



**Federal PKI**  
**Management Authority**  
**Enabling Trust**

**GSA**

# FPKIMA Industry Day 2015

*FPKI Overview*



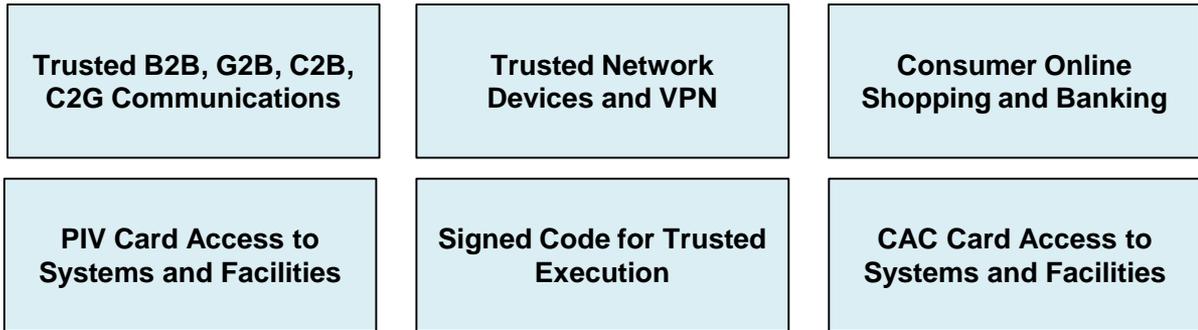
# Agenda

- Overview of the FPKI Trust Infrastructure
- Overview of the FPKI Ecosystem
- FPKI Interoperability

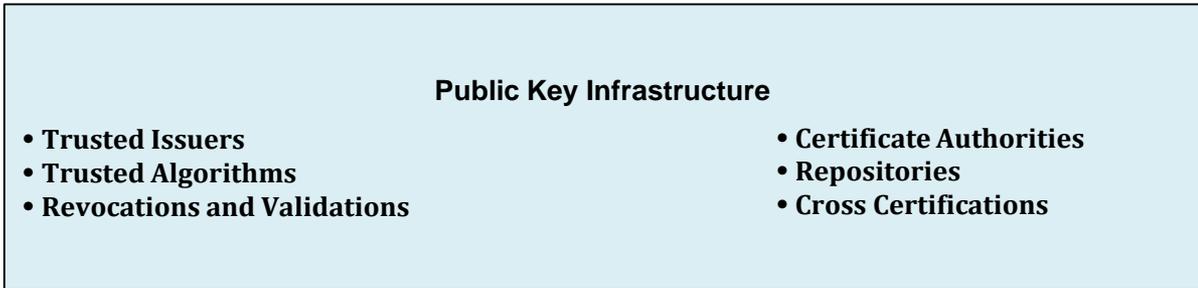


# Why?

## PKI Enables



## Trust Components





# FPKI Trust Infrastructure Overview

## Federal PKI Management Authority (FPKIMA)

- Managed by FAS within GSA
- Responsible for:
  - Management and operation of the FPKI Trust Infrastructure Certificate Authorities and repositories
  - Entity Interoperability testing
  - Path Discovery and Validation testing
  - Implementing new FPKI services to meet community needs
- Enables trust by operating Infrastructure Certificate Authorities



# FPKI Trust Infrastructure Overview

## Common Policy Root

Federal Bridge CA

SHA-1 FRCA

E-Governance CA

- ❖ The Root for PIV, Trust Anchor for the Federal Government
- ❖ FIPS 201 Section 4.2.2 CHUID and Section 4.4.2, Biometric Data: *“The X.509 certificate containing the public key required to verify the digital signature shall be issued under [COMMON]...”*
- ❖ FIPS 201 Section 5.4.2, PKI Certificate: *“All certificates issued to support PIV Card authentication shall be issued... ..as defined in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON].”*



# FPKI Trust Infrastructure Overview

Common Policy Root

**Federal Bridge CA**

SHA-1 FRCA

E-Governance CA

- ❖ Originally developed to facilitate interoperability between Federal agency enterprise PKI implementations
- ❖ FBCA's role expanded to include external entities
- ❖ FBCA Maps CA policies to standard federal policies
  - ❖ Medium, Medium Hardware, PIV-I, etc
- ❖ Mapping function enables trust across different communities of interest



# FPKI Trust Infrastructure Overview

Common Policy Root

Federal Bridge CA

**SHA-1 FRCA**

E-Governance CA

- ❖ Starting 1/1/2011 the FPKI PA prohibited the use of the SHA-1 algorithm for PIV
- ❖ FPKIMA Migrated Common to SHA-256 as required and established the SHA-1 FRCA to facility interoperability with communities that could not migrate



# FPKI Trust Infrastructure Overview

Common Policy Root

Federal Bridge CA

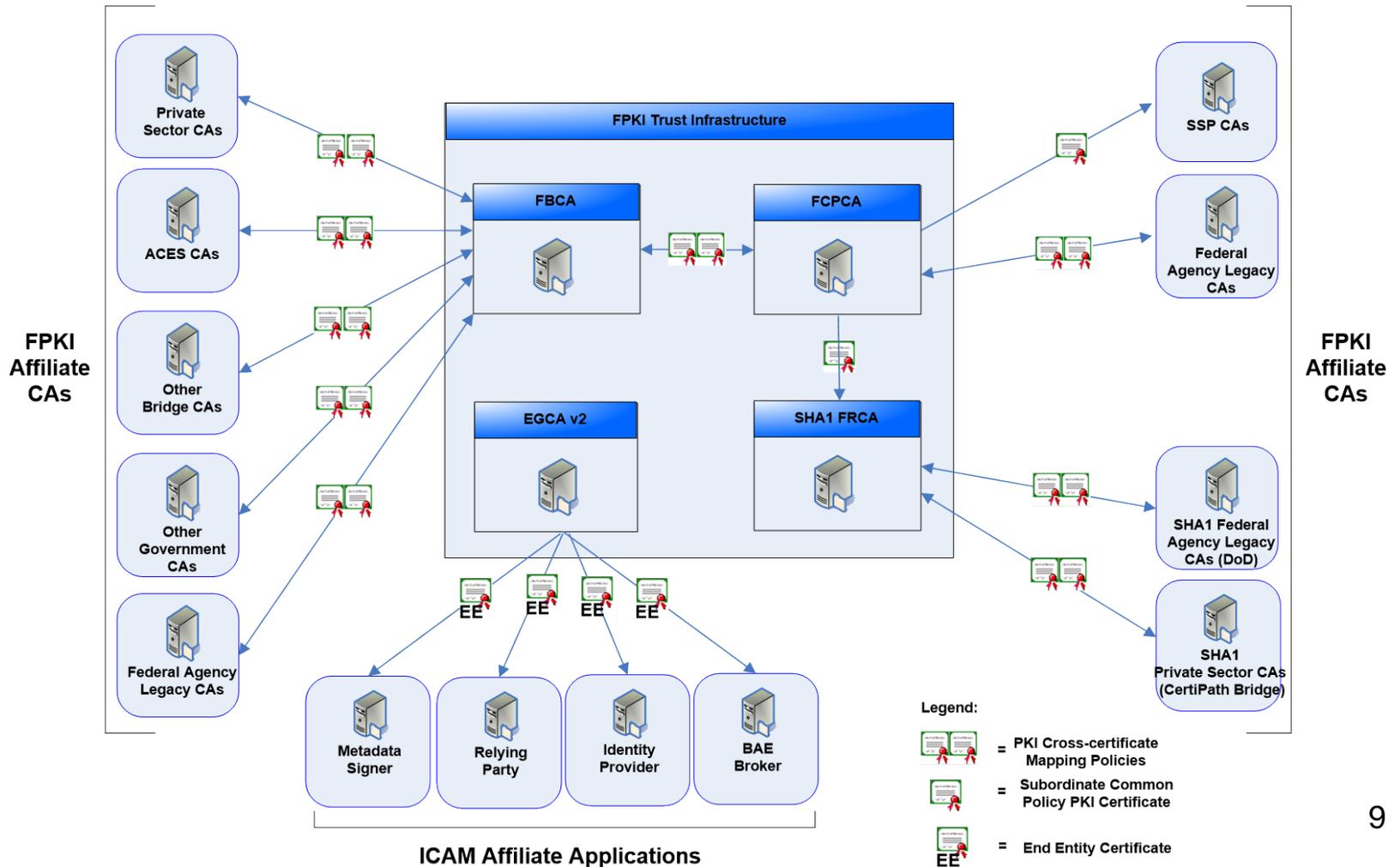
SHA-1 FRCA

**E-Governance CA**

- ❖ EGCA issues certificates to approved non-PKI credential service providers at LOA 1,2,3 and Federal Relying Parties
- ❖ The certificates are used to secure protocols such as SAML for Authentication and Attribute Exchange
- ❖ EGCA includes the E-Governance Trust Services to support Federations and Backend Attribute Exchange (BAE)

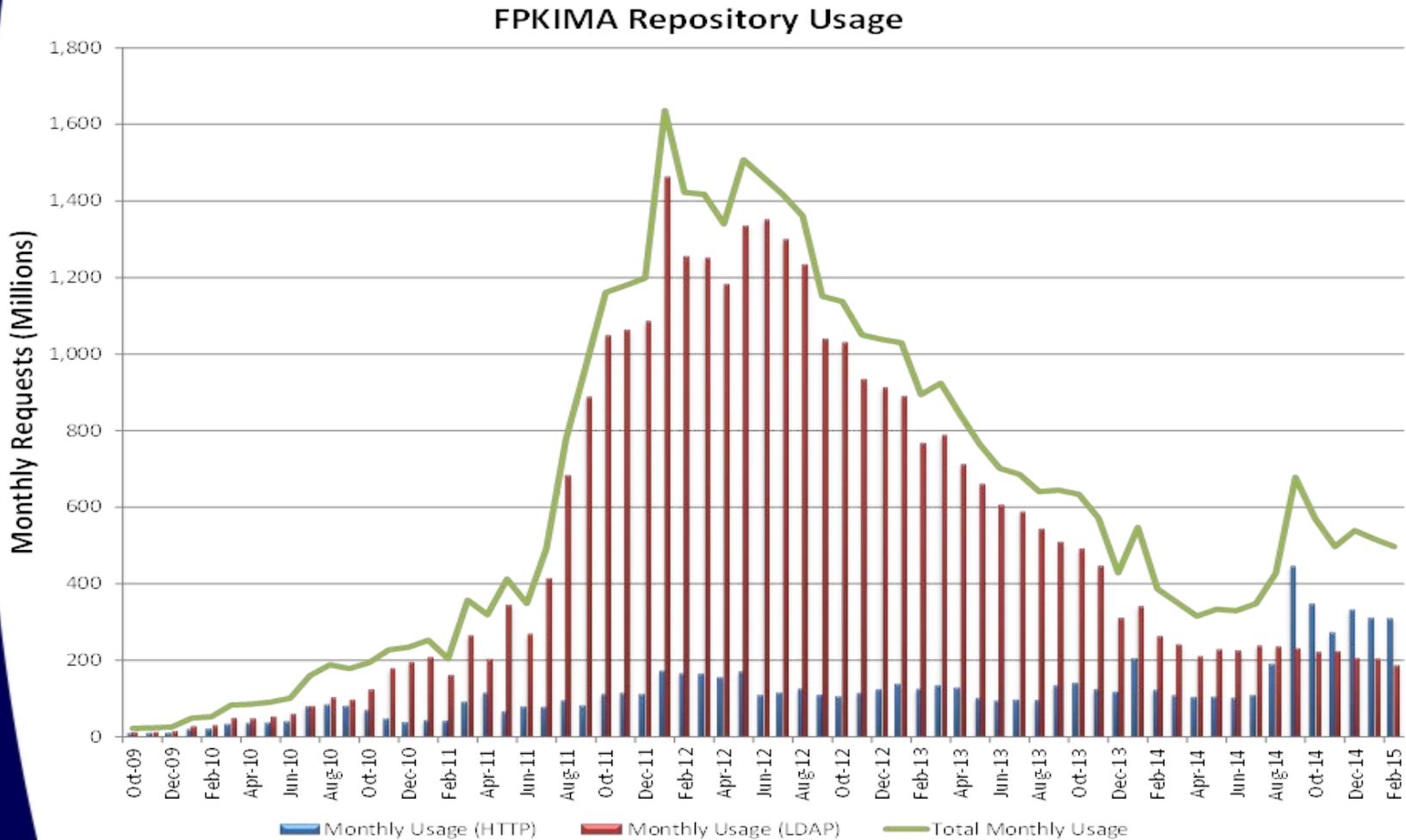


# FPKI Trust Infrastructure Overview





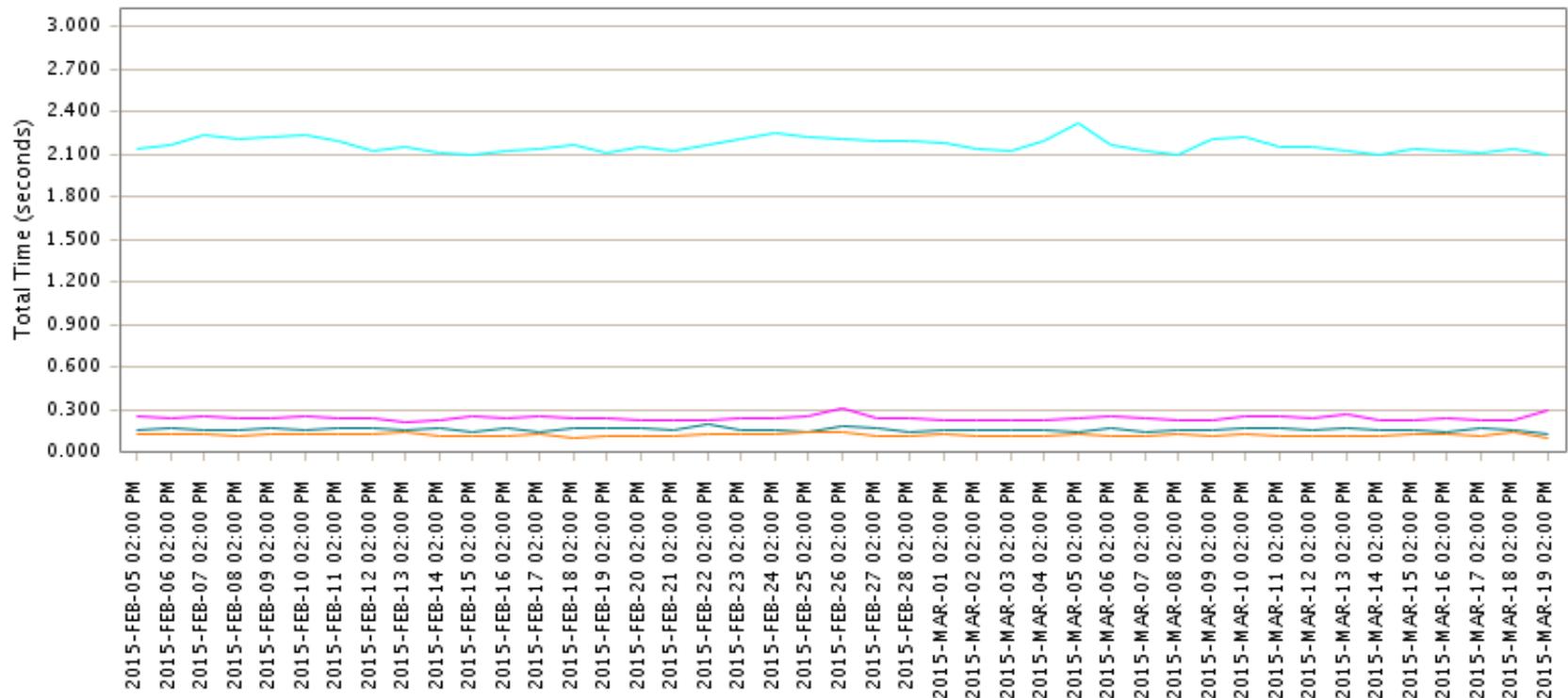
# FPKI Trust Infrastructure Overview





# FPKI Trust Infrastructure Overview

## FPKIMA Repository Response Time





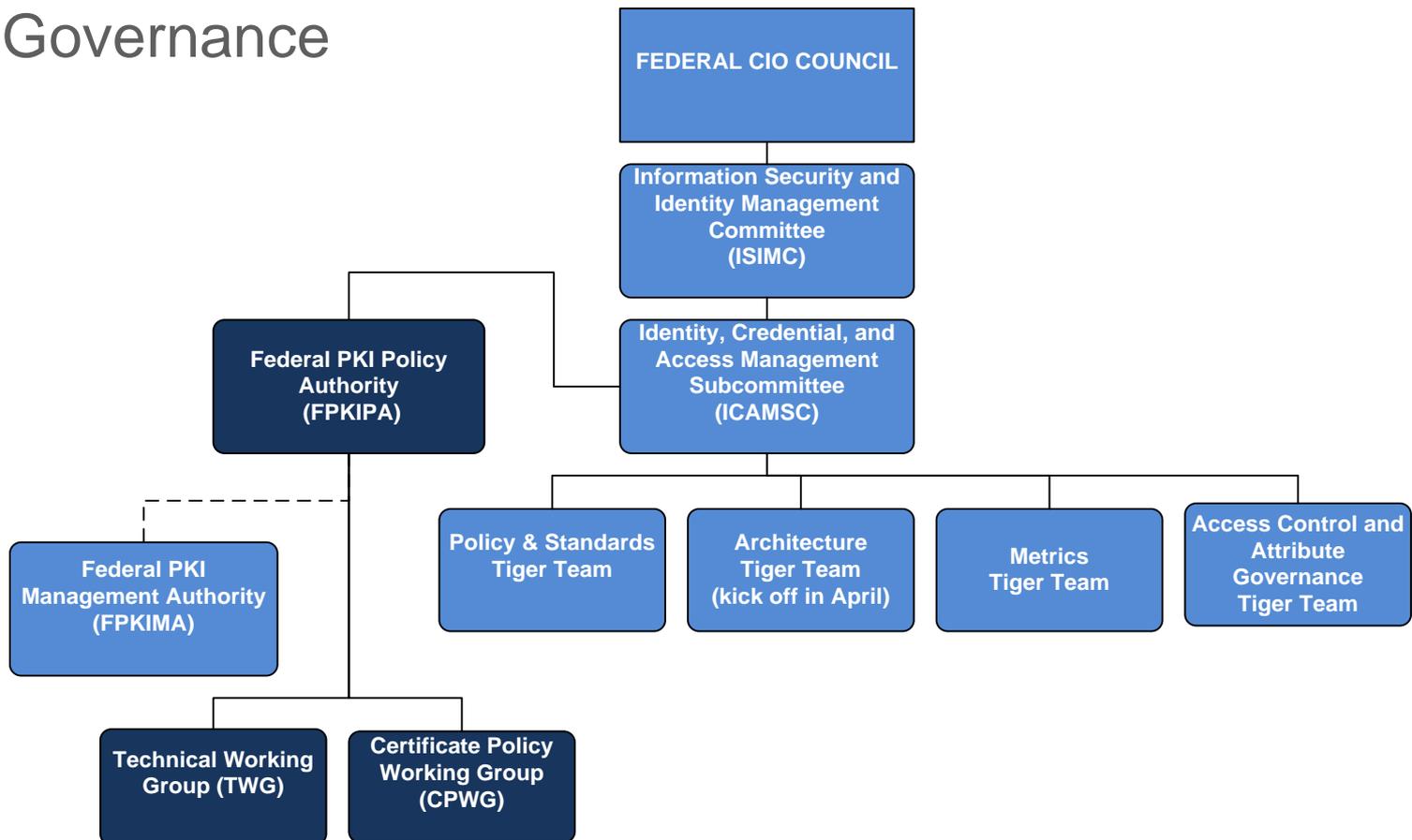
# Agenda

- ✓ Overview of the FPKI Trust Infrastructure
- Overview of the FPKI Ecosystem
- FPKI Interoperability



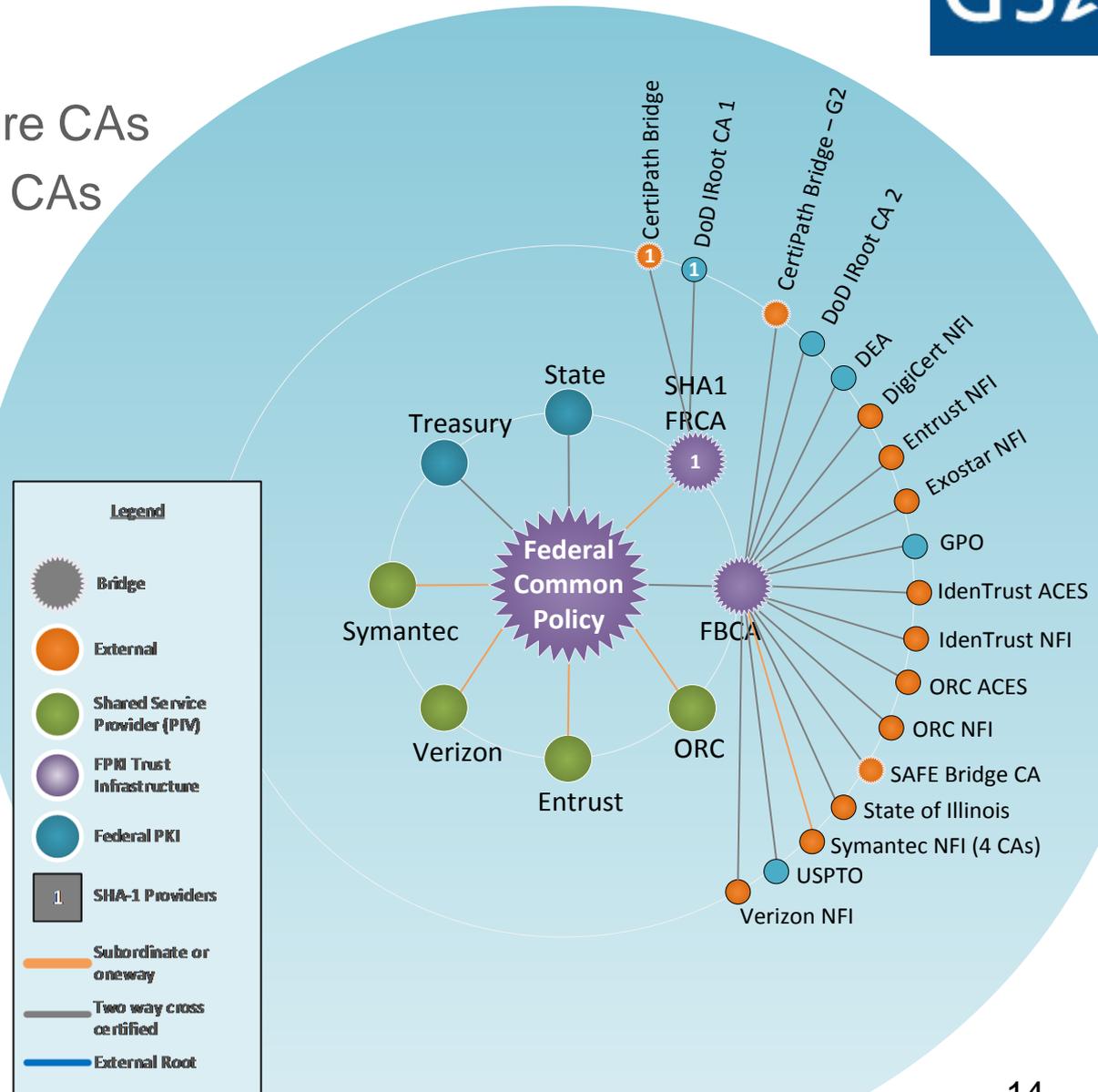
# Overview of the FPKI Ecosystem

- Governance



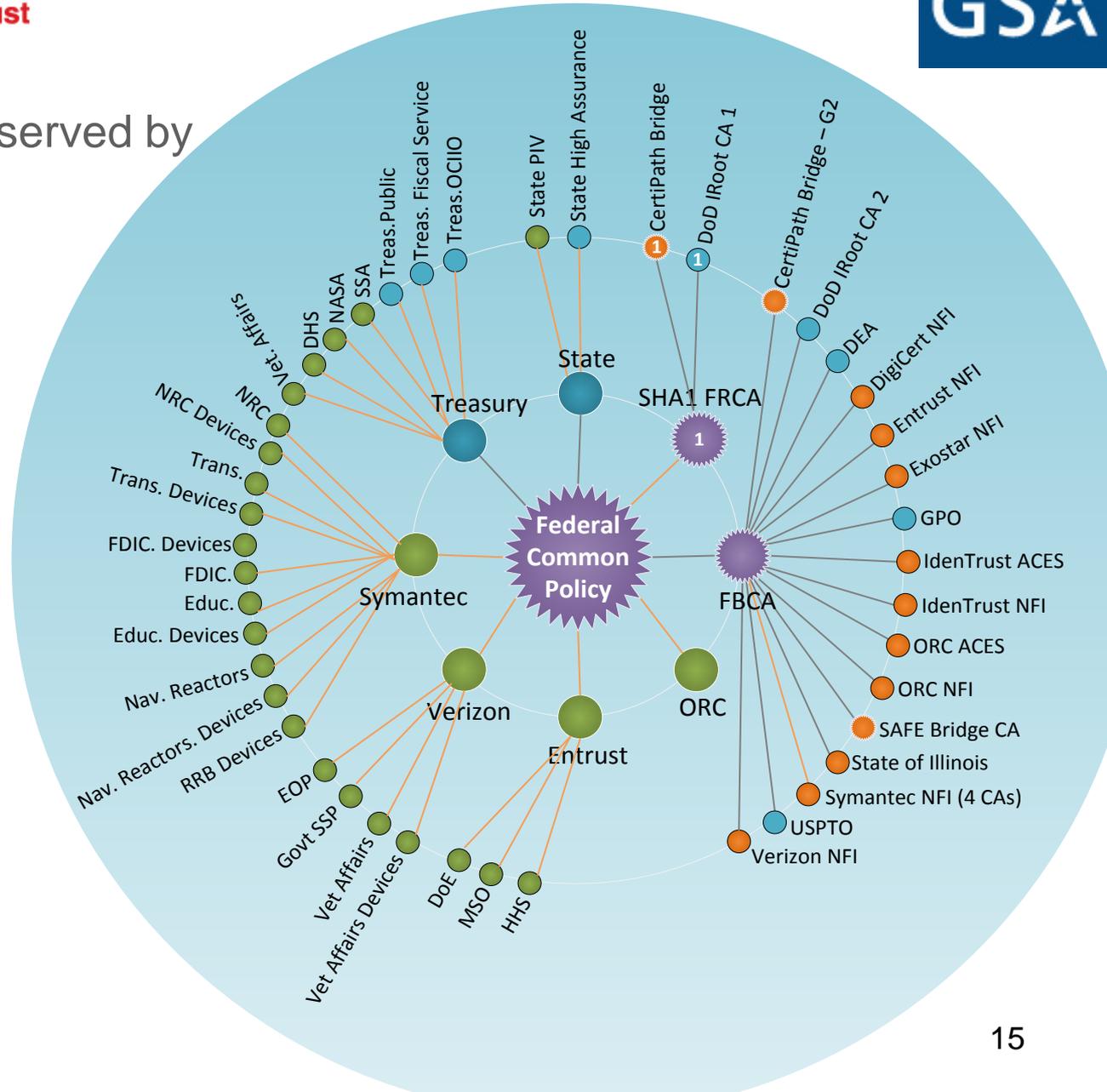


- 3 Trust Infrastructure CAs
- 16 Bridge Certified CAs
- 5 SSPs





- 27 Agency CAs served by SSPs
- ~2M PIV Cards

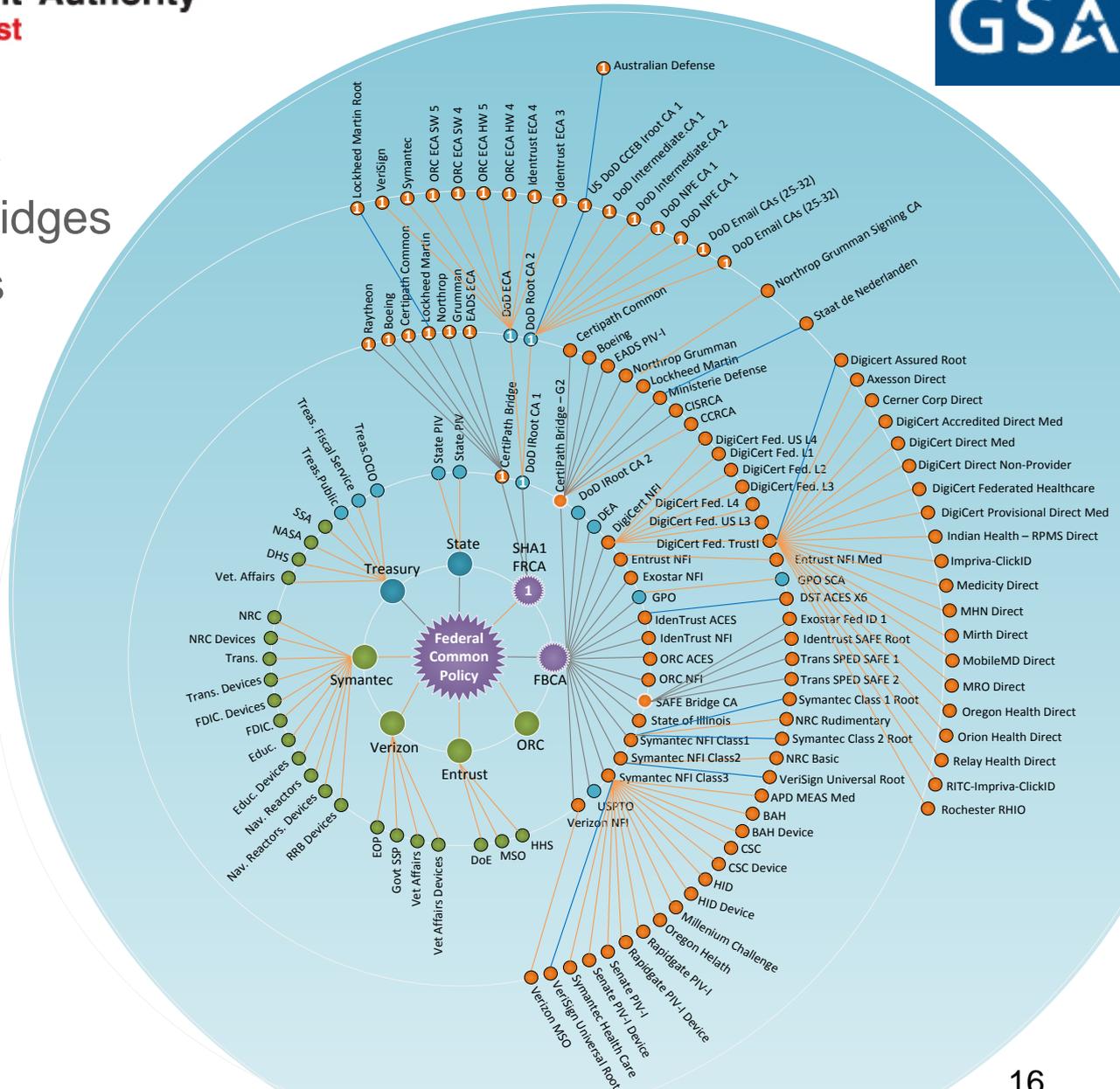




- 146 Trusted CAs
- 2 Commercial Bridges
  - +2 in process
- ~5.5m PIV/CAC

**Trusted Providers:**

- 5 PIV SSPs
- 9 PIV-I Issuers
- 4 SHA-1 Issuers





# Agenda

- ✓ Overview of the FPKI Trust Infrastructure
- ✓ Overview of the FPKI Ecosystem
- FPKI Interoperability



# FPKI Interoperability

- Interoperability Strategies
  - Standard Policies
  - Standard Certificate Profiles
  - Shared Test Environment
    - Community Interoperability Test Environment (CITE)
  - FIPS 201 Evaluation Program product testing
    - ICAM Cards



# PACs and Integrated Applications

**agilquest** GSA U.S. General Services Administration

## BookIT!

▶

- Introduction
- Logging In - Authentication & Bookmarking
- Home Page
- Profile
  - Personal Information
  - Preferences for Everyone
  - Delegates
  - Credentials
- Make a One Click Reservation
- Make a Reservation
  - Make a Reservation Through the Homepage (Short)
  - Make a Reservation Through the Reservation Summary (More detailed)
- Modify a Reservation
  - Cancel
  - Modify
- Locate
  - Locate People
  - Locate Reservation
- Express Check In & Other Ways to Check In & Out
- Difference between a reservation and a request
- Adding Equipment and Services

**GSA leveraging FPKI**



# Electronic Submission of Documents

Certified by Superintendent of Documents <pkisupport@gpo.gov>, United States Government Printing Office, certificate issued by VeriSign CA for Adobe CDS. Signature Panel

 **11186** Federal Register / Vol. 80, No. 40 / Monday, March 2, 2015 / Rules and Regulations

substantial direct costs on Tribal governments or preempt Tribal law. The Congressional Review Act, 5 U.S.C. 801 *et seq.*, as added by the Small Business Regulatory Enforcement Fairness Act of 1996, generally provides that before a rule may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of the rule, to each House of the Congress and to the Comptroller General of the United States. EPA will submit a report containing this action and other required information to the U.S. Senate

**Signature Properties**

Document certification is valid, signed by Superintendent of Documents <pkisupport@gpo.gov>.

Signing Time: 2015/02/26 02:18:12 -05'00'

**Reason: GPO attests that this document has not been altered since it was disseminated by GPO**

Location: US GPO, Washington, DC 20540

Validity Summary

**GPO leveraging FPKI**



# Mutual Authentication of Web Applications

**MAX.gov LOGIN** Don't Have a MAX ID Yet? [Register Now](#)

Home Manage Password Contact Us

LOGIN WITH YOUR...

**MAX.gov User ID & Password**

User ID  Set a Personal Username

\_\_\_\_\_  
 Password [Forgot, set, or change your password?](#)

\_\_\_\_\_  
 LOGIN

Coming Soon: MAX SECURE+

**PIV or CAC Card**

Please make sure your card is plugged into the reader



LOGIN WITH YOUR  
**PIV OR CAC**

**OMB leveraging FPKI**

**Intelink**  
Driven by Mission. Enabled by Innovation

[Reset Login Session](#)

Please choose one of the following authentication options  
 In order to access Intelink. Selection of an authentication method constitutes your acceptance of both Intelink's [Terms Of Use](#) and the monitoring of system activity, as described in the warning notice to the right.

[Valid PKI Certificate \(ie. DOD, CAC, FED, PIV\)](#)

[Intelink Account \(Remote Access or Passport\)](#)

Intelink Federated Partner Login

**U.S. Government Warning**

This is a United States Government computer system. This computer system, including all related equipment, networks, and network devices, including Internet access, are provided only for authorized U.S. Government use. U.S. Government computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes authorized attacks by authorized U.S. Government entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information including personal information, placed on or sent over this system may be monitored.

Use of this U.S. Government system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse actions.

For technical assistance, please contact the ISMC Watch: 301-688-1800 (commercial), 644-1800 (DSN)

Client network = Internet(ASH-55.75)

**DNI leveraging FPKI**



# Agenda

- ✓ Overview of the FPKI Trust Infrastructure
  - ✓ Overview of the FPKI Ecosystem
  - ✓ FPKI Interoperability
- 
- Questions?