HSPD-12 : The Role of Federal PKI

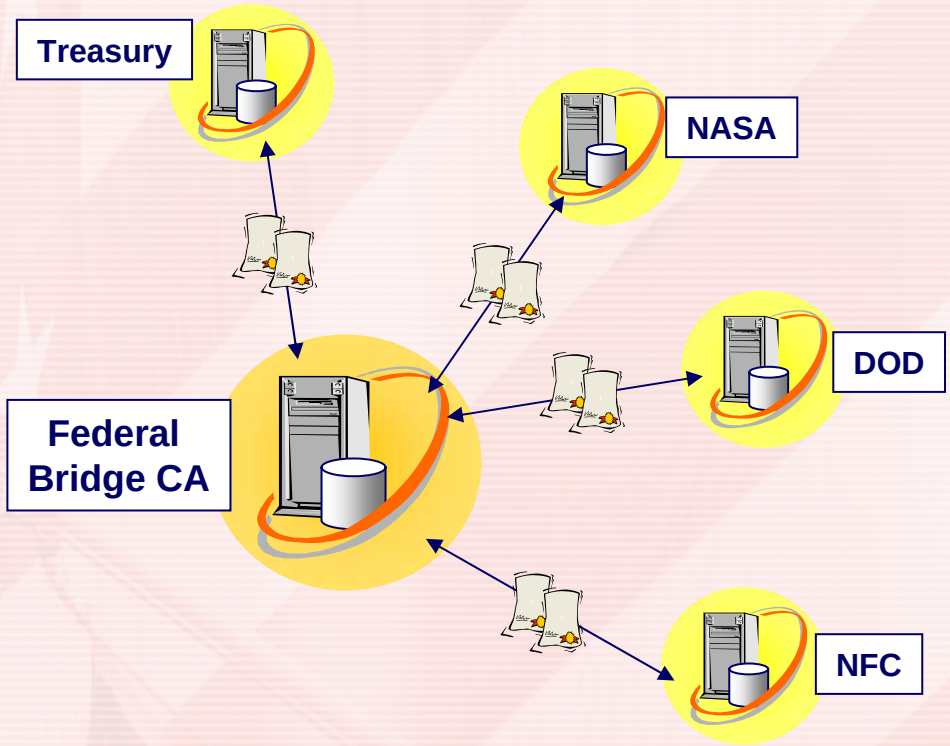
Judith Spencer
Chair, Federal Identity Credentialing
Office of Governmentwide Policy
General Services Administration
judith.spencer@gsa.gov

How We Got Here

- 2005 – FIPS-201 Released
- 2004 – HSPD-12 signed by President Bush
- 2003 – *E-Authentication Guidance for Federal Agencies* released by OMB/Federal Identity Credentialing Initiative launched
- 2002 – E-Authentication Initiative launched
- 2002 – Federal Bridge CA cross-certifies first 4 Federal agencies
- 2000 – E-Sign Act signed electronically in Philadelphia/*Evolving Federal PKI* Issued
- 1997 – *Access America* identifies identity assurance/information security as a key enabler for e-Government
- 1994 – Federal PKI Steering Committee launched

Federal Bridge Certification Authority

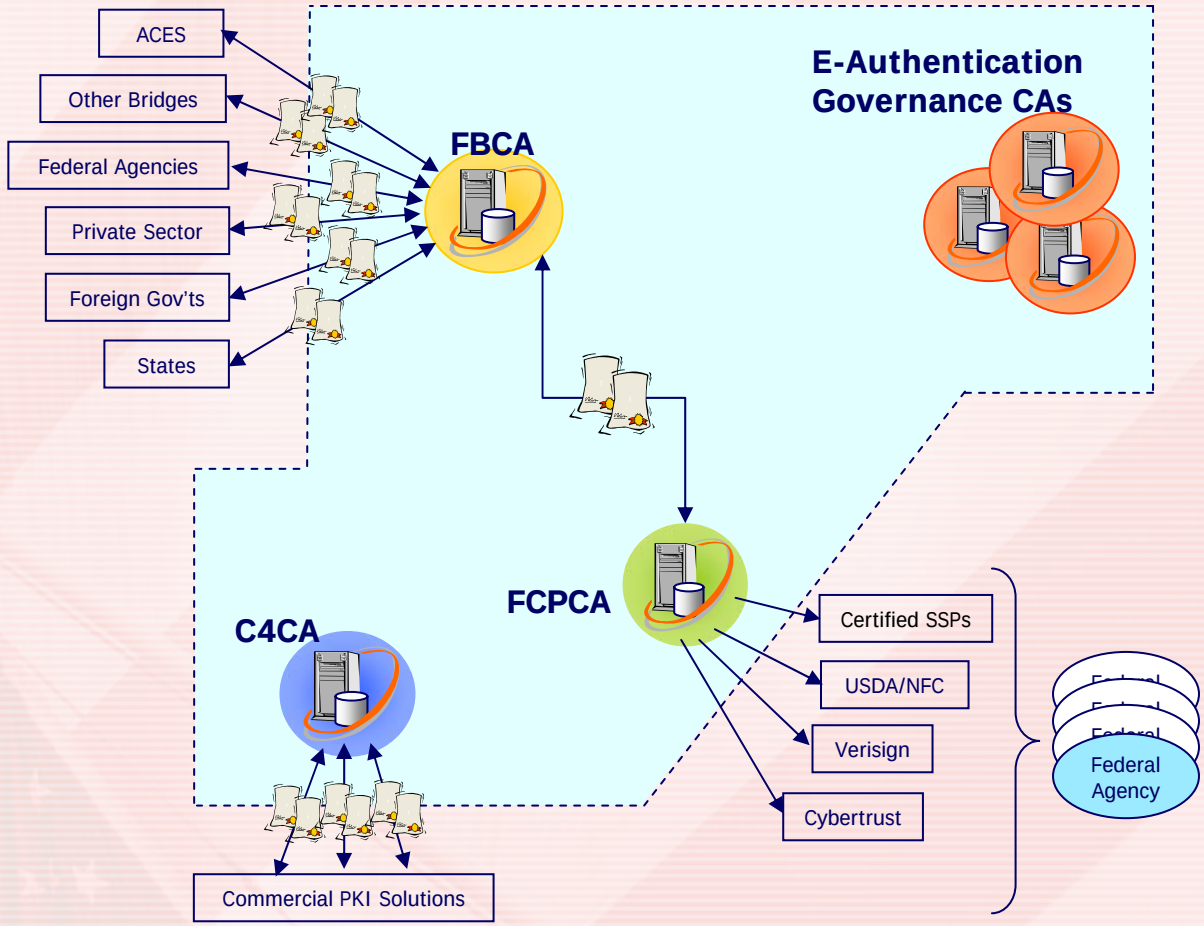
Circa: 2002



The Federal PKI Architecture

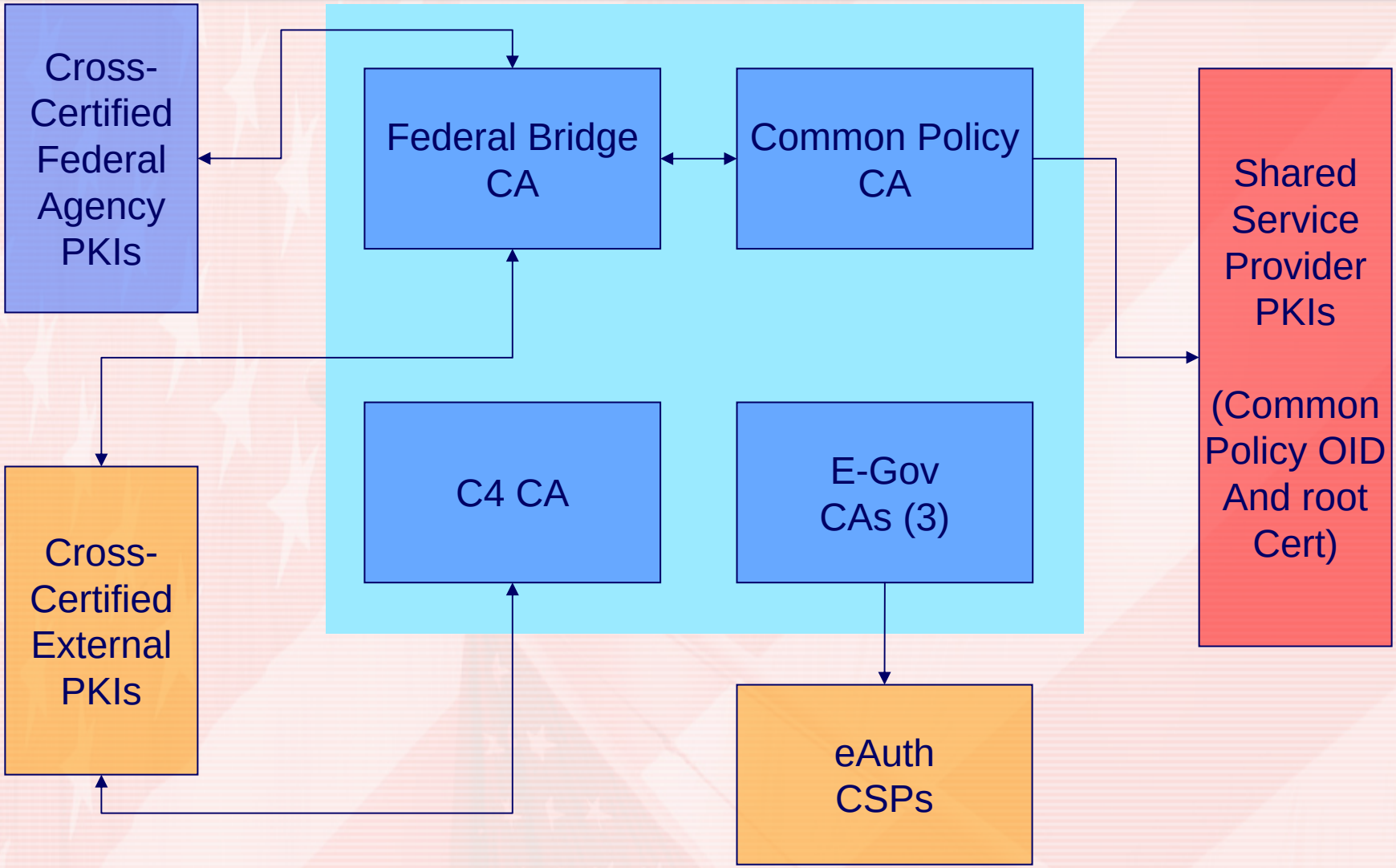
Four Primary Components

- Federal Bridge Certification Authority
- Citizen and Commerce Certification Authority
- Federal Common PKI Certification Authority
- E-Authentication Governance Certification Authority

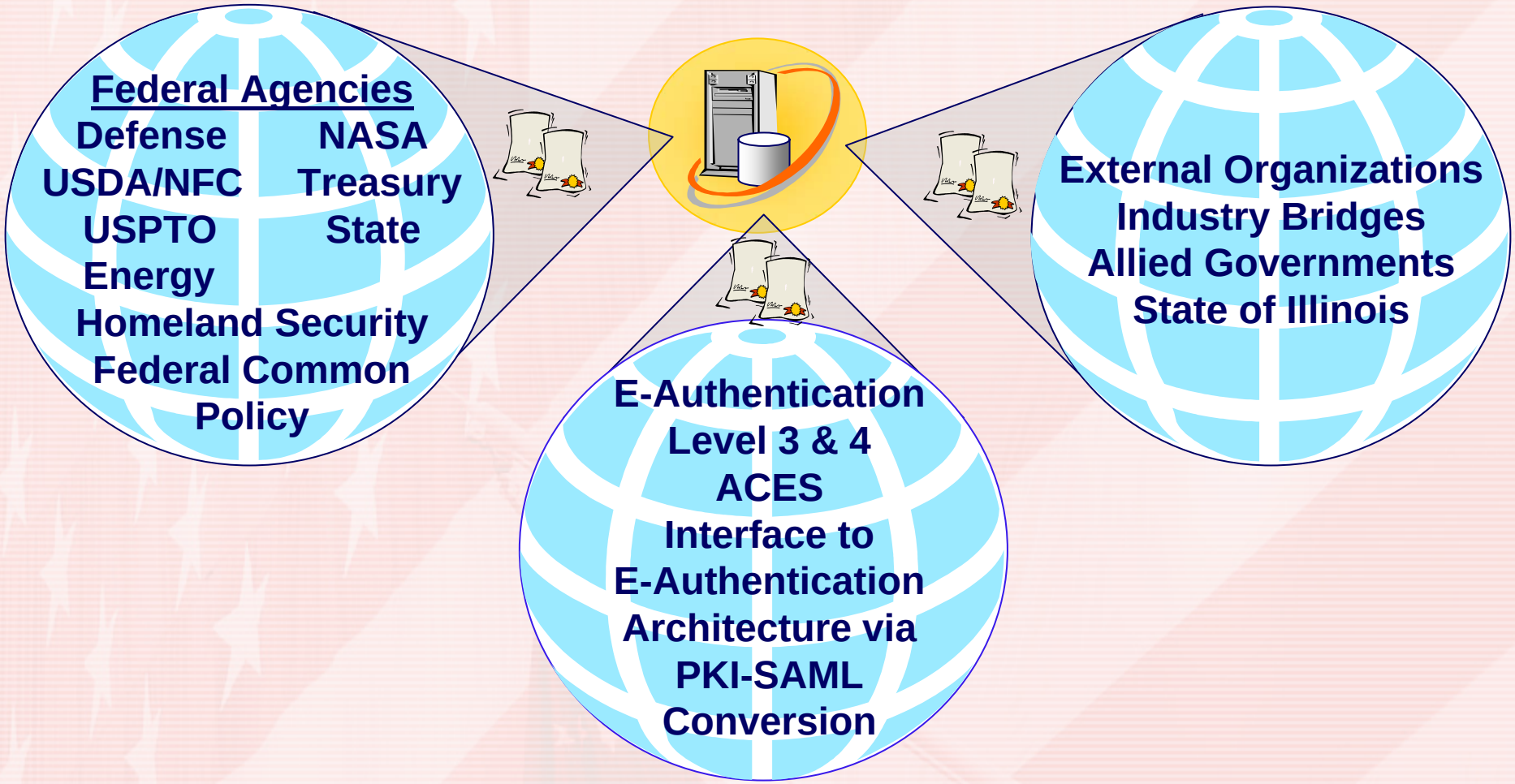


Circa: 2006

Federal PKI Block Diagram



The World According to Bridge



Federal Bridge Today

- FBCA originally conceived as an interoperability mechanism for Federal organizations
- It is now recognized as an interoperability mechanism between Federal organizations and the private sector, states, academia, and allied governments.

International Interoperability

- Canada – Final stages of cross-certification currently underway with Government of Canada
- United Kingdom – Discussions underway with UKMOD for cross-certification
- Australia – Pursuing mutual recognition initiative with Australian Government Information Management Office (AGIMO)
- Asia-Pacific Economic Cooperation – Participation in E-Security Task Group National PKI Mapping initiative
- European Telecommunications Standards Initiative (ETSI) – Completed Mapping of TS101456, *Policy requirements for certification authorities issuing qualified certificates,* & FBCA CP
- Transatlantic Secure Collaboration Program

Bridge to Bridge Interoperability

- 2003 – NIH & Higher Ed conduct demonstration project to determine technical feasibility of Bridge-to-Bridge interoperability
- 2004 – Aerospace Industry embarks on Certipath Bridge
- 2004 – Pharmaceutical Industry announces SAFE Bridge
- 2005 – Federal PKI and Certipath begin Cross-Certification activities
- First Bridge-to-Bridge Cross-Certification expected in 2006.
- Issues:
  - Reliable Path Discovery & Validation capabilities
  - Reliable Name constraints

PMC E-Government Agenda

Government to Citizen

1. USA Service
2. EZ Tax Filing
3. Online Access for Loans
4. Recreation One Stop
5. Eligibility Assistance Online

Government to Business

1. Federal Asset Sales
2. Online Rulemaking Management
3. Simplified and Unified Tax and Wage Reporting
4. Consolidated Health Informatics
5. Business Compliance 1 Stop
6. Int'l Trade Process Streamlining

Government to Govt.

1. e-Vital (business case)
2. e-Grants
3. Disaster Assistance and Crisis Response
4. Geospatial Information One Stop
5. Wireless Networks

Internal Effectiveness and Efficiency

1. e-Training
2. Recruitment One Stop
3. Enterprise HR Integration
4. e-Travel
5. e-Clearance
6. e-Payroll
7. Integrated Acquisition
8. e-Records Management

Determining Assurance Levels

- *E-Authentication Guidance for Federal Agencies*, issued by the Office of Management & Budget, Dec. 16, 2003
  - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
  - About identity authentication, not authorization or access control
  - Incorporates Standards for Security Categorization of Federal Information and Information Systems (FIPS-199)
- NIST SP800-63: *Recommendation for Electronic Authentication*
  - Companion to OMB e-Authentication guidance
  - http://csrc.nist.gov/eauth
  - Covers conventional token based remote authentication

Assurance Levels

M-04-04:E-Authentication Guidance for Federal Agencies

OMB Guidance establishes 4 authentication assurance levels

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity	Some confidence in asserted identity	High confidence in asserted identity	Very high confidence in the asserted identity
Self-assertion minimum records	On-line, instant qualification – out-of-band follow-up	On-line with out-of-band verification for qualification Cryptographic solution	In person proofing Record a biometric Cryptographic Solution Hardware Token

Maximum Potential Impacts

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

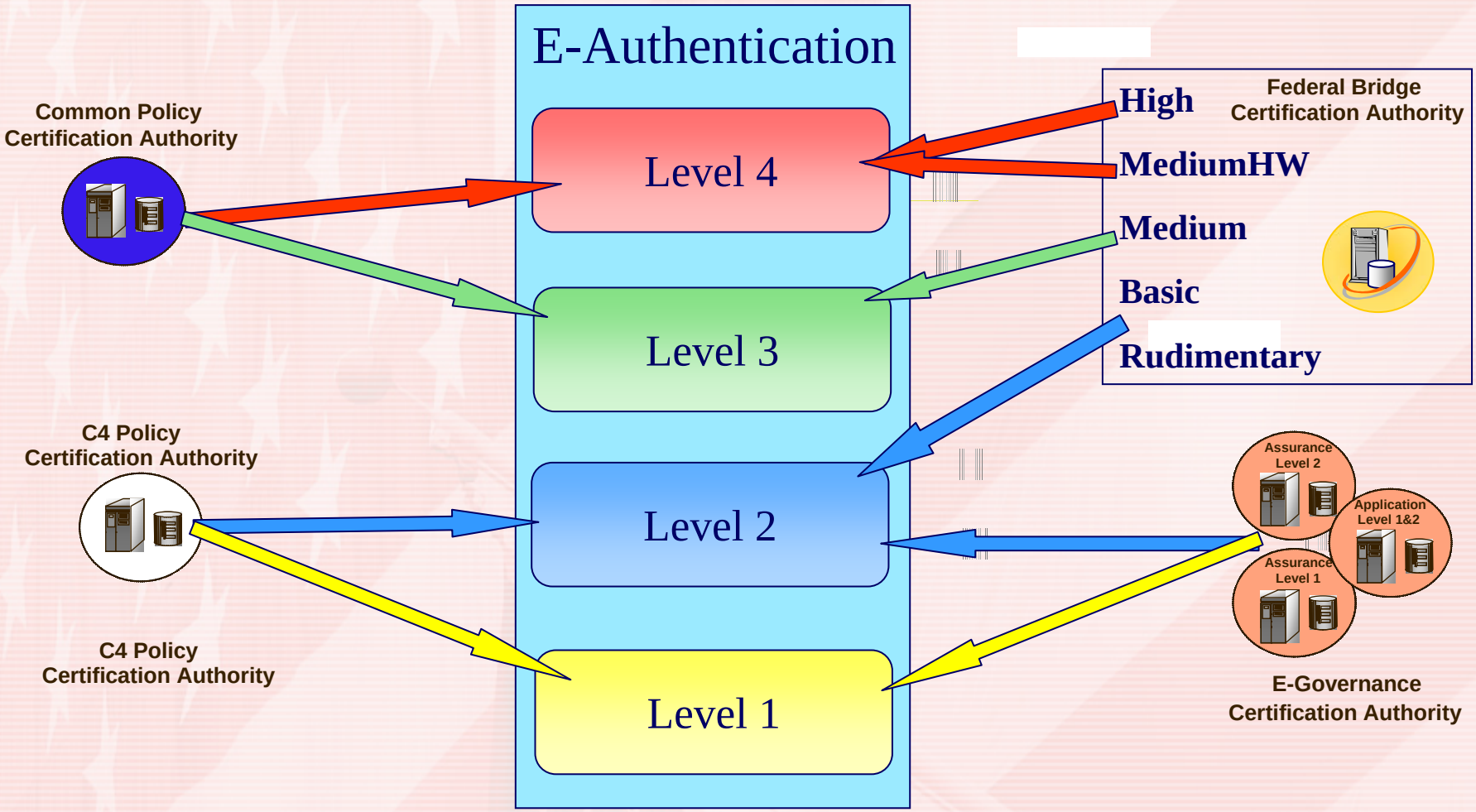
Token Type by Level

	Assurance Level			
Allowed Token Types	1	2	3	4
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
Zero knowledge password	√	√	√	
One-time Password Device	√	√	√	
Strong password	√	√		
PIN	√			

One Size Does NOT Fit All
FBCA Policy – Levels of Assurance

- Defines 4 levels of Assurance
  - Rudimentary – Several areas undefined
  - Basic – Allows on-line identity assurance
  - Medium – Requires in-person antecedent
  - Medium (hardware) – same as medium using hardware token
  - High – Requires in-person and hardware token
- Cross-walk to E-Authentication Guidance for Federal Agencies
  - FBCA Rudimentary = E-Authentication Level 1 or 2
  - FBCA Basic = E-Authentication Level 3
  - FBCA Medium (software) = E-Authentication Level 3
  - FBCA Medium Commercial Best Practices (software) = E-Authentication Level 3
  - FBCA Medium (hardware) = E-Authentication Level 4
  - FBCA Medium Commercial Best Practices (hardware) = E-Authentication Level 4
  - FBCA High = E-Authentication Level 4

FPKI to E-Authentication



PMC E-Government Agenda

Government to Citizen

1. USA Service
2. EZ Tax Filing
3. Online Access for Loans
4. Recreation One Stop
5. Eligibility Assistance Online

Government to Business

1. Federal Asset Sales
2. Online Rulemaking Management
3. Simplified and Unified Tax and Wage Reporting
4. Consolidated Health Informatics
5. Business Compliance 1 Stop
6. Int'l Trade Process Streamlining

Government to Govt.

1. e-Vital (business case)
2. e-Grants
3. Disaster Assistance and Crisis Response
4. Geospatial Information One Stop
5. Wireless Networks

Internal Effectiveness and Efficiency

1. e-Training
2. Recruitment One Stop
3. Enterprise HR Integration
4. e-Travel
5. e-Clearance
6. e-Payroll
7. Integrated Acquisition
8. e-Records Management

Assurance Levels

M-04-04:E-Authentication Guidance for Federal Agencies

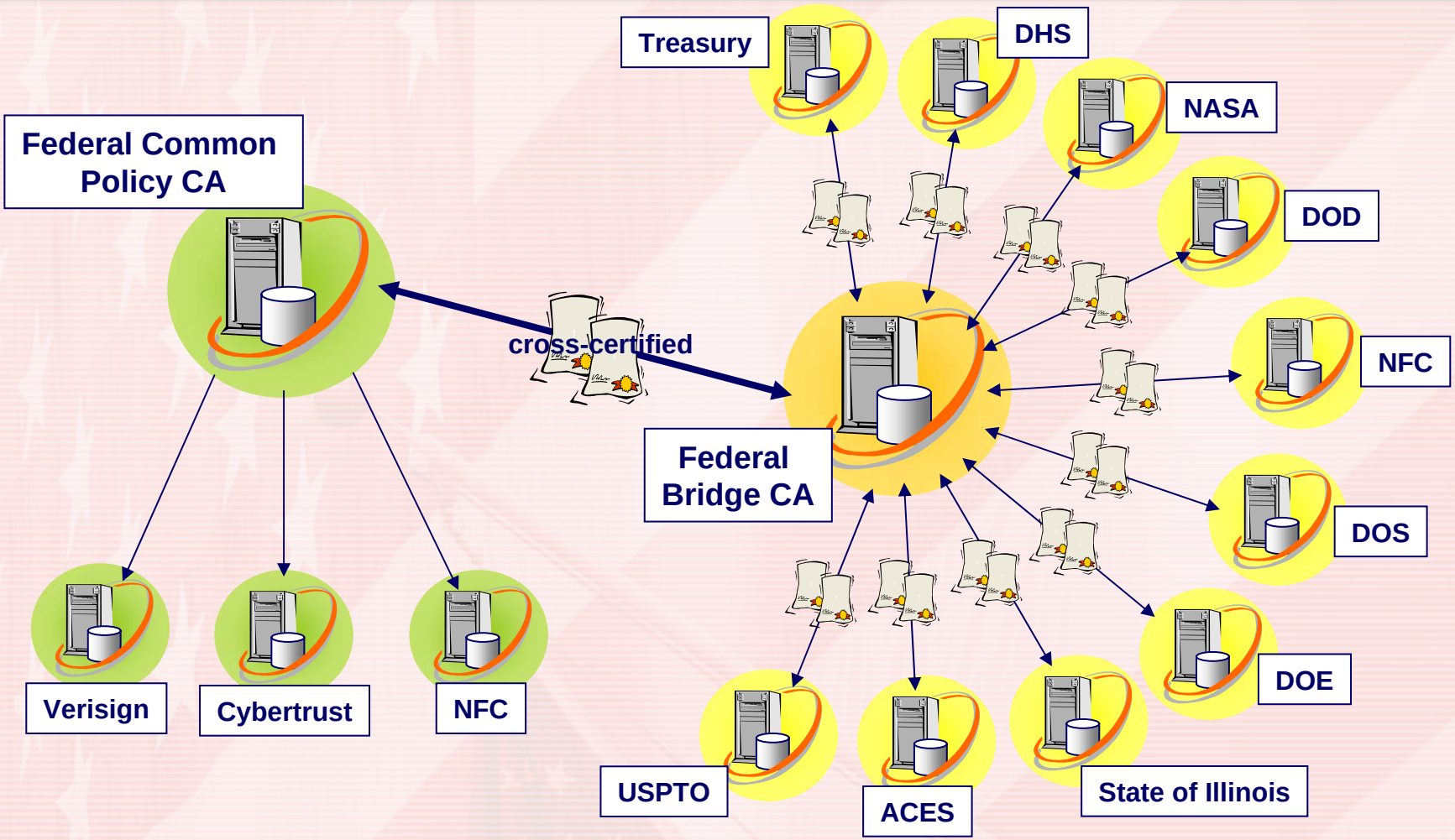
OMB Guidance establishes 4 authentication assurance levels

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity	Some confidence in asserted identity	High confidence in asserted identity	Very high confidence in the asserted identity
Self-assertion minimum records	On-line, instant qualification – out-of-band follow-up	On-line with out-of-band verification for qualification Cryptographic solution	In person proofing Record a biometric Cryptographic Solution Hardware Token

Federal Common PKI CA

- Developed in support of the Federal Identity Credentialing Initiative
- Implementation mechanism for Federal Common PKI Certificate Policy which sets minimum requirements for issuance of PKI credentials to Federal employees.
- Operates at FBCA Medium Assurance/E-Authentication Levels 3 and 4
- Cross-certified with the FBCA
- Acts as the root CA for the Shared PKI Service Provider program
- Provides E-Authentication support to the 4th Sector: Internal Effectiveness and Efficiencies.

Federal Common Policy Compliance



Implementing PKI in accordance with FIPS-201

- X.509 Certificate Policy for the Federal Common Policy Framework
  - Provides minimum requirements for Federal agency implementation of PKI
  - Operates at FBCA Medium Assurance/E-Authentication Levels 3 and 4
  - Cross-certified with the FBCA
  - Governing policy for the Shared PKI Service Provider program
- Certified PKI Shared Service Provider Program
  - Evaluates services against the Common Policy Framework
  - Conducts Operational Capabilities Demonstrations
  - Populates Certified Provider List with service providers who meet published criteria
  - Agencies not operating an Enterprise PKI must buy PKI services from certified providers

Approved Shared Service Providers

- Verisign, Inc
- Cybertrust
- Operational Research Consultants
- USDA/National Finance Center

- Agencies operating an Enterprise PKI cross-certified with the FBCA at Medium Assurance or higher are considered compliant with FIPS-201.
- In January 2008, these Enterprise PKIs will start including the Common Policy OIDs in their certificates.

PKI Decision Making for HSPD-12