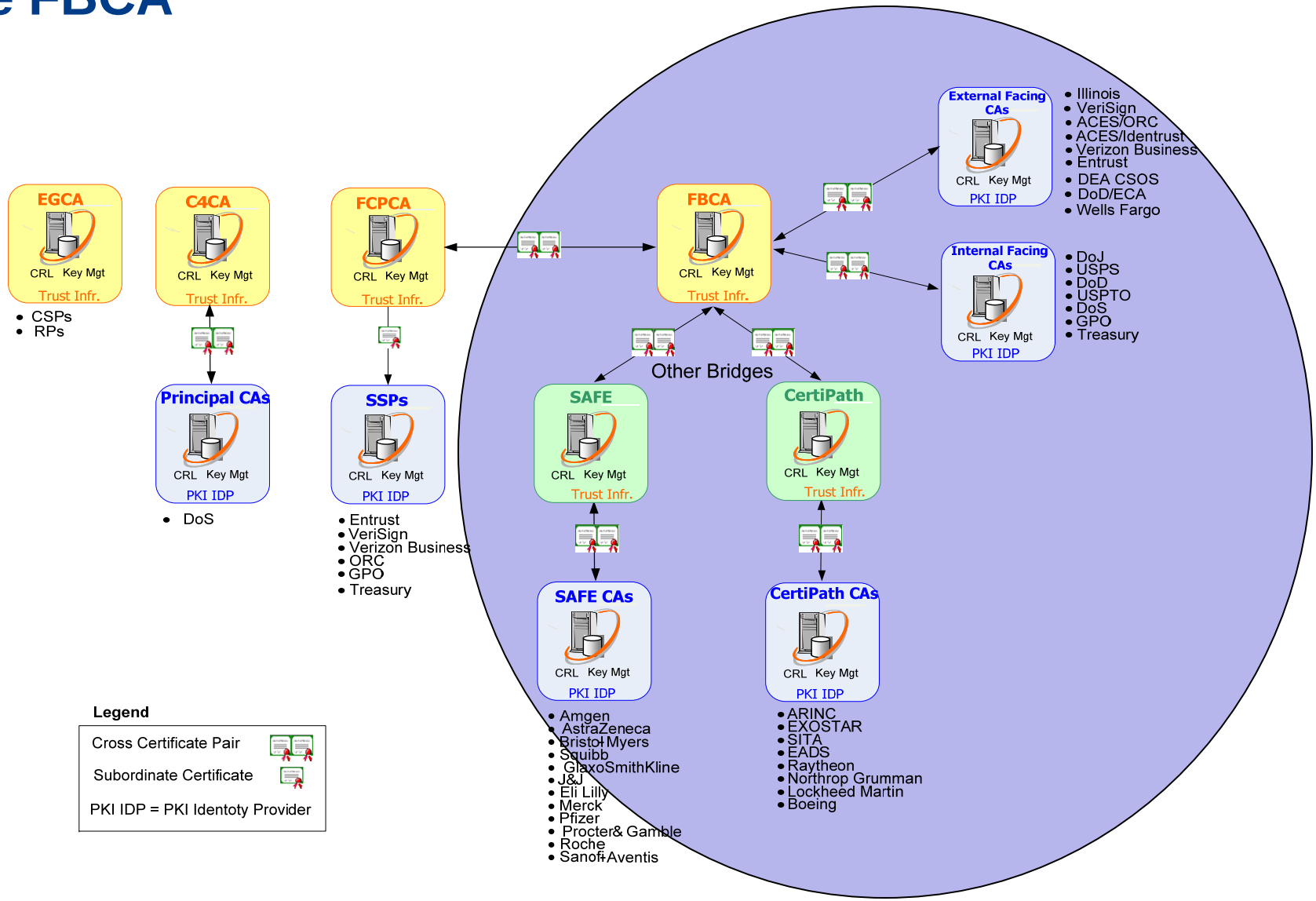
Judith Spencer
Agency Expert - IDM
Office of Governmentwide Policy
GSA
Judith.Spencer@GSA.Gov

What is Federal PKI?

- Federal PKI is comprised of two primary components:
  - The Federal PKI Policy Authority
  - The Federal PKI Architecture
- The Policy Authority develops Federal PKI policy and provides operational oversight
- The Architecture consists of four primary components:
  - The Federal Bridge Certification Authority (FBCA)
  - The Federal Common Policy Root CA (COMMON)
  - The Citizen and Commerce Class Common CAs (C4CA)
  - The E-Government CAs (EGCA)



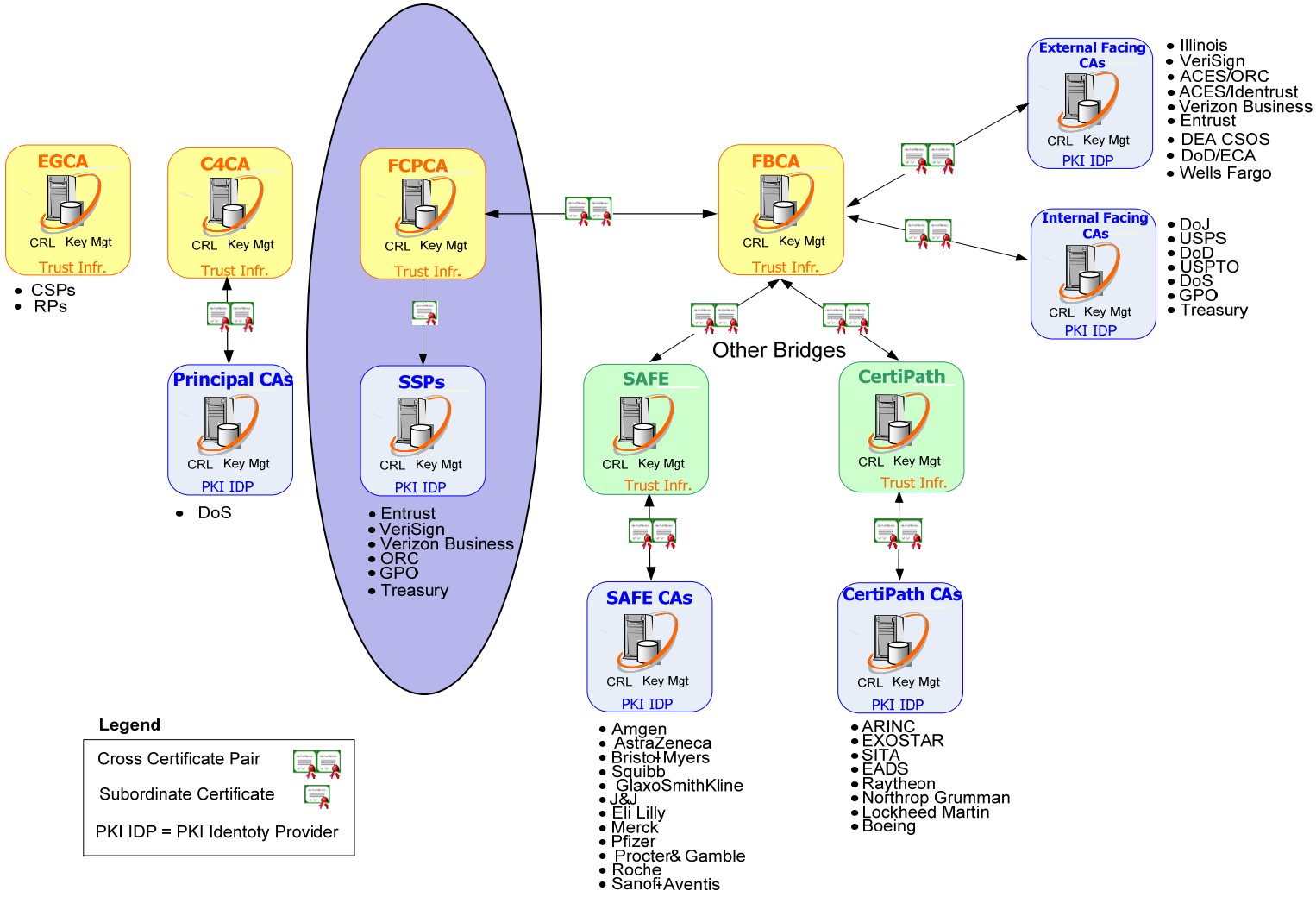
The FBCA


EGCA
CRL Key Mgt
Trust Infr.
• CSPs
• RPs
C4CA
CRL Key Mgt
Trust Infr.
Principal CAs
CRL Key Mgt
PKI IDP
• DoS
FCPCA
CRL Key Mgt
Trust Infr.
SSPs
CRL Key Mgt
PKI IDP
• Entrust
• VeriSign
• Verizon Business
• ORC
• GPO
• Treasury
FBCA
CRL Key Mgt
Trust Infr.
External Facing CAs
CRL Key Mgt
PKI IDP
• Illinois
• VeriSign
• ACES/ORC
• ACES/Identrust
• Verizon Business
• Entrust
• DEA CSOS
• DoD/ECA
• Wells Fargo
Internal Facing CAs
CRL Key Mgt
PKI IDP
• DoJ
• USPS
• DoD
• USPTO
• DoS
• GPO
• Treasury
Other Bridges
SAFE
CRL Key Mgt
Trust Infr.
SAFE CAs
CRL Key Mgt
PKI IDP
• Amgen
• AstraZeneca
• Bristol-Myers
• Squibb
• GlaxoSmithKline
• J&J
• Eli Lilly
• Merck
• Pfizer
• Procter& Gamble
• Roche
• Sanofi-Aventis
CertiPath
CRL Key Mgt
Trust Infr.
CertiPath CAs
CRL Key Mgt
PKI IDP
• ARINC
• EXOSTAR
• SITA
• EADS
• Raytheon
• Northrop Grumman
• Lockheed Martin
• Boeing
Legend
Cross Certificate Pair
Subordinate Certificate
PKI IDP = PKI Identoty Provider

The FBCA

- The FBCA is the identity trust hub that enables peer-to-peer transactions between its member organizations, both Federal and non-Federal.
- Federal agencies operating PKIs cross-certified with the FBCA are :
  - Department of Defense
  - Department of Justice
  - Government Printing Office
  - United States Postal Service
  - Department of State
  - Drug Enforcement Administration
  - Treasury;
  - United States Patent and Trademark Office
- Non-Federal entities cross-certified with the FBCA are:
  - State of Illinois,
  - Commercial PKI Bridges:
    - CertiPath, which serves the Aerospace and Defense industry
    - SAFE-BioPharma, which has established FBCA-comparable digital identity and signature standards for the pharmaceutical and healthcare industries.
  - PKI service providers associated with the FBCA:
    - VeriSign
    - Entrust
    - Verizon Business
    - Access Certificates for Electronic Services (ACES) – GSA-owned Policy
    - DOD External Certification Authority – DOD-owned Policy

COMMON


EGCA
CRL Key Mgt
Trust Infr.
• CSPs
• RPs
C4CA
CRL Key Mgt
Trust Infr.
Principal CAs
CRL Key Mgt
PKI IDP
• DoS
FCPCA
CRL Key Mgt
Trust Infr.
SSPs
CRL Key Mgt
PKI IDP
• Entrust
• VeriSign
• Verizon Business
• ORC
• GPO
• Treasury
FBCA
CRL Key Mgt
Trust Infr.
External Facing CAs
CRL Key Mgt
PKI IDP
• Illinois
• VeriSign
• ACES/ORC
• ACES/Identrust
• Verizon Business
• Entrust
• DEA CSOS
• DoD/ECA
• Wells Fargo
Internal Facing CAs
CRL Key Mgt
PKI IDP
• DoJ
• USPS
• DoD
• USPTO
• DoS
• GPO
• Treasury
Other Bridges
SAFE
CRL Key Mgt
Trust Infr.
SAFE CAs
CRL Key Mgt
PKI IDP
• Amgen
• AstraZeneca
• Bristol-Myers
• Squibb
• GlaxoSmithKline
• J&J
• Eli Lilly
• Merck
• Pfizer
• Procter& Gamble
• Roche
• Sanofi-Aventis
CertiPath
CRL Key Mgt
Trust Infr.
CertiPath CAs
CRL Key Mgt
PKI IDP
• ARINC
• EXOSTAR
• SITA
• EADS
• Raytheon
• Northrop Grumman
• Lockheed Martin
• Boeing
Legend
Cross Certificate Pair
Subordinate Certificate
PKI IDP = PKI Identoty Provider

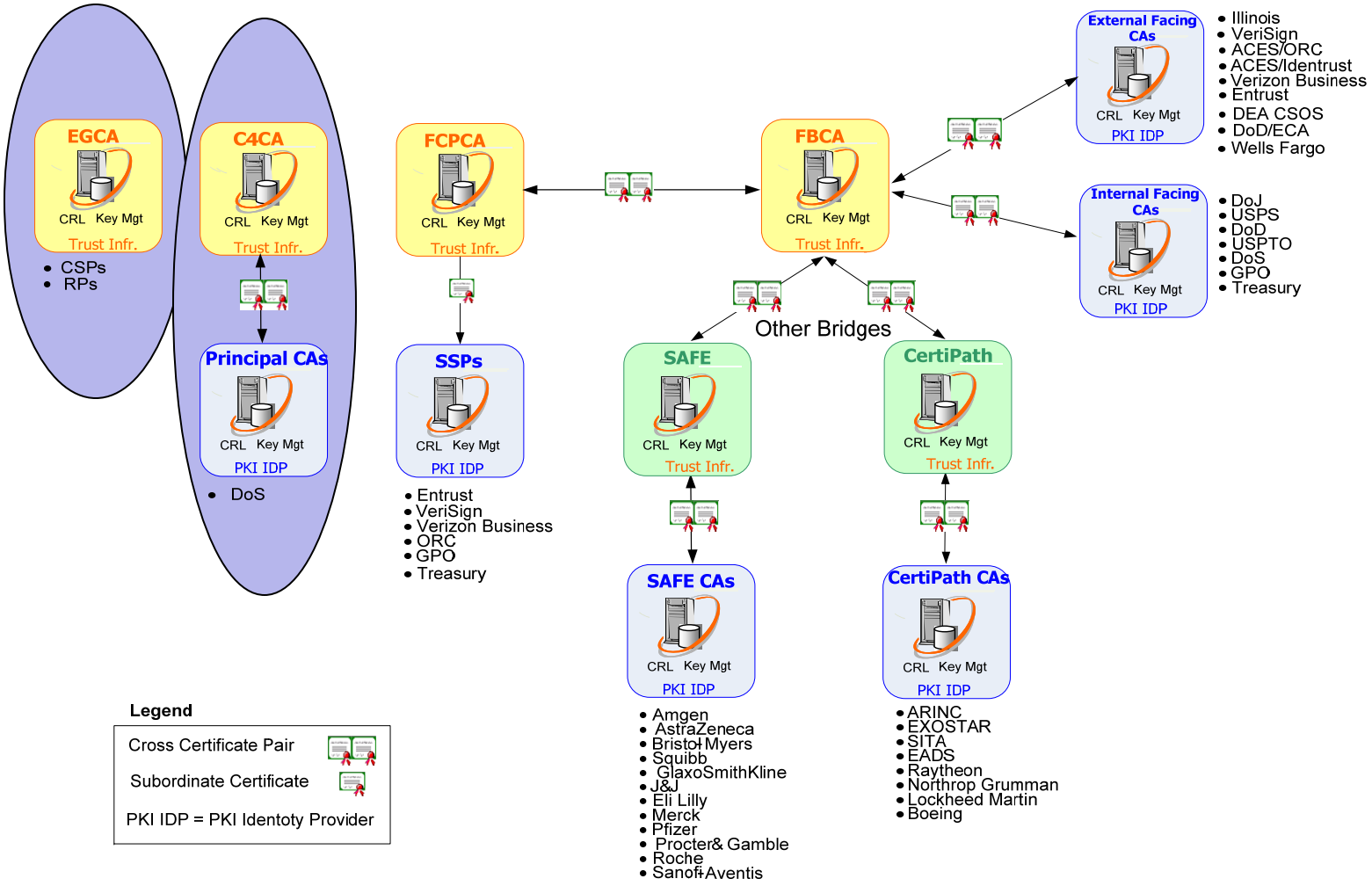
COMMON

- In April 2003, the CIO Council challenged the FPKIPA to establish an FPKI hierarchical trust anchor for all Federal agency CAs.
- Commercial SSPs were invited to apply for subordination to COMMON via Certification Practices Statement (CPS) mapping to the COMMON CP.
- Departments and agencies were then free to acquire services from one of these approved providers.
- COMMON provides a single trust anchor for Federal PKI transactions and interfaces with the external trusted PKI communities through a single cross certification between COMMON and the FBCA.

Benefits of COMMON

- COMMON enhances the FPKI as follows:
  - Federal agencies can deploy digital credentials without having to operate and maintain an Enterprise PKI.
  - Individual Federal agencies are relieved from the requirement to establish their own CPs and to map to the FBCA.
  - COMMON is the single trust root supporting interoperability within the Federal government.
  - COMMON is public facing and has its root CA in an increasing number of COTS product trust stores.
  - FIPS 201 identifies COMMON as the source of digital authentication certificates for the PIV credentials.

C4CA & EGCA


EGCA
CRL Key Mgt
Trust Infr.
• CSPs
• RPs
C4CA
CRL Key Mgt
Trust Infr.
Principal CAs
CRL Key Mgt
PKI IDP
• DoS
FCPCA
CRL Key Mgt
Trust Infr.
SSPs
CRL Key Mgt
PKI IDP
• Entrust
• VeriSign
• Verizon Business
• ORC
• GPO
• Treasury
FBCA
CRL Key Mgt
Trust Infr.
External Facing CAs
CRL Key Mgt
PKI IDP
• Illinois
• VeriSign
• ACES/ORC
• ACES/Identrust
• Verizon Business
• Entrust
• DEA CSOS
• DoD/ECA
• Wells Fargo
Internal Facing CAs
CRL Key Mgt
PKI IDP
• DoJ
• USPS
• DoD
• USPTO
• DoS
• GPO
• Treasury
Other Bridges
SAFE
CRL Key Mgt
Trust Infr.
SAFE CAs
CRL Key Mgt
PKI IDP
• Amgen
• AstraZeneca
• Bristol-Myers
• Squibb
• GlaxoSmithKline
• J&J
• Eli Lilly
• Merck
• Pfizer
• Procter& Gamble
• Roche
• Sanofi-Aventis
CertiPath
CRL Key Mgt
Trust Infr.
CertiPath CAs
CRL Key Mgt
PKI IDP
• ARINC
• EXOSTAR
• SITA
• EADS
• Raytheon
• Northrop Grumman
• Lockheed Martin
• Boeing
Legend
Cross Certificate Pair
Subordinate Certificate
PKI IDP = PKI Identoty Provider

C4CA & EGCA

C4CA

- C4CA is the U.S. Federal government's mechanism for enabling a PKI trust domain satisfying level of assurance 2.
- Its primary purpose is to ensure that "commercial grade" PKI implementations (e.g., those that do not aspire to the requirements for FBCA cross-certification) are not disenfranchised as identity solutions.
- Uptake of C4CA is somewhat limited. However, DoS has been approved for cross-certification with C4CA in anticipation of extending electronic services to citizens without commingling certificates with employees.

EGCA

- The EGCA issues PKI certificates to approved Credential Service Provider (CSP) and Federal Relying Party (RP) systems to enable mutual authentication, and therefore mutual trust.
- Since only approved CSP and RP applications have EGCA credentials, the ability for a non-trusted entity to impersonate either identity or intercept the transaction is eliminated.

Qualitative Benefits

- Strong Digital Signatures: When used within a federated model, digital signatures allow important business and regulatory transactions to occur in a fully electronic, secure environment.
- Support for Technical Non-Repudiation: When a document is "digitally signed," the document's contents are incorporated into the signature.
- Strong Authentication: When the individual attempts to gain access (either by logging on to a system or network, or approaching a physical access terminal), a challenge is presented which is signed using the individual's private key
- Strong Encryption: Data at rest and data in motion
- Trusted Interoperability between Disparate Systems: Federated PKI trust mechanisms, such as the FBCA and the other bridges that are partnering with it, allow trusted interoperability between disparate systems, greatly facilitating e-Commerce.

Quantitative Benefits

- Synergy with HSPD-12: PIV Cards are issued with the mandatory PKI credential under COMMON
- Multi-factor Authentication: Something you know – PIN; Something you have – Digital Credential
- Network Security
  - Access Control
  - Secure Tunneling
  - Single-sign On
- PKI-enablement of Applications: an application is able to process any public key certificate it receives and make a trust decision without relying on end-user cognizance

Realized Value

- Department of State: PKI-enablement of the Immigrant Visa Allocation Management System (IVAMS) provides an annual savings to US taxpayers of over **$718,600** by reducing the time required to process requests for Visa numbers from days to less than an hour.
- SAFE-BioPharma/Johnson & Johnson: Estimated net savings due to strong electronic signatures in excess of **$1M** annually, which will grow over time as such use grows .
- DOD: A **46%** reduction in NIPRNET Intrusion Activity as a result of Smart Card Logon implementation.

45

The Future of PKI

- Technology Maturity
- Global Deployment
- Increasing adoption by Industry
  - E-mail clients (digitally signing and encrypting e-mails);
  - Form signing software (digitally signing forms);
  - Root Stores of major internet browser and products;
  - Word processors and readers;
  - Internet browsers; and
  - Smart Identity Cards (e.g., DoD CAC, PIV Card, FRAC, TWIC) that move PKI into the physical and logical access control arenas
- The Future is Now