ActivCard®

ActivCard®

US Federal PKI Bridge

Ram Banerjee
VP Vertical Markets

e-Gov and PKI Drivers

ActivCard

- Government Paperwork Elimination and ESIGN Acts
- Public Expectations
- Long-term Cost Savings
- The Need for Privacy and Security
  - Government is held to higher standard
- Trading Partner Practices

Business Driver: Savings by Process Type

ActivCard

	Traditional System	Internet	Percent Savings
Bill Payment	$2.22 - $3.32	$0.65 - $1.10	71% - 67%
Insurance Policy	$400 - $700	$200 - $350	50%
Software Distribution	$15	$0.20 - $0.50	97% - 67%
Procurement			70%
Motor Vehicle Registration	$7	<$2	71%
Order-Filling (DOD)	$24	$12	50%

Electronic Signatures in Global and National Commerce Act

ActivCard

- Signed by President Clinton on 6/30/00.
- E-SIGN addresses:
  - Commercial, consumer, and business transactions affecting interstate or foreign commerce
  - Legality of electronic signatures and records
  - Preemption of inconsistent statutes/rules
- E-SIGN does not address
  - Security, authentication, or records requirements
  - Interoperability
  - Electronic signatures based on different technologies
  - Rules for reliance/accepting different kinds of signatures

GPEA Requirements

ActivCard

- Federal Agency activities and requirements are generally not within the scope of this legislation; they are instead addressed by the Government Paperwork Elimination Act (GPEA)

- **GPEA of 1998 addresses:**
  - requirement for federal agencies to offer the public the option of electronic filings/transactions/record-keeping for agency business by October 2003
  - Legality of electronic signatures and records
  - Technology neutrality -- electronic signature alternatives

Issues with a U.S. Federal PKI

ActivCard

For

- Statutory mandates for e-government and implementing electronic signature technology
- Demands for improved services at lower cost
- International Competition
- International Collaboration

Against

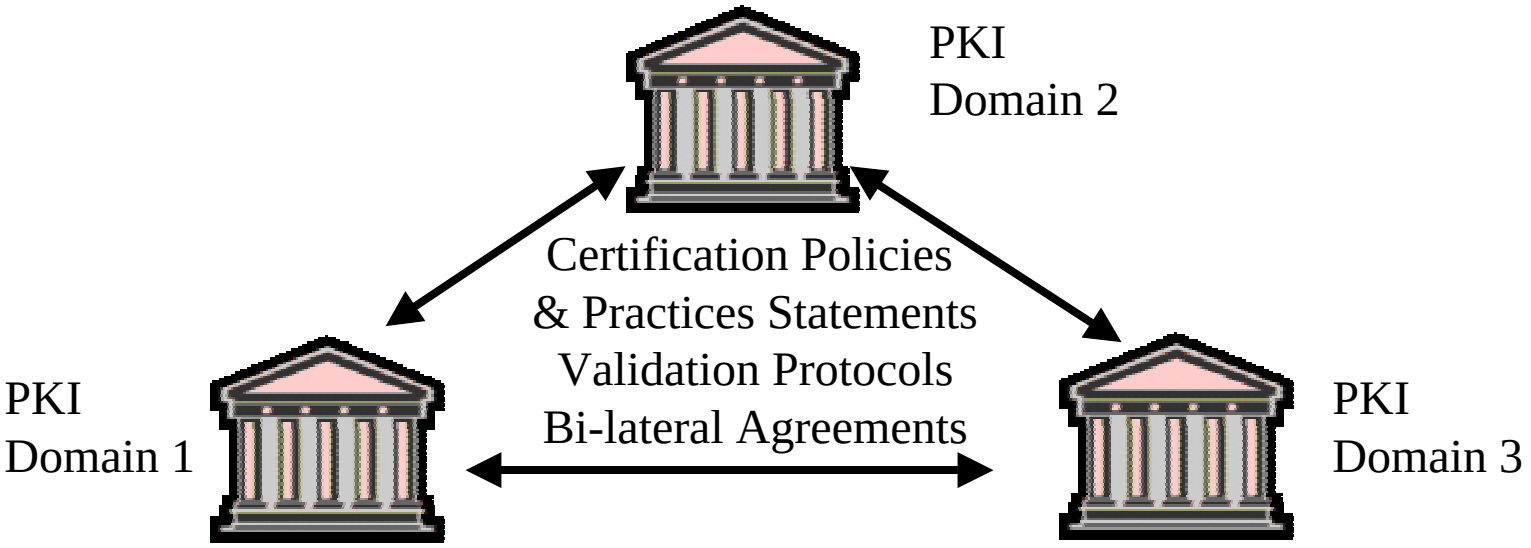
- Concerns of Privacy Advocates
- Agency internal politics
- Vendor battles for market space
- Cost

The Approach to a U.S. Federal PKI

ActivCard

- Agencies implement their own PKIs
- Create a Federal Bridge CA using COTS products to bind Agency PKIs together
- Establish a Federal PKI Policy Authority to oversee operation of the Federal Bridge CA
- Ensure directory compatibility
- Use Access Certs for Electronic Services (ACES) for transactions with the public

PKI Interoperability

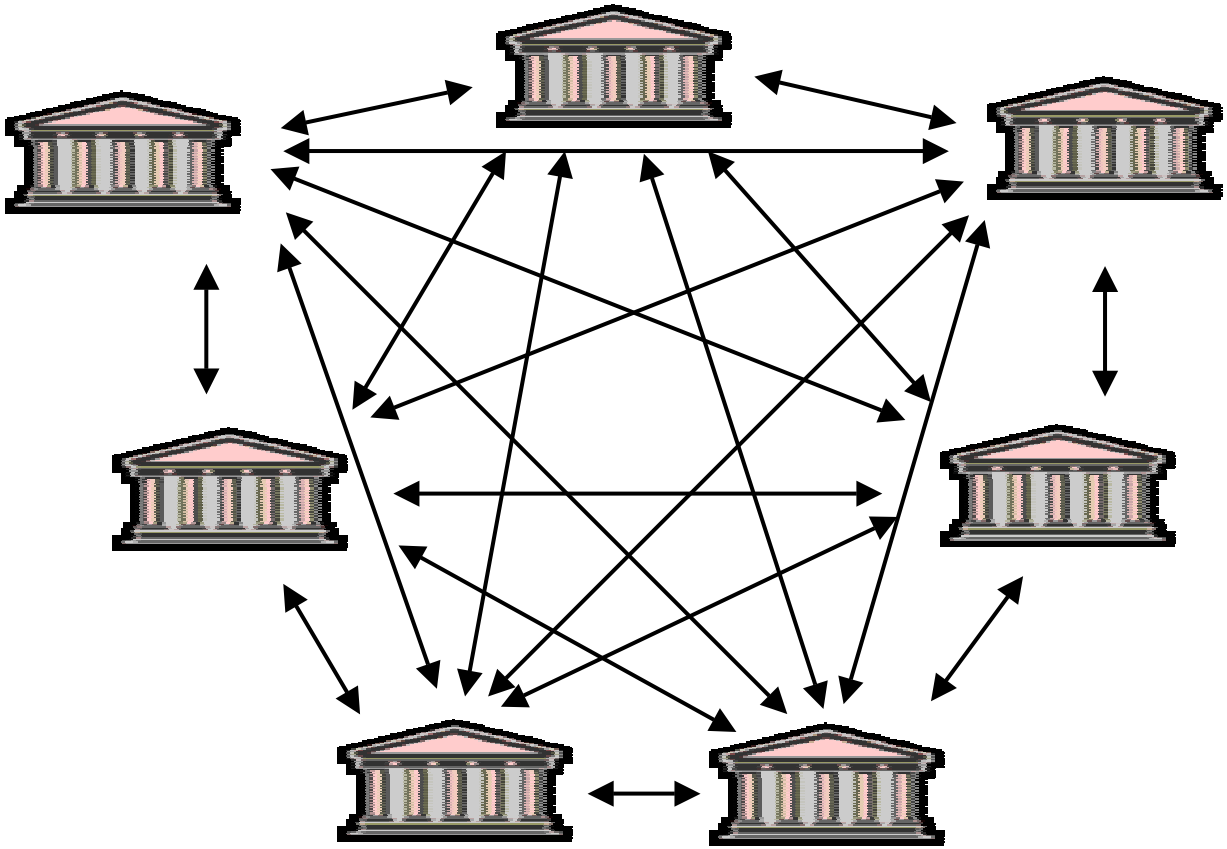


- Policy PKI Interoperability involves the determination of "Trusted" PKI domains which will meet the level of assurance needed.
- Technical PKI interoperability involves the validation of certificates form a different PKI domain to determine validity of certificates and paths.
- A small number of PKI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

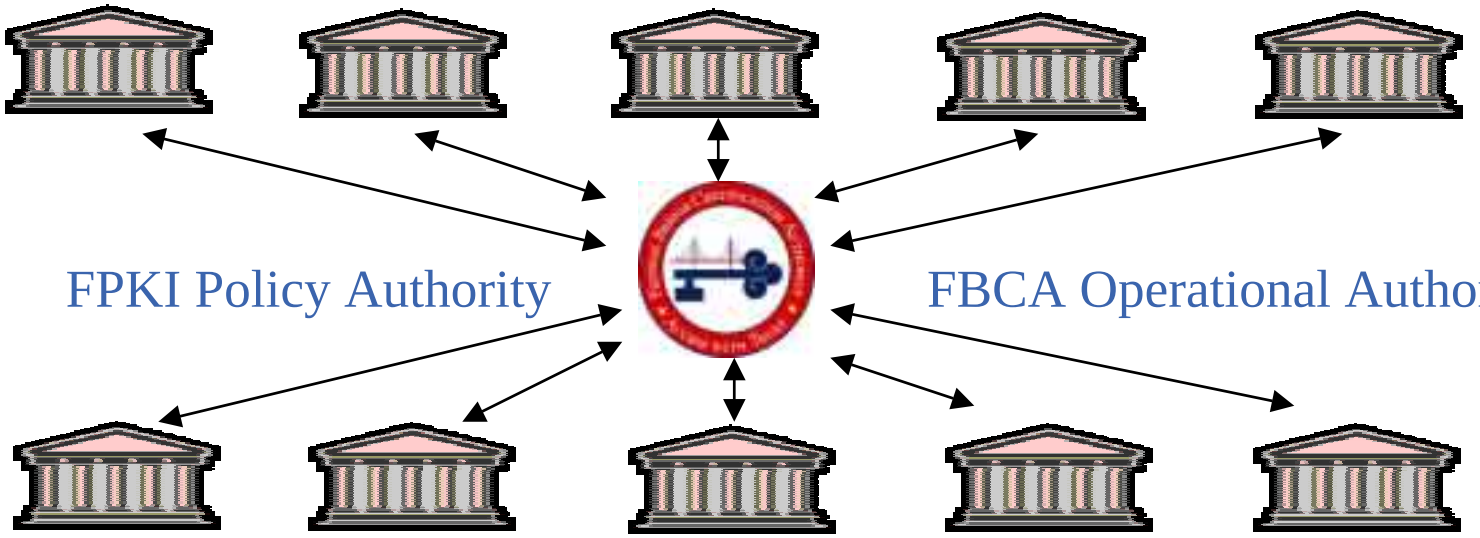
The Challenge to PKI Interoperability

ActivCard

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



Non hierarchical HUB



- 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

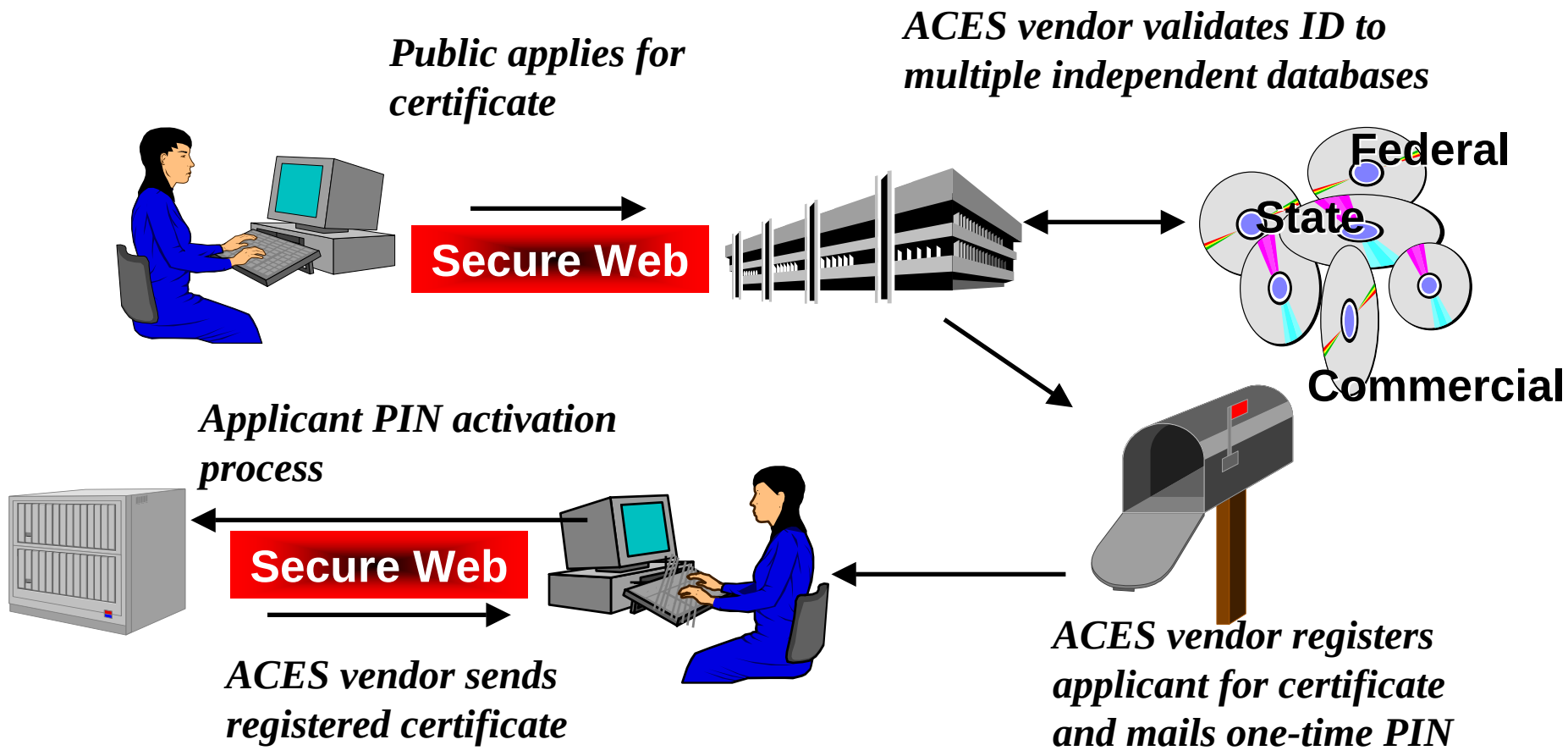
Access Certs for Electronic Services

ActivCard

- “No-cost” certificates for the public
- For business with Federal agencies only (but agencies may allow other uses on case basis)
- On-line registration, vetting with legacy data; information protected under Privacy Act
- Regular mail one-time PIN to get certificate
- Agencies billed per-use and/or per-certificate

ACES Remote (On-line) Certificate Application Process

ActivCard



Accessing Web-Based Applications and Services

ActivCard

Citizen

Access Authorized System with ACES authentication

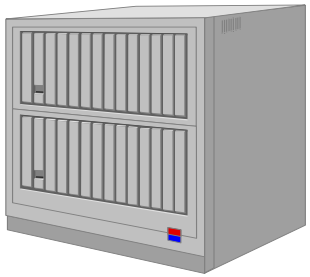
Secure Web

Return Personalized Services/Benefits/ Information

Federal Agency

Authorized Web-based Application

Validate Electronic ID (ACES) through standard on-line protocol (OCSP)



ACES Contracted Certificate Authority

PKI and Smart Cards

ActivCard

- Securely store, protect, and transport multiple cryptographic keys (public/private keys) and digital certificates
- Provide secure computational and processing facility without exposing sensitive information
- Provides security for:
  - generation of digital signature
  - use of private key for personal authentication, portable permissions/logical access control
- Convenience for end user
- PKI can be one set of functions on a multi-application smart card
- Uniquely identify the user through PIN/Biometric

References

ActivCard

- Federal PKI Steering Committee Website: http://www.cio.gov/fpkisc
- NIST PKI Website: http://csrc.nist.gov/pki
- GSA Website: http://www.gsa.gov/ACES
- ANSI Website: http://www.ansi.org