


The background of the slide is a close-up, slightly blurred image of the American flag, showing the stars and stripes. The flag is oriented vertically, with the stars in the upper left and the stripes extending downwards.

# HSPD-12 : Defining a Federal PKI Framework

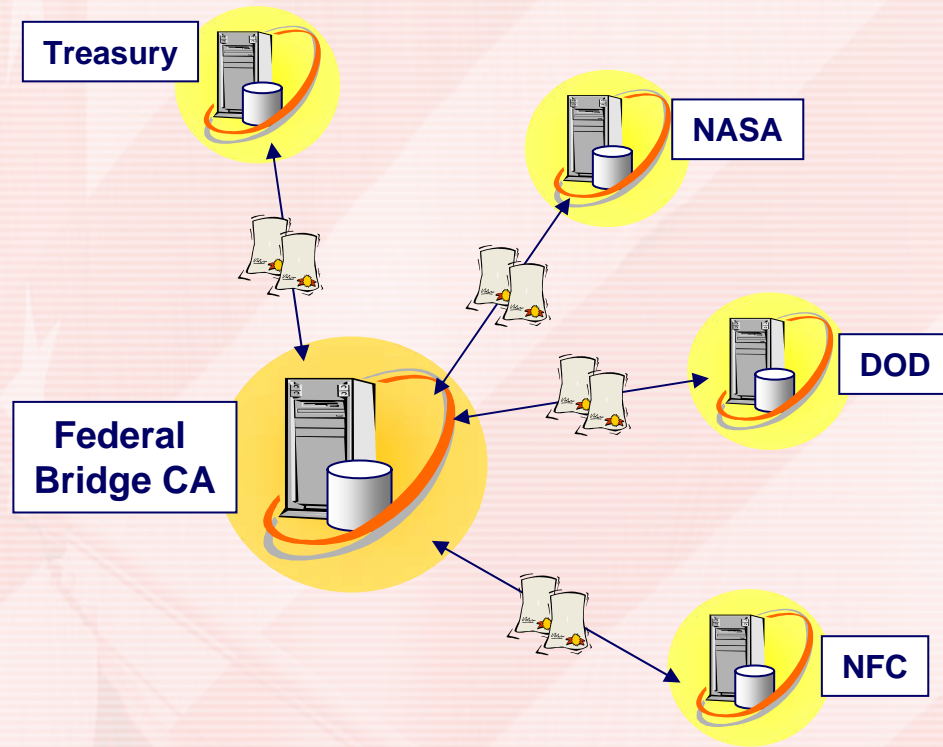
Judith Spencer  
Chair, Federal Identity Credentialing  
Office of Governmentwide Policy  
General Services Administration  
[judith.spencer@gsa.gov](mailto:judith.spencer@gsa.gov)

# How We Got Here

- 
- 2005 – FIPS-201 Released
  - 2004 – HSPD-12 signed by President Bush
  - 2004 – PKI Shared Service Provider Certification Program launched
  - 2003 – *E-Authentication Guidance for Federal Agencies* released by OMB
  - 2003 – Federal Common PKI Policy released.
  - 2003 – 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
  - 1997 – *Access America* identifies identity assurance/information security as a key enabler for e-Government

# Federal Bridge Certification Authority

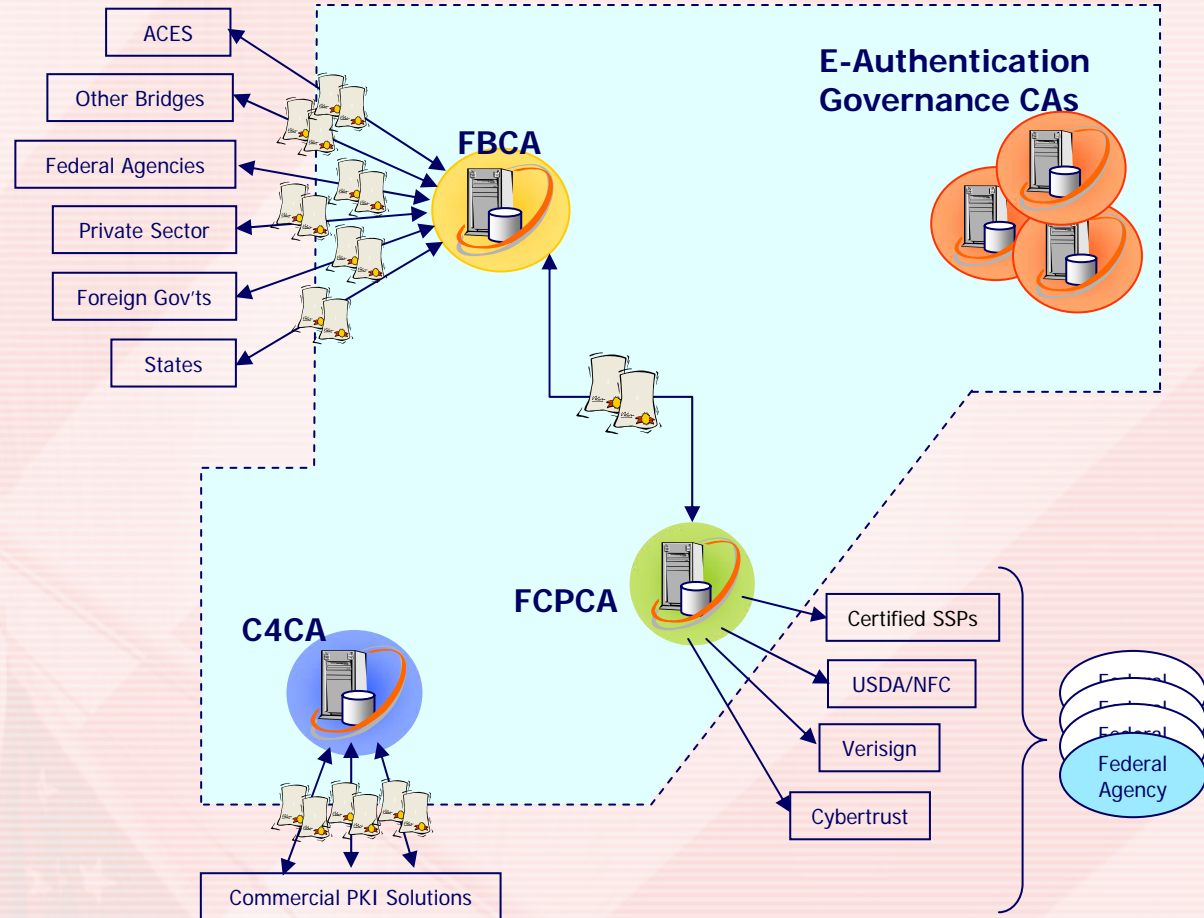
Circa: 2002



# The Federal PKI Architecture

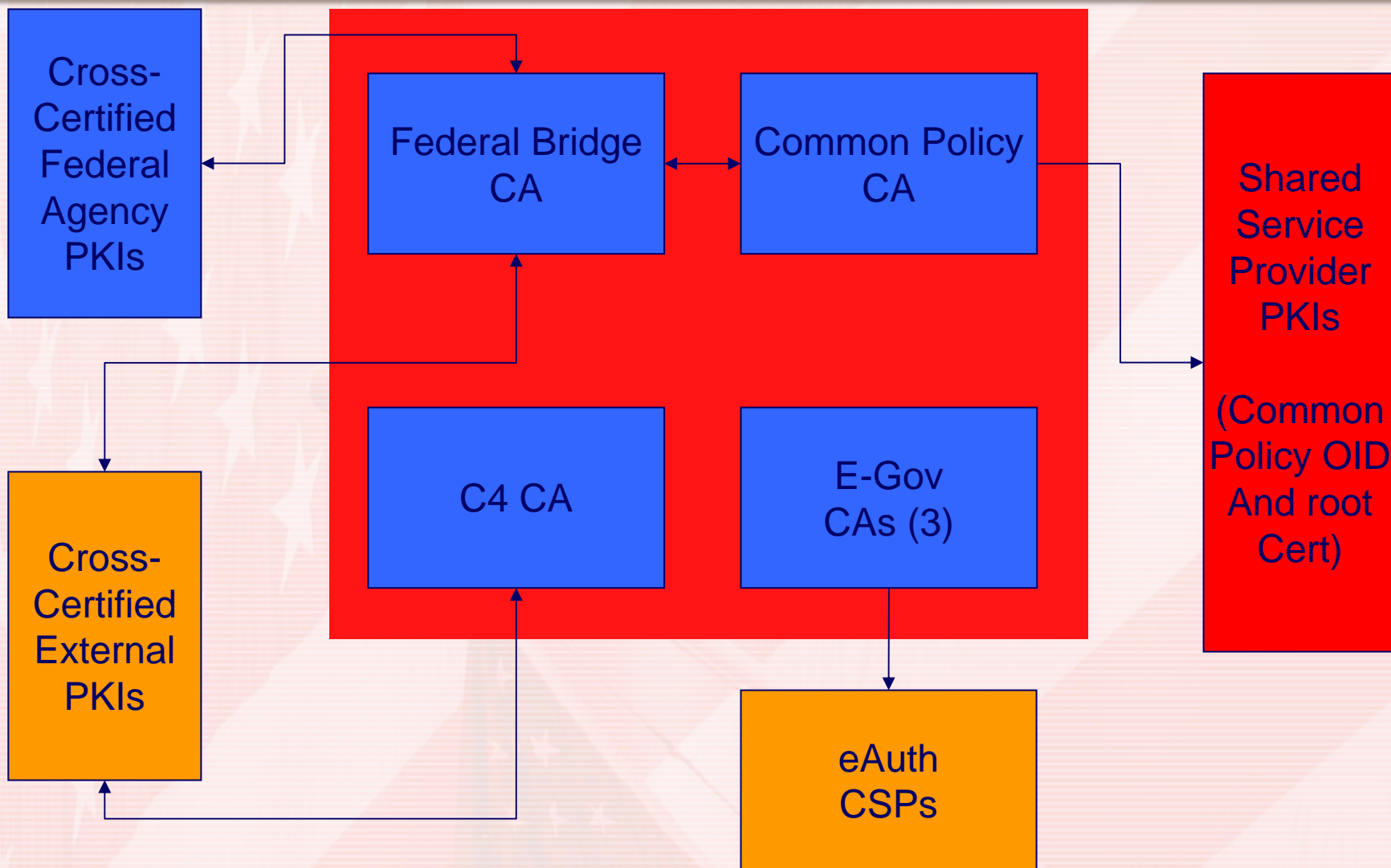
## Four Primary Components

- 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



# 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

# 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

# Token Type by Level

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

# Assurance Levels

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

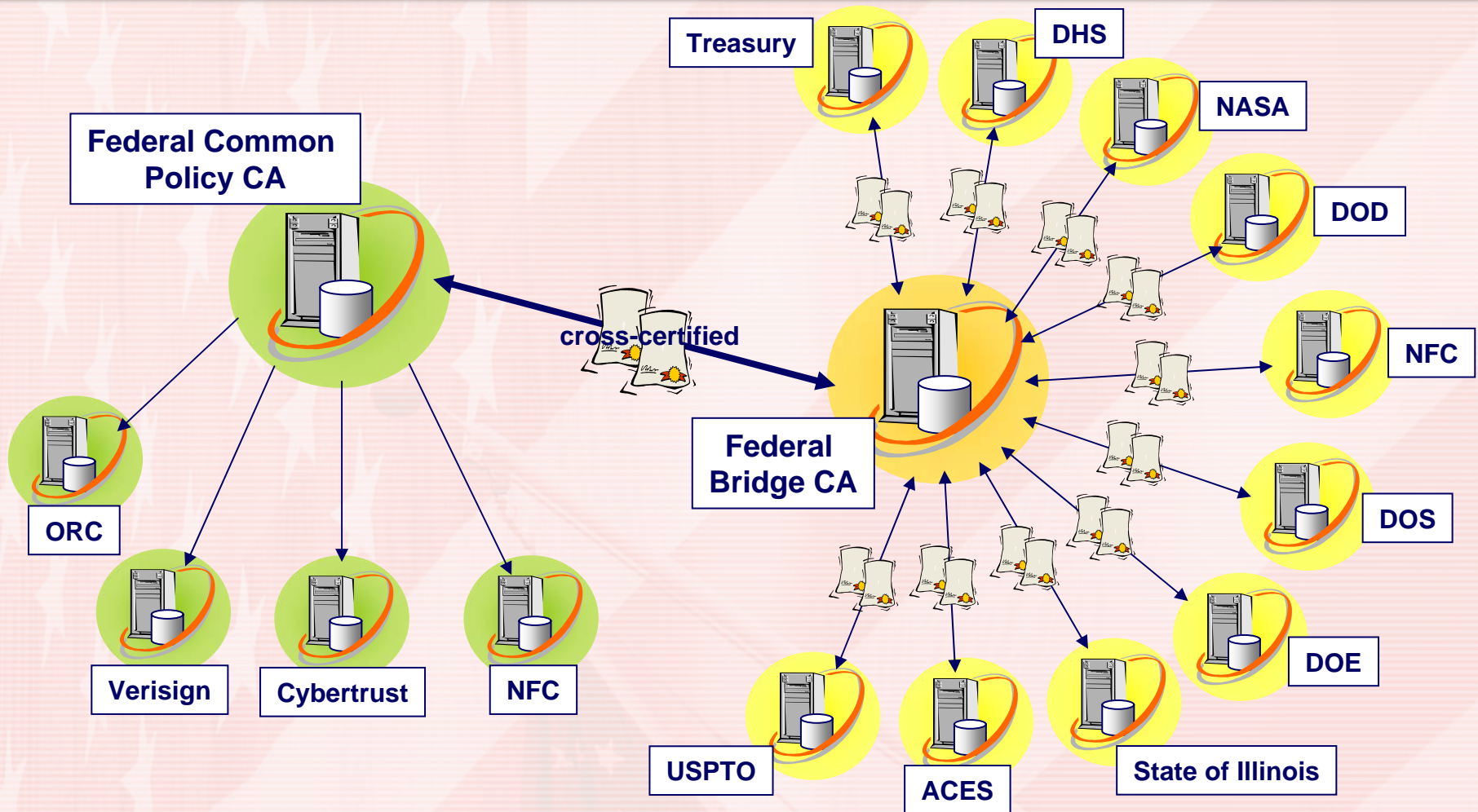
OMB Guidance establishes 4 authentication assurance levels

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 4<sup>th</sup> Sector: Internal Effectiveness and Efficiencies.

# Federal Common Policy Compliance



# Implementing PKI in accordance with FIPS-201

- 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
- 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

