PKI in the Federal Government

e-Authentication and Federal PKI Policy and Processes

Federal Bridge Certification Authority
Access with Trust

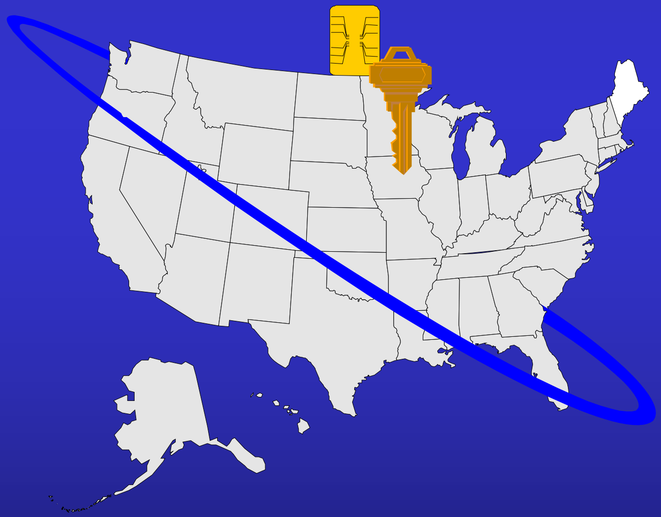
PKI ACES
Access Certificates for Electronic Services
Securing the Business of Government

David Temoshok
Federal PKI Policy Manager
GSA Office of Governmentwide Policy

Defining E-Government

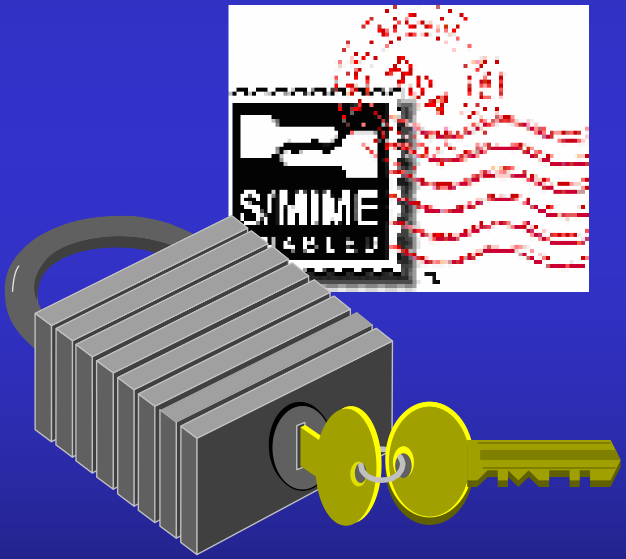
The use of electronic systems to perform business and service-related transactions

- Improve internal government operations
  - Intra-governmental transactions
  - Government as Buyer
  - Government as Seller
- Enhance the delivery of services to citizens



E-Government Challenges

- Data Privacy and security
- Authentication: Knowing who’s on the other end
- Confidentiality: Protecting data in transit
- Data integrity: ensuring integrity in transit and storage



E-Gov Initiatives -- Presidents Management Council

Government to Citizen

	Managing Partner
1. USA Service	GSA
2. EZ Tax Filing	Treasury
3. Online Access for Loans	DoEd
4. Recreation One Stop	DOI
5. Eligibility Assistance Online	Labor

Government to Business

	Managing Partner
1. Federal Asset Sales	GSA
2. Online Rulemaking Management	DOT
3. Simplified and Unified Tax and Wage Reporting	Treasury
4. Consolidated Health Informatics (business case)	HHS
5. Business Compliance One Stop	SBA
6. Int’l Trade Process Streamlining	DOC

Government to Government

	Managing Partner
1. e-Vital (business case)	SSA
2. e-Grants	HHS
3. Disaster Assistance and Crisis Response	FEMA
4. Geospatial Information One Stop	DOI
5. Wireless Networks	DOJ
6. Enterprise Legal Case Management	DOJ

Internal Effectiveness and Efficiency

	Managing Partner
1. e-Training	OPM
2. Recruitment One Stop	OPM
3. Enterprise HR Integration including e-Travel	OPM
4. Integrated Acquisition	GSA
5. e-Records Management	NARA

Core Infrastructure: e-Authentication

The Electronic Signatures in Global and National Commerce (E-SIGN) Act

- Applies broadly to commercial transactions affecting interstate or foreign commerce, including:
  - banking, securities, insurance, mortgage and student loans, and retirement services.
- Establishes legal validity of electronic records/signatures.
- Pre-empts laws/regulations that:
  - Deny legal effect, validity or enforceability of a signature, contract, or other record of a transaction solely because it is in electronic form.
- Government activities generally are not within the scope of this legislation; they are instead addressed by the Government Paperwork Elimination Act.
- E-SIGN began to take effect on October 1.

What is an Electronic Signature under E-SIGN?

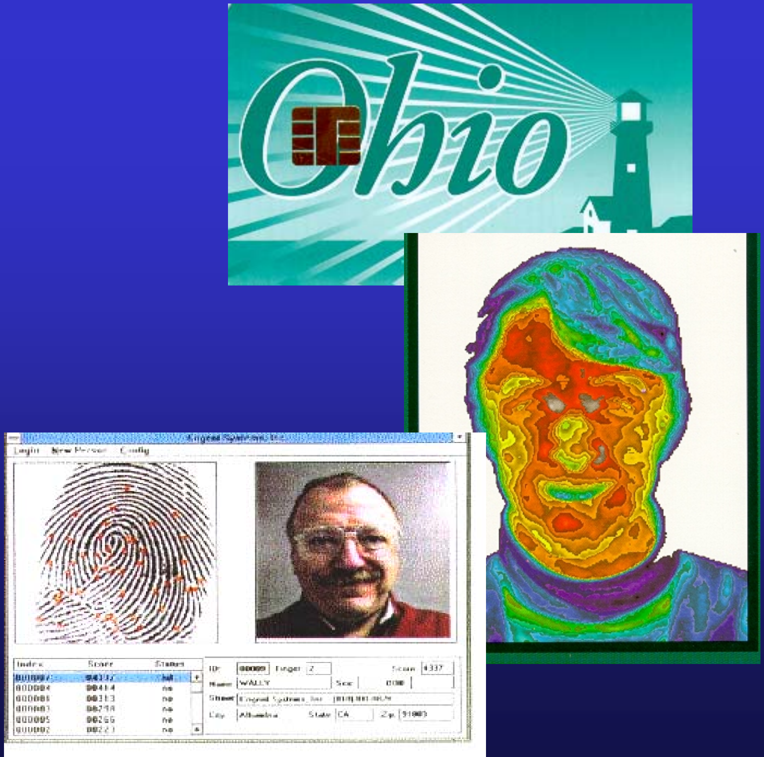
> *“…means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”*

- PIN or Password
- Digitized image of a handwritten signature
- Knowledge-based Authentication
- Biometric Profile
- Click through on software program’s dialog box
- Typed names
- Digital Signature or other encrypted authentication system

Electronic Signature requires some degree of authentication

E-Authentication Enabling Technologies

- Smart Cards - Card-Based Data Sharing
- Internet - Network-Based Data Sharing
- Identity Authentication
  - PINs
  - Biometrics
  - Public Key Infrastructure



Security Needs Met by PKI

- Authentication: *Is originator who they really say they are?*
  - Achieved by binding the sender's identity credentials to the message (digital signature)

- Data Integrity: *Has message/transaction been accidentally or maliciously been altered?*
  - Achieved via comparing hash of the data (digital signature)

- Confidentiality: *Can message be read only by authorized entities?*
  - Encryption protects information from unauthorized disclosure

- Non-repudiation: *Can sender or receiver dispute that message was actually sent or received?*
  - Enabled through digital signature process

Why build a Federal PKI?

- Statutory mandates for e-government and implementing electronic signature technology
- Business Demands for improved services at lower cost
- Leverage infrastructure costs
- Critical security need

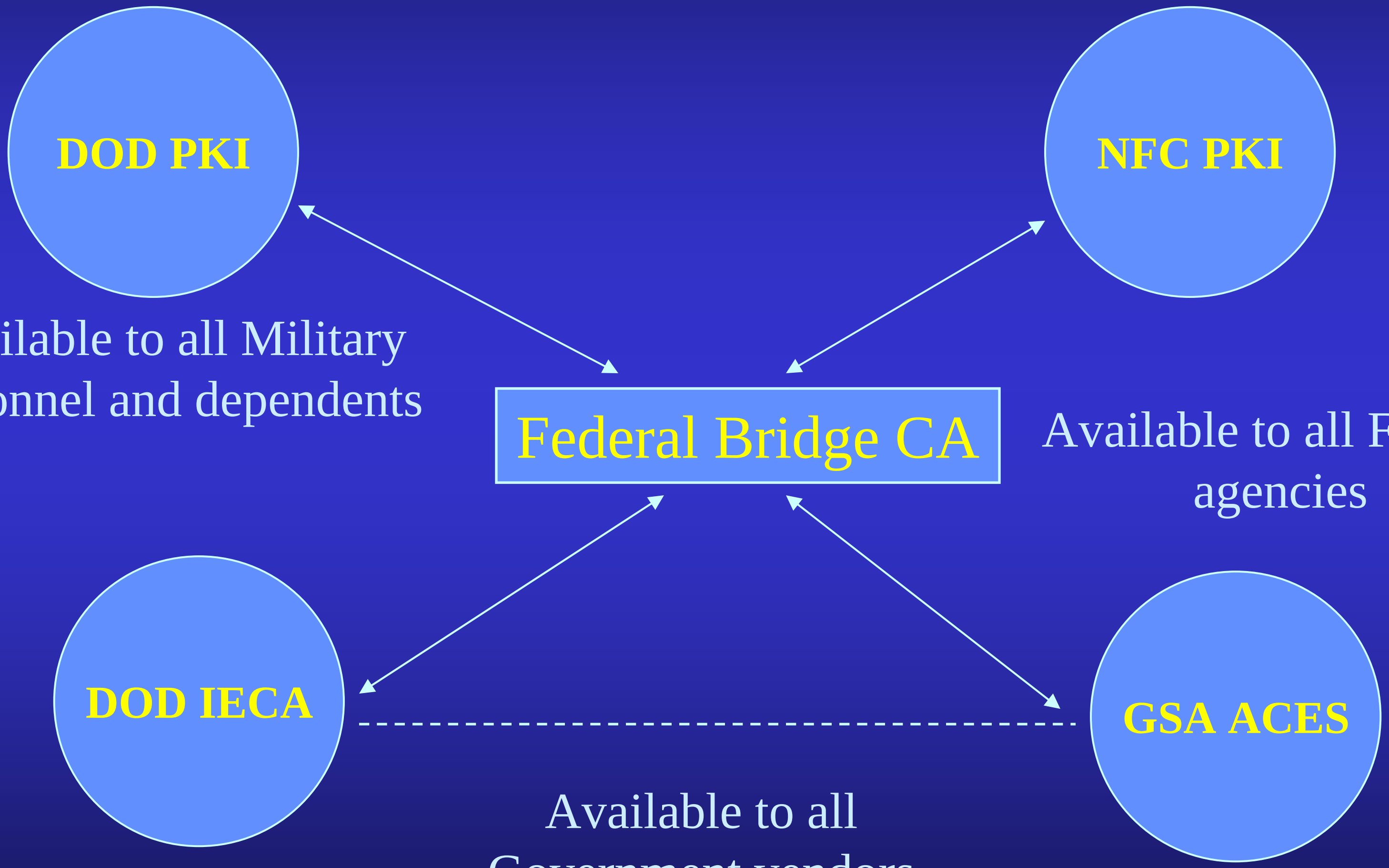
Why not a Federal PKI?

- Privacy concerns
- Agency internal politics
- Vendor battles for market space
- Cost

Federal PKI Approach

- Determine need for PKI through risk assessment.
- Use PKI when electronic signature and document/data integrity must be assured (non-repudiation).
- Provide Federal PKI and PKI services contract for government-wide use -- ACES.
- Build Federal PKI Interoperability
  - Establish Federal PKI Policy Authority (for policy interoperability).
  - Implement Federal Bridge CA using COTS (for technical interoperability).
- Organize federal agency PKI use around common citizen and industry groups.

The Federal PKI



DOD PKI

NFC PKI

Available to all Military
personnel and dependents

Federal Bridge CA

Available to all Federal
agencies

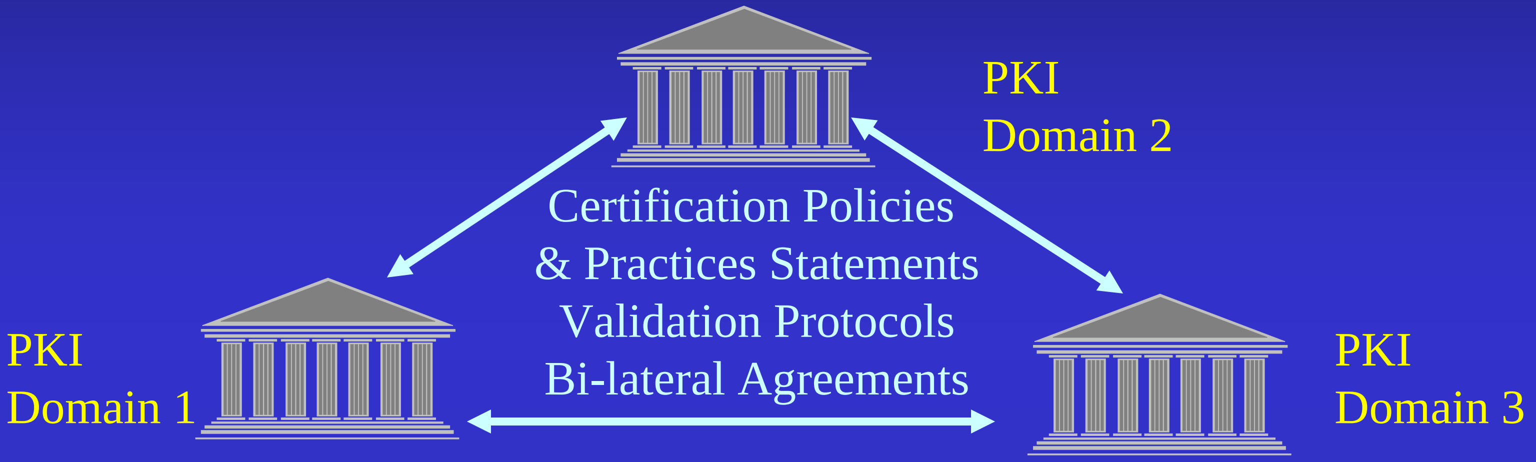
DOD IECA

GSA ACES

Available to all
Government vendors
and contractors

Available to all U.S.
citizens, businesses,
government agencies

PKI Interoperability



PKI
Domain 2

Certification Policies
& Practices Statements
Validation Protocols
Bi-lateral Agreements

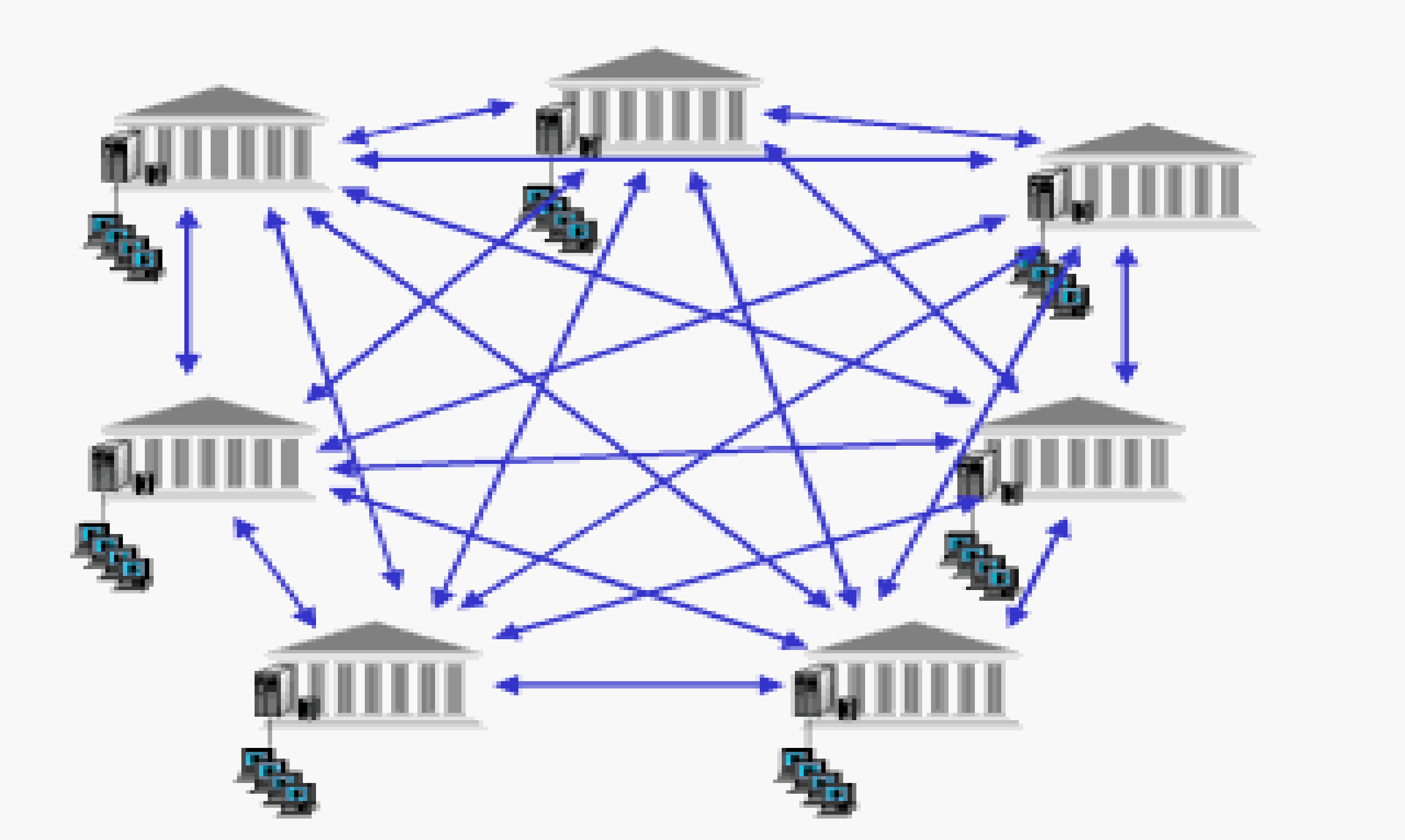
PKI
Domain 1

PKI
Domain 3

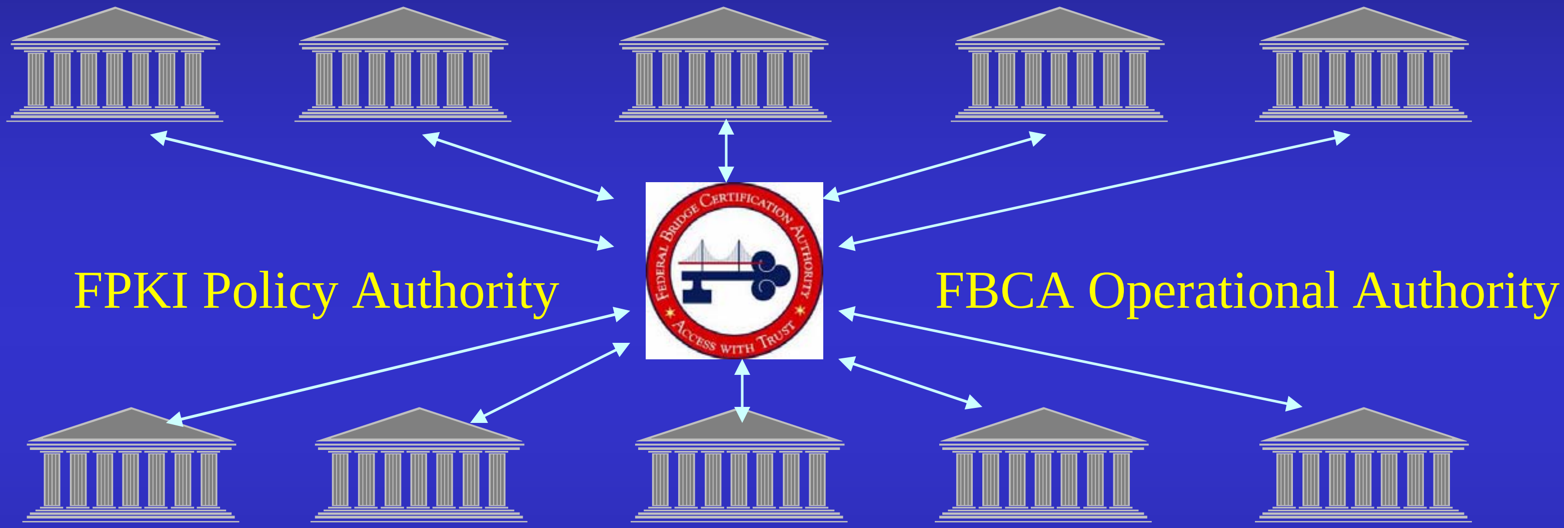
- Policy PKI Interoperability involves the determination of “Trusted” PKI domains which will meet the level of assurance needed.
- Technical PKI interoperability involves the validation of certificates form a different PKI domain to determine validity of certificates and paths.
- A small number of PKI domains makes it easier to achieve interoperability -- however it is still complex.

The Challenge to PKI Interoperability

PKI interoperability becomes much more complex as the number of PKI domains increase.



The Solution: The Federal Bridge CA



FPKI Policy Authority

FBCA Operational Authority

The Federal Bridge CA simplifies PKI interoperability:

- Common and easy way to determine “Trusted” PKI domains and assurance levels (policy mapping);
- Common and, relatively, easy way to validate certificate status through cross certification;
- Standard Bi-lateral Agreement between the Bridge and Agency CA.

PKI Policy Mapping -- Equivalence Example

FBCA Requirements	NFC PKI	DOD PKI	DOD IECA PKI	ACES PKI
FBCA High	NFC PKI High	DoD 4		
FBCA Medium	NFC PKI Medium)	DoD 3	DoD IECA (Med)	GSA ACES (Med)
FBCA Basic	NFC PKI Basic	DoD 2		
FBCA Rudimentary	NFC PKI Test			

PKI ACES
Access Certificates for Electronic Services
Securing the Business of Government

ACES Program Vision

- Common PKI solution encourages agencies to work together
- Allows equitable cost sharing among agencies
- Efficient, effective, economical due to aggregation of Federal needs
- One digital identity credential can be used by multiple Agency processes
- “Anonymous” certificate numbering for identification
- Public pays nothing for digital ID.

Who Can Be a Member of the ACES PKI?

- Certificate Authorities
  - ACES contractors

- Relying Parties
  - Any Federal agency
  - Non-federal entities if authorized by a Federal Agency for legitimate program purposes.

- Subscribers
  - Any individual in U.S.
  - Any individual as a representative of a business, organization, or governmental entity

For More Information

Phone

David Temoshok
202-208-7655

E-mail

david.temoshok@gsa.gov

Websites

http://cio.gov/fpkisc
http://gsa.gov/ACES
http://ec.fed.gov