Security in knowledge

FPKIMA: The Dial-Tone for FPKI

Darlene Gore

FPKIMA Program Manager, GSA

Chris Louden

FPKIMA Security Lead, Protiviti

RSA CONFERENCE 2013

Session ID: PNG-R35A

Session Classification: General Interest

Learning Objectives

1. Understanding of the Federal Public Key Infrastructure (FPKI)
2. Awareness of the Federal Public Key Infrastructure Management Authority (FPKIMA) services
3. Knowledge that the FPKIMA is willing to help promote the use of PKI technologies

Agenda

I. FPKIMA Background
II. Why Should You Care?
III. Summary

Agenda

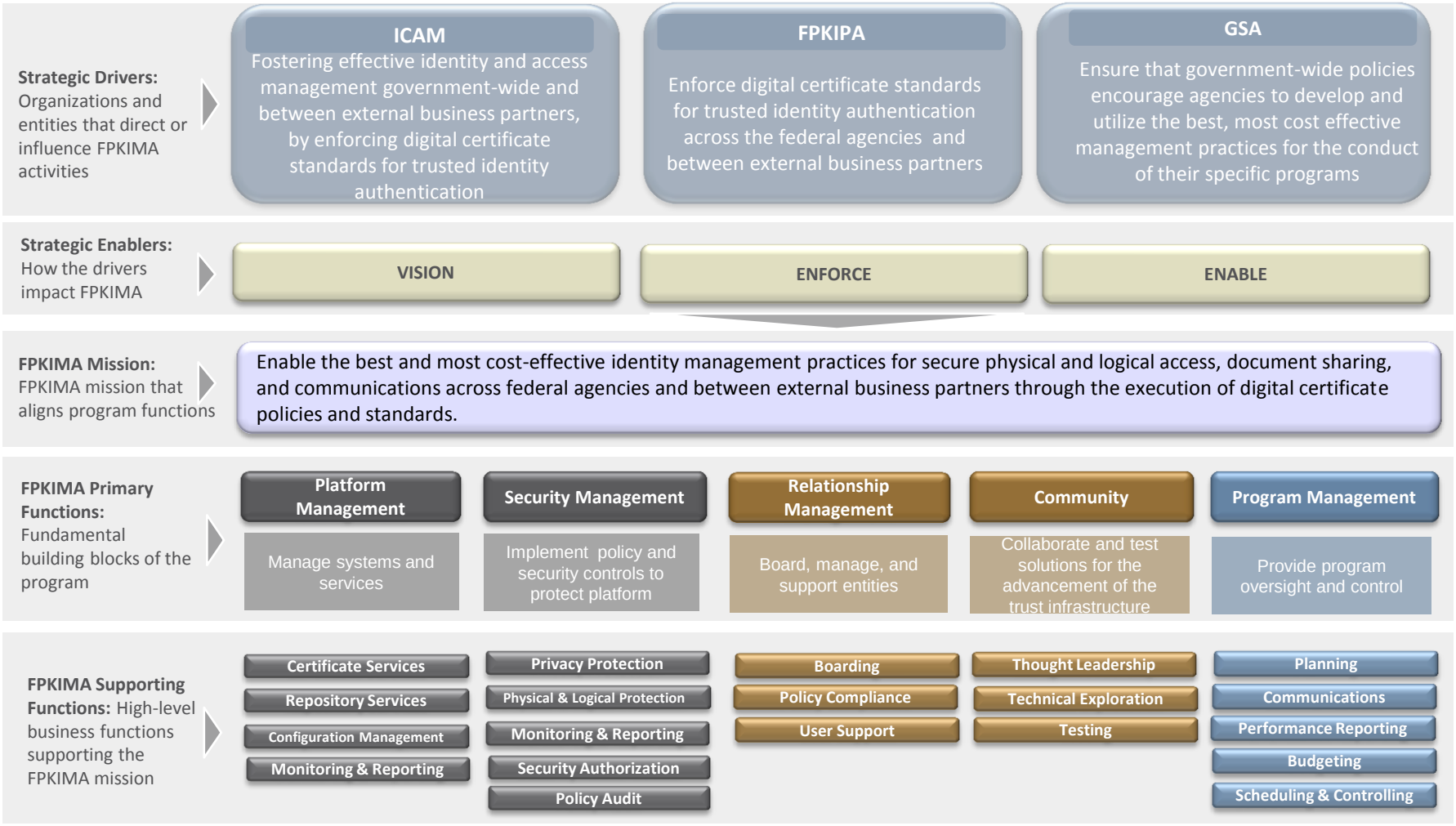
- FPKIMA Background
  - Who we are
  - b. What is the FPKI
  - c. What we protect
- II. Why Should You Care?
- III. Summary

Who We Are

- The E-Government Act of 2002 appointed the General Services Administration (GSA) to manage the design, development, implementation, and operation of the Production FPKI Trust Infrastructure in support of the FPKI.
- GSA created the FPKIMA to manage the FPKI Trust Infrastructure.
- Find us at:

  http://www.idmanagement.gov/pages.cfm/page/Federal-PKI-Management-Authority-Home-Page

Who We Are – The Big Picture



Agenda

- FPKIMA Background
  - ✓ Who we are
  - What is the FPKI
  - c. What we protect
- II. Why Should You Care?
- III. Summary

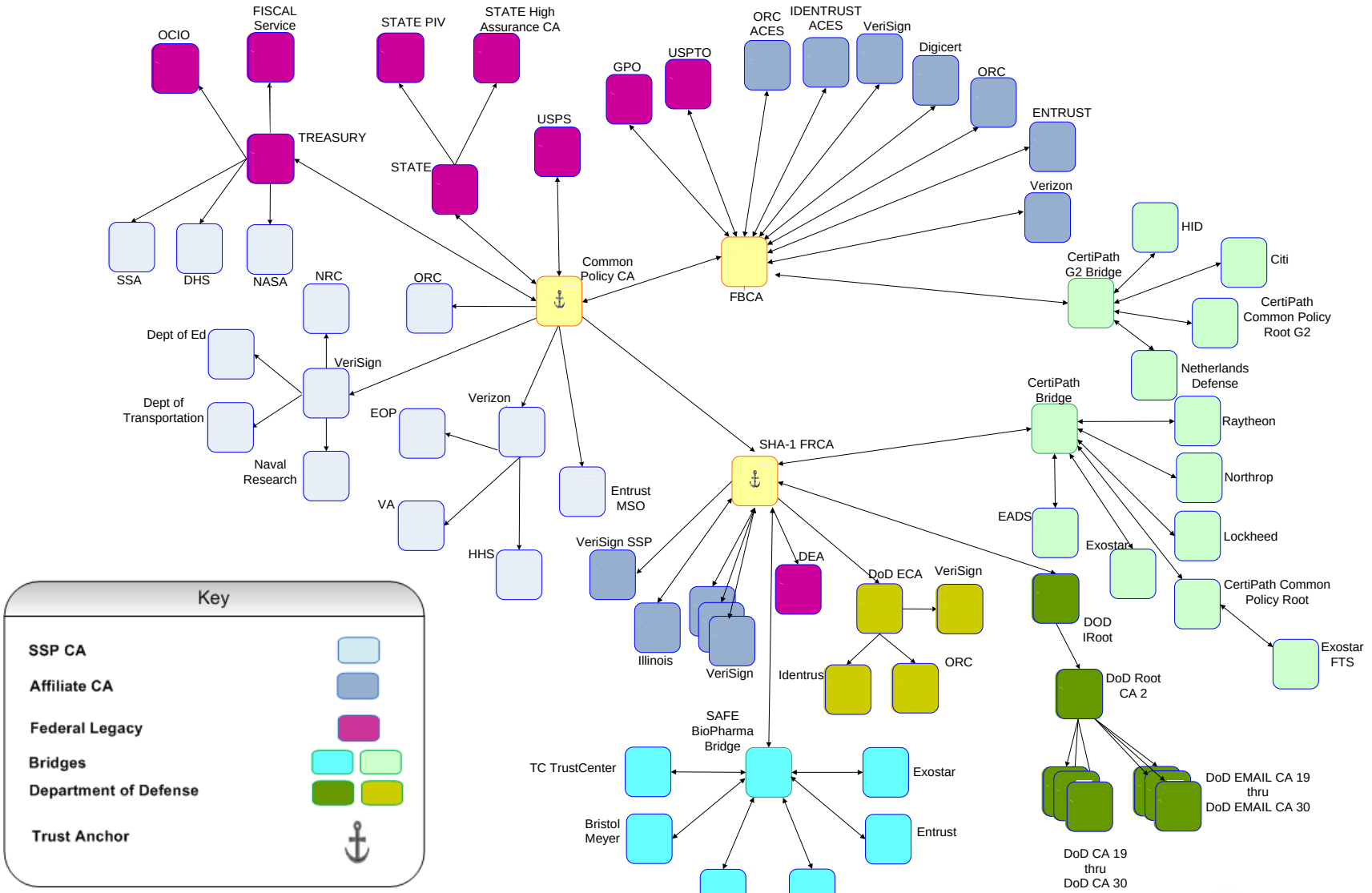
Federal Public Key Infrastructure (FPKI)

- Cryptographic infrastructure that **enables cross-organizational, interoperable security services** for **confidentiality, access control,** and **identity assurance.**
- Foundation for **secure e-government** transactions at the highest e-Authentication level.
- Enables numerous Federal directives and programs.
- Provides the **trust anchor** for the Federal Government's HSPD-12/Personal Identity Verification (PIV) and other FPKI services.

Customers of the FPKI

- Entities relying on U.S. Government trusted credentials are customers of the FPKIMA Program. For example, our customers include:
  - Federal Agencies for logical and physical access.
  - Shared Service Providers and certified PIV issuers relying on the trust chain provided by the federal root.
  - Business partners and relying parties who depend on certificate paths through the Federal Bridge CA to validate certificates issued by an FPKI Affiliate or certified PIV-I issuer.
  - External relying parties validating FPKI community credentials to the Federal Common Policy CA root certificate as a trust anchor.

The Federal PKI



FPKIMA Customers

Certificates Issued by the FPKI Trust Infrastructure CAs

- FBCA (12):

  Common Policy
  CertiPath Bridge
  Verisign
  Entrust
  VBS
  Identrust
  Operational Research Consultants (ORC) (2)
  GPO
  PTO
  DigiCert
  State of Illinois

- Common Policy (11):

  Federal Bridge
  SHA-1 Federal Root
  Department of Treasury
  Department of State
  VeriSign
  Verizon Business
  Entrust
  ORC (2)
  Legacy-Common Policy (issued to Common Policy)
  SHA-1 Federal Root

- SHA-1 Federal Root (9):

  CertiPath Bridge,
  SAFE BioPharma Bridge
  Department of Defense (DoD)
  DoD ECA
  DEA
  VeriSign(4)

- E-Governance CAs (4):

  Office of Personnel Management,
  United States Department of Agriculture,
  ORC
  Department of Transportation

Agenda

- FPKIMA Background
  - ✓ Who we are
  - ✓ What is the FPKI
  - What we protect
- II. Why Should You Care?
- III. Summary

What We Protect - Context

- Cyber security attacks are commonplace
  - Unauthorized access to data
  - Facility breaches
  - Sensitive data leakage
  - Information warfare
- Identity theft is commonplace
- Attacker sophistication is increasing
  - Advanced Persistent Threat
  - Organized Crime
  - Cloud based "attack for hire"
  - PKI elements being attacked

We Protect Sensitive Artifacts

Strategic Drivers: Organizations and entities that direct or influence FPKIMA activities

- **ICAM** — Fostering effective identity and access management government-wide and between external business partners, by enforcing digital certificate standards for trusted identity authentication
- **FPKIPA** — Enforce digital certificate standards for trusted identity authentication across the federal agencies and between external business partners
- **GSA** — Ensure that government-wide policies encourage agencies to develop and utilize the best, most cost effective management practices for the conduct of their specific programs

Strategic Enablers: How the drivers impact FPKIMA

- VISION
- …BLE

FPKIMA Mission: FPKIMA mission that aligns program functions

- Enable the best and most cost-effective identity … and communications across federal agencies an… policies and standards.
- …ocument sharing, …digital certificate

FPKIMA Primary Functions: Fundamental building blocks of the program

- **Platform Management** — Manage systems and services
- **Security Managemen…** — Implement policy and security controls to protect platform
- **…rogram Management** — Provide program …oversight and control

FPKIMA Supporting Functions: High-level business functions supporting the FPKIMA mission

- Certificate Services
- Repository Services
- Privacy Protection
- Physical & Logical Protection
- Monitoring & Reporting
- Security Authorization
- Policy Audit
- Boarding
- Policy Compliance
- User Support
- Thought Leadership
- Technical Exploration
- Testing
- Planning
- Communications
- Performance Reporting
- Budgeting
- Scheduling & Controlling

What happens if U.S. Government Sensitive Artifacts are compromised?

- Disruption in government services and business
- Adverse effect on individual privacy
- Denied access to government facilities
- Denied access to official systems

We Protect Foundational Trust

Strategic Drivers: Organizations and entities that direct or influence FPKIMA activities

ICAM
Fostering effective identity and access management government-wide and between external business partners, by enforcing digital certificate standards for trusted identity authentication

FPKIPA
Enforce digital certificate standards for trusted identity authentication across the federal agencies and business partners

GSA
Ensure that government-wide policies encourage agencies to develop and utilize the best, most cost effective management practices for the conduct of their specific programs

Strategic Enablers: How the drivers impact FPKIMA

VISION

RCE

ENABLE

FPKIMA Mission: FPKIMA mission that aligns program functions

Enable the best and most cost-effective identity management practices for secure physical and logical access, document sharing, and communications across federal agencies and between external business partners through the execution of digital certificate policies and standards.

FPKIMA Primary Functions: Fundamental building blocks of the program

Platform Management	Security Management	Relationship Management
Manage systems and services	Implement policy and security controls to protect platform	Board, manage, and support entities

FPKI MA Supporting Functions: High-level business functions supporting the FPKIMA mission

Certificate Services	Privacy Protection	Boarding
Repository Services	Physical & Logical Protection	Policy Compliance
Configuration Management	Monitoring & Reporting	User Support
Monitoring & Reporting	Security Authorization	
	Policy Audit	

What happens if foundational trust is in question?

- Serious adverse effect on agency operations
- Serious consequence for public confidence
- Private and public partners cost impact to recover
- Disruption of relying party applications and transactions

We Protect Business Partners

Strategic Drivers: Organizations and entities that direct or influence FPKIMA activities

ICAM
Fostering effective identity and access management government-wide and between external business partners, by enforcing digital certificate standards for trusted identity authentication

FPKIPA
Enforce digital certificate standards for trusted identity authentication across the federal agencies and between external business partners

GSA
Ensure that government-wide policies encourage agencies to develop and utilize the best, most cost effective management practices for the conduct of their specific programs

Strategic Enablers: How the drivers impact FPKIMA

VISION

ENABLE

FPKI A Mission: FPKIMA mission that aligns program functions

Enable the best and most cost-effective identity n… physical and logical access, document sharing, and communications across federal agencies and between external business partners through the execution of digital certificate policies and standards.

FPKIMA Primary Functions: Fundamental building blocks of the program

…ship …ment

Community

Collaborate and test solutions for the advancement of the trust infrastructure

Program Management

Provide program oversight and control

FPKIMA Supporting Functions: High-level business functions supporting the FPKIMA mission

…ling
…pliance
…pport

Thought Leadership
Technical Exploration
Testing

Planning
Communications
Performance Reporting
Budgeting
Scheduling & Controlling

What happens if trust in affiliates is undermined?

- Disruption of Business Partner's and Affiliate PKI's trust chains
- Revocation and re-issuance of cross certificates to Federal agencies and Shared Service Providers
- Chaos in electronic-government solutions until resolved

We Provide Authentication Assurance

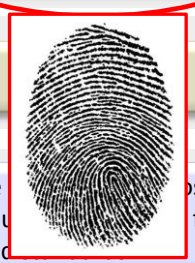
Strategic Drivers: Organizations and entities that direct or influence FPKIMA activities

ICAM
Fostering effective identity and access management government-wide and between external business partners, by enforcing digital certificate standards for trusted identity authentication

FPKIPA
Enforce digital certificate standards for trusted identity authentication across the federal agencies and between external business partners

GSA
Ensure that government-wide policies encourage agencies to develop and utilize the best, most cost effective management practices for the conduct of their specific programs

Strategic Enablers: How the drivers impact FPKIMA



ENFORCE

ENABLE

FPKIMA Mission: FPKIMA mission that aligns program functions

Enable the ...st-effective identity management practices for secure physical and logical access, document sharing, and commu... federal agencies ... of digital certificate policies and ...

FPKIMA Primary Functions: Fundamental building blocks of the program

Platform Management
Manage systems and services

Security Manage...
Implement policy ... security controls ... protect platform

Program Management
Provide program oversight and control

FPKIMA Supporting Functions: High-level business functions supporting the FPKIMA mission

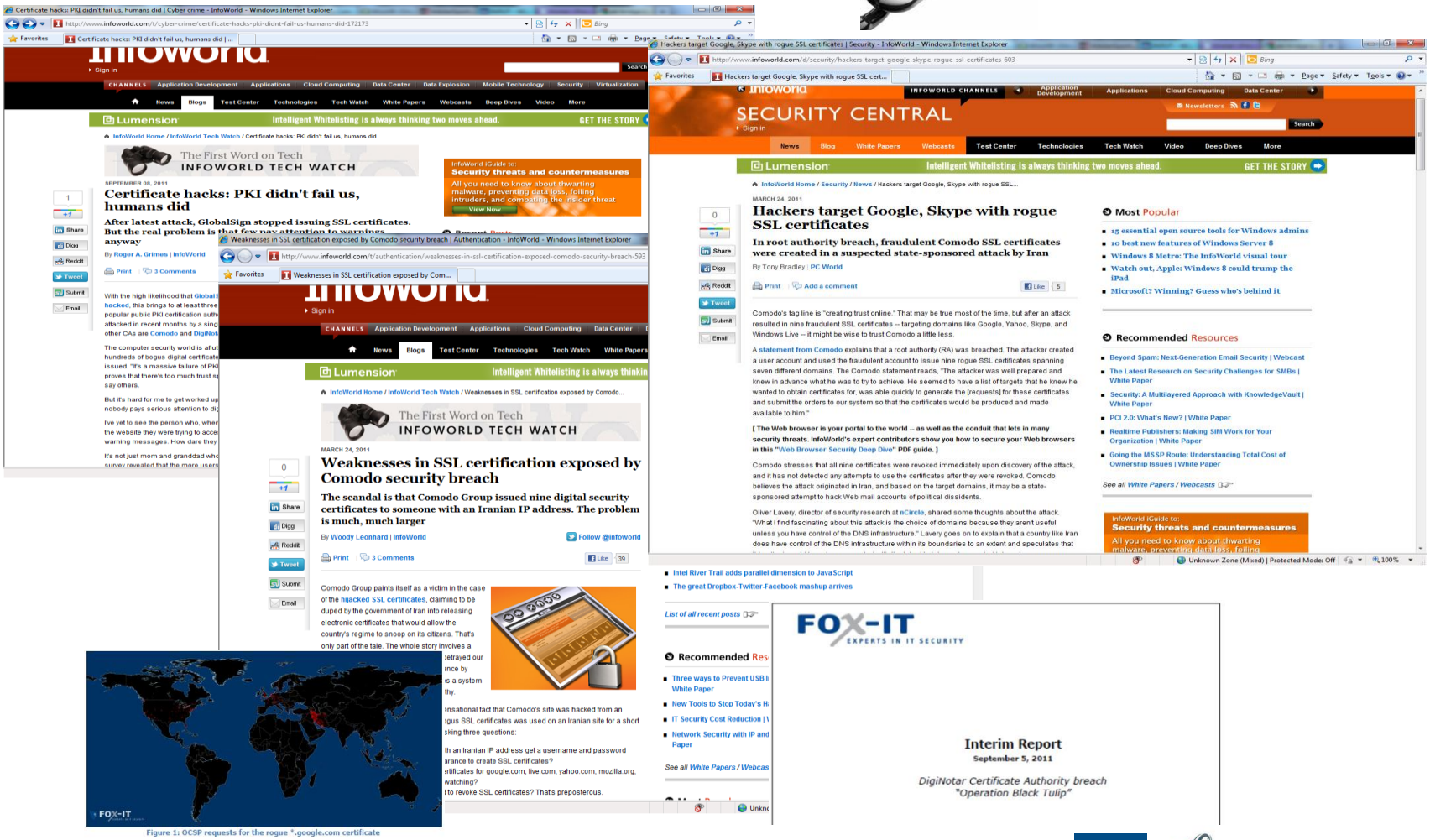
- Certificate Services
- Repository Services
- Configuration Management
- Monitoring & Reporting
- Privacy Protecti...
- Physical & Logical Prot...
- Monitoring & Repo...
- Security Authoriz...
- Policy Audit
- Planning
- Communications
- Performance Reporting
- Budgeting
- Scheduling & Controlling

What happens if authentication assurance is in jeopardy?

- Damaged reputation, agency liability or financial loss
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Cost of Poor Protection?

Broken Trust.



Agenda

- ✓ FPKIMA Background
- ➢ Why Should You Care?
  - ➢ What we Do
  - b. Services You Use (or Will Soon)
  - c. FPKI Usage Statistics
- III. Summary

FPKIMA Overview

- Perform Infrastructure (IT Service) Management
  - Manage the FPKI Trust Infrastructure CAs and their repositories.
  - Operate the FPKI Service Desk
    - FPKIPA-MA@listserv.gsa.gov
    - 1-888-754-1229 (1-888-PKI-1A2Z)
- Manage the full life cycle of digital certificates issued by the FPKI Trust Infrastructure
- Repository services to enable relying parties to locate certificate status

We Do – Community Working Groups

Working Group Name	Description
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKI governing body. It is an interagency body that develops digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.
FPKI Technical Working Group (FPKI TWG)	Discusses technical issues related to the usability of the PKI and future enhancements to the FPKI are brought to the TWG. It is focused on advancing PKI technology through collaboration, discussion and investigation. FPKIMA Co-chairs this working group.
Certificate Policy Working Group (CPWG)	Serves as the advisory group to the Federal FPKI Policy Authority on policy mappings and changes to the FPKI CPs.
PKI Shared Service Provider Working Group (SSPWG)	Oversees the processes involved in the PKI Shared Service Provider (SSP) program.

Agenda

- ✓ FPKIMA Background
- ➢ Why Should You Care?
  - ✓ What we Do
  - ➢ Services You Use (or Will Soon)
  - c. FPKI Usage Statistics
- III. Summary

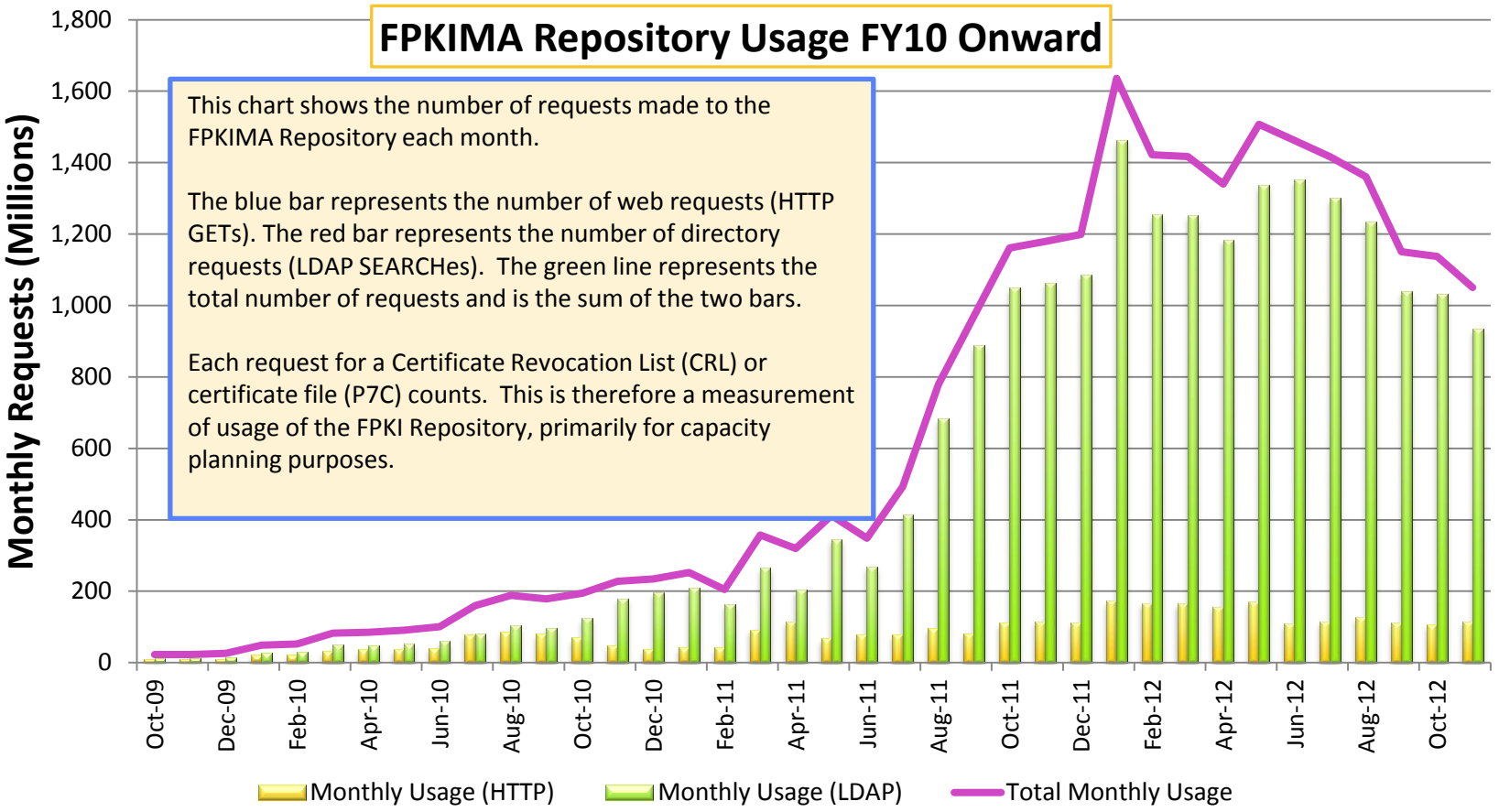
Why You Should Care – Our Services

- The FPKIMA Trust Infrastructure enables:
  - Smart card logon using PIV, PIV-Interoperable (PIV-I) or Common Access Card (CAC)
  - Facility access using PivAuth or cardAuth certificates
  - Authenticated access to web services or portals
- Fount of PKI knowledge to help in your PKI journey
  - CPS development
  - PKI-enablement information sharing
  - PKI implementation lessons learned
  - Technical and architectural concerns
  - etc.

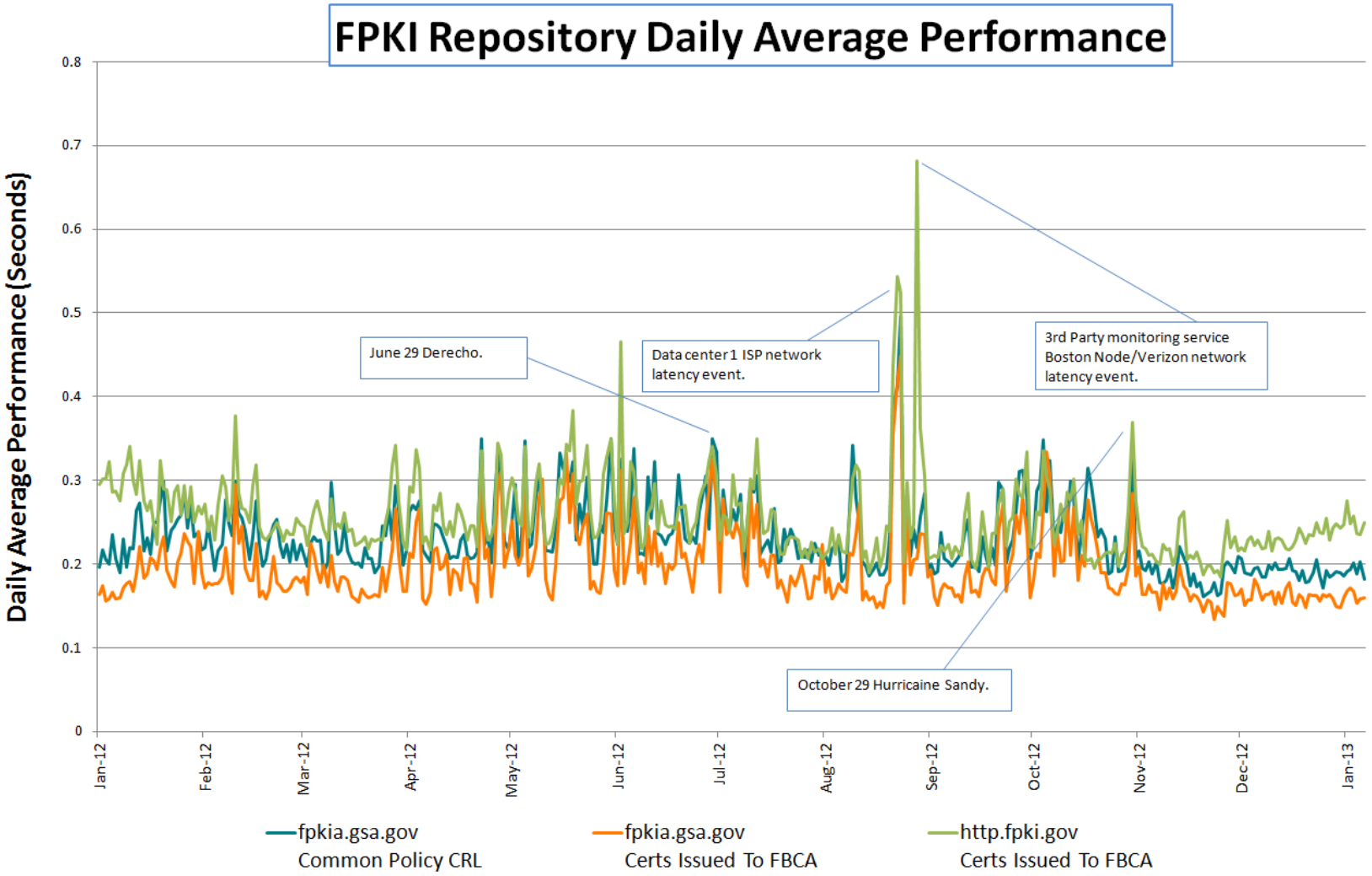
Agenda

- ✓ FPKIMA Background
- ➢ Why Should You Care?
  - ✓ What we Do
  - ✓ Services You Use (or Will Soon)
  - ➢ FPKI Usage Statistics
- III. Summary

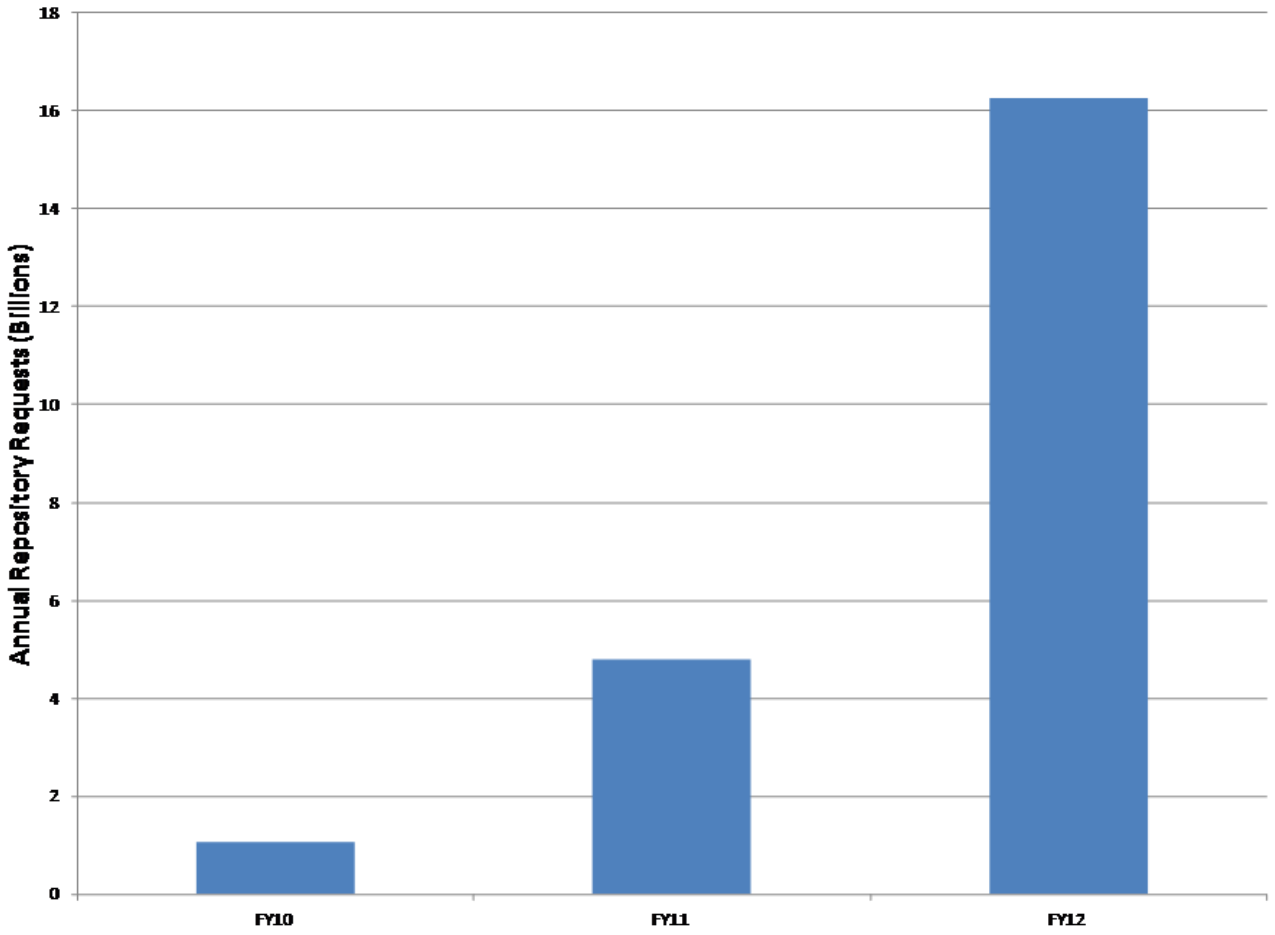
FPKI Statistics – Platform Usage



FPKI Statistics - Performance



FPKI Statistics – Repository Requests

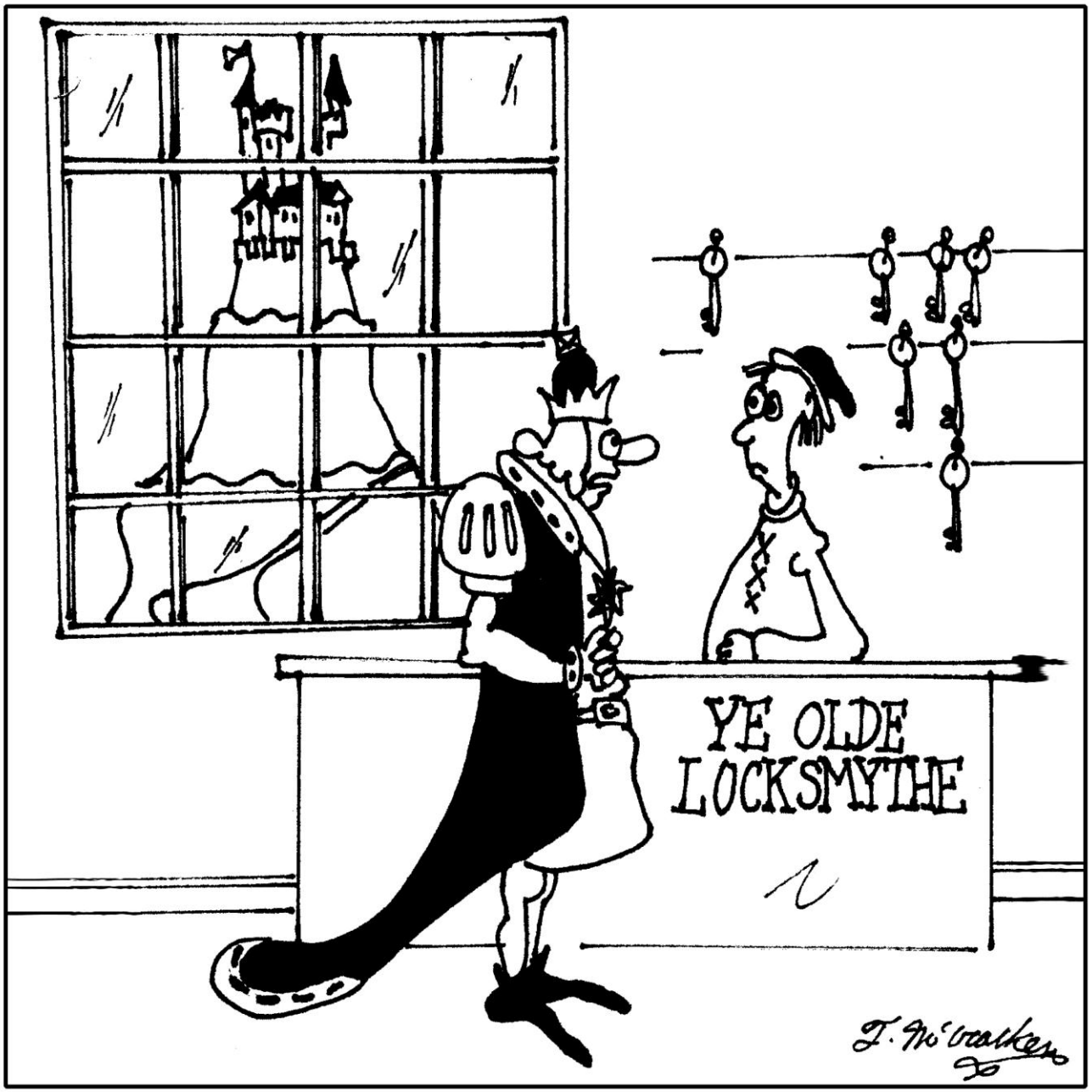


Agenda

- ✓ FPKIMA Background
- ✓ Why Should You Care?
- ➢ Summary

Summary

- The FPKI is critical infrastructure for high-assurance trust, security, and interoperability.
- The U.S. Government and various other communities rely on the FPKI to help meet their mission-critical objectives – including internal and cross-community (federation) purposes.
- FPKI importance and use continue to grow.
- Our team is willing to share our lessons-learned with your organization to help promote PKI or help with PKI-enablement.



“I lost my key to the kingdom.”

Learning Objectives Review

1. Understanding of the Federal Public Key Infrastructure (FPKI)
2. Awareness of the Federal Public Key Infrastructure Management Authority (FPKIMA) services
3. Knowledge that the FPKIMA is willing to help promote the use of PKI technologies

QUESTIONS?

Thank You and Contact Information

Darlene K. Gore

FPKI Program Manager

Security Services Division

Office of Integrated Technology Services

Federal Acquisition Service

General Services Administration

D: 703-306-6109

BB#703-517-0805

darlene.gore@gsa.gov

Chris Louden

FPKIMA Technical Lead

Protiviti, Inc.

D: 703-299-3444

C: 703-447-7431

chris.louden@pgs.protiviti.com

FPKI Service Desk

Toll Free: 888-754-1229

FPKIPA-MA@listserv.gsa.gov

FPKIMA:
Dial-Tone for FPKI

Security in knowledge