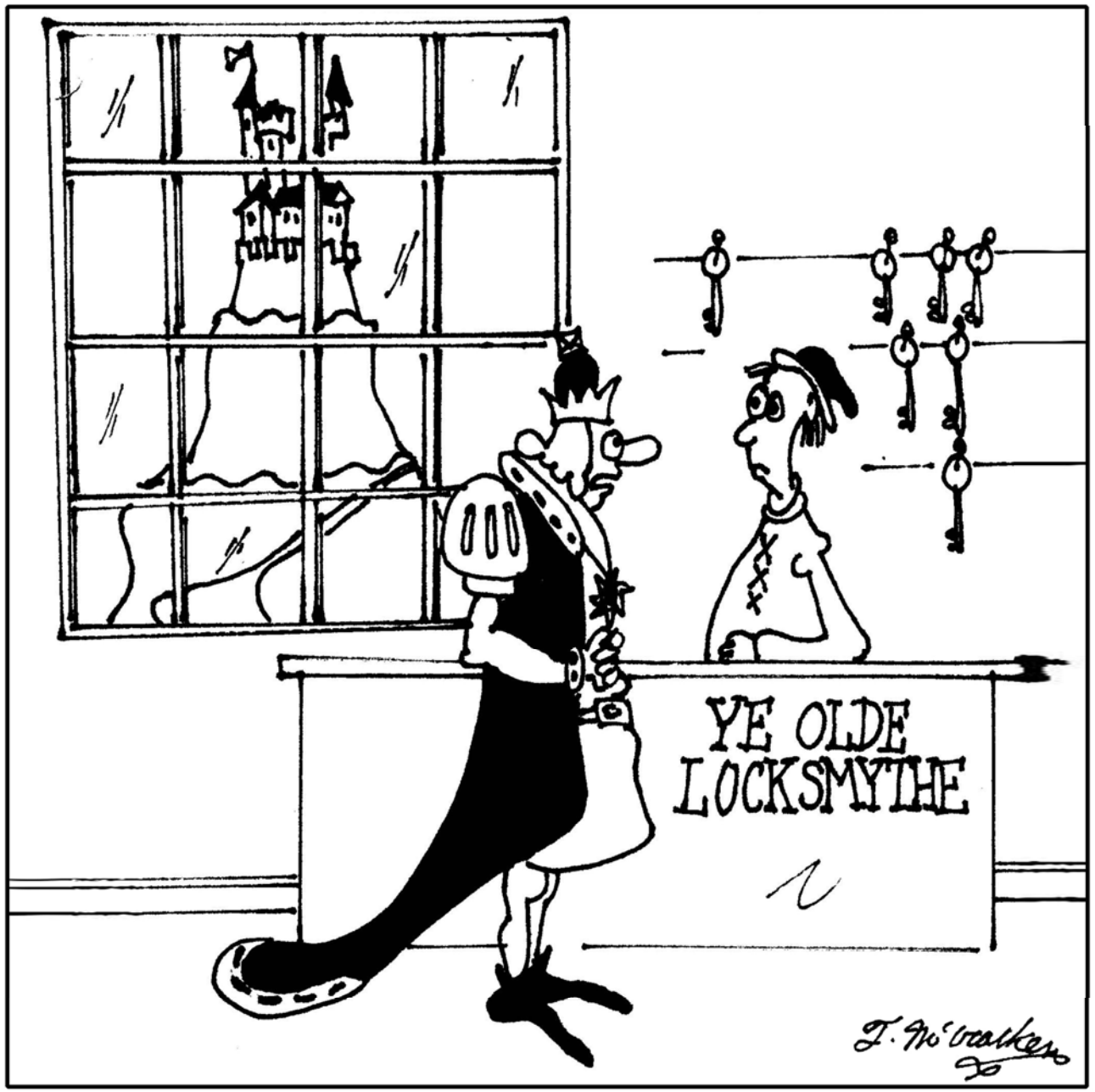


"I lost my key to the kingdom."

Federal PKI
Management Authority
Enabling Trust

GSA

Why doesn't my badge let me in my building? It worked yesterday!

Darlene Gore, FPKIMA Program Manager, GSA
John DiDuro, FPKIMA Security Team Lead
India Donald, FPKIMA Security Analyst

Federal PKI
Management Authority
Enabling Trust

GSA

Learning Objectives

1. Understanding of the Federal Public Key Infrastructure (FPKI)
2. Awareness of the Federal Public Key Infrastructure Management Authority (FPKIMA) mission
3. Learning of recent attacks by the advanced persistent threat against certification authorities (CAs) world-wide
4. Understanding how the FPKIMA's incident response capability helps to ensure US Government continuity of operations

Agenda

I. FPKIMA Background
II. Why Does US-CERT Care?
III. Incident Response Use Cases
IV. Looking Forward

Federal PKI Management Authority
Enabling Trust

GSA

Agenda

- FPKIMA Background
  - What is the FPKI
  - b. Who we are
  - c. What we do
  - d. What we protect
- II. Why Does US-CERT Care?
- III. Incident Response Use Cases
- IV. Looking Forward

Federal PKI Management Authority
Enabling Trust

GSA

The 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 HSPD-12/PIV, OMB M-04-04, PIV-I, Third-party Credentials, Backend Attribute Exchange (BAE), National Strategy for Trusted Identity in Cyberspace (NSTIC), and meets the expectations of e-government initiatives.
- Provides the **trust anchor** for the Federal Government's HSPD-12/PIV and other FPKI services.
- Considered a high priority, mission-critical service to the Federal Government. **System availability is essential to providing all services necessary to meet the aforementioned government wide objectives**.

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 and contractors required by HSPD-12 to use PIV for logical and physical access.
  - Shared Service Providers and certified PIV-I issuers relying on the trust chain provided by the federal root.
  - Relying parties who depend on certificate paths through the Federal Bridge CA to validate certificates issued by an FPKI Affiliate.
  - External relying parties validating FPKI community credentials to the Federal Common Policy CA root certificate as a trust anchor.

Federal PKI Management Authority
Enabling Trust

GSA

Customers of the FPKIMA

Certificates Issued by the FPKI Trust Infrastructure CAs

- FBCA (11):

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

- SHA-1 Federal Root (10):

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

- Common Policy (11):

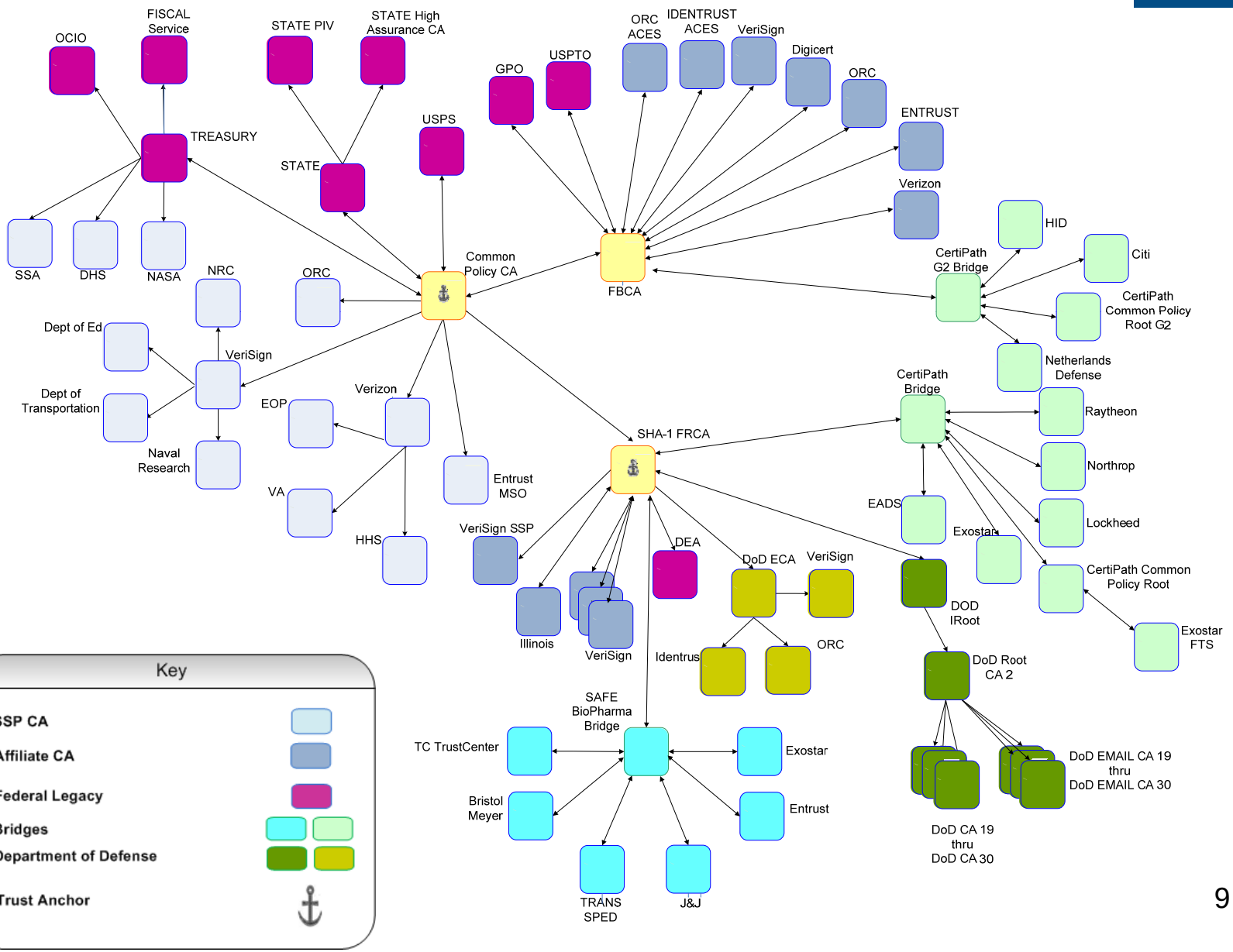
Federal Bridge
SHA-1 Federal Root
Department of Treasury
Department of State
VeriSign
Verizon Business
Entrust
ORC (2)
Legacy-Common Policy (issued to Common Policy)
SHA-1 Federal Root

- E-Governance CAs (4):

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

Federal PKI Management Authority
Enabling Trust

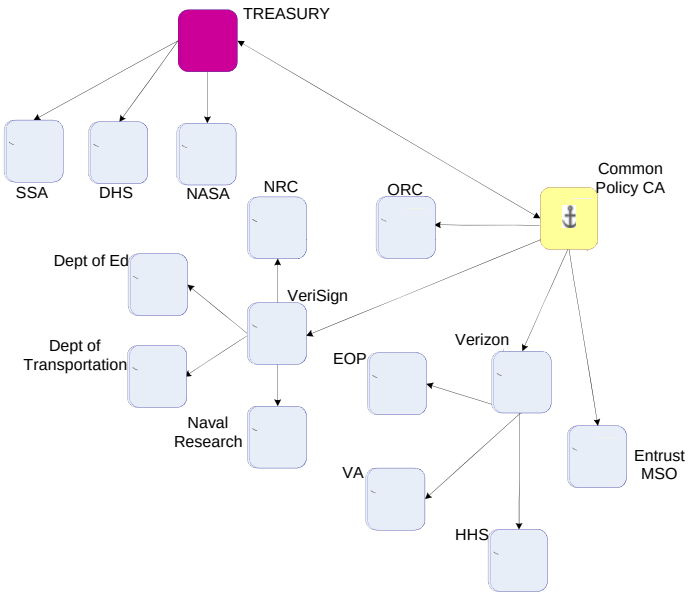
The Federal PKI



Federal PKI Management Authority
Enabling Trust

The Federal PKI (cont.)

GSA



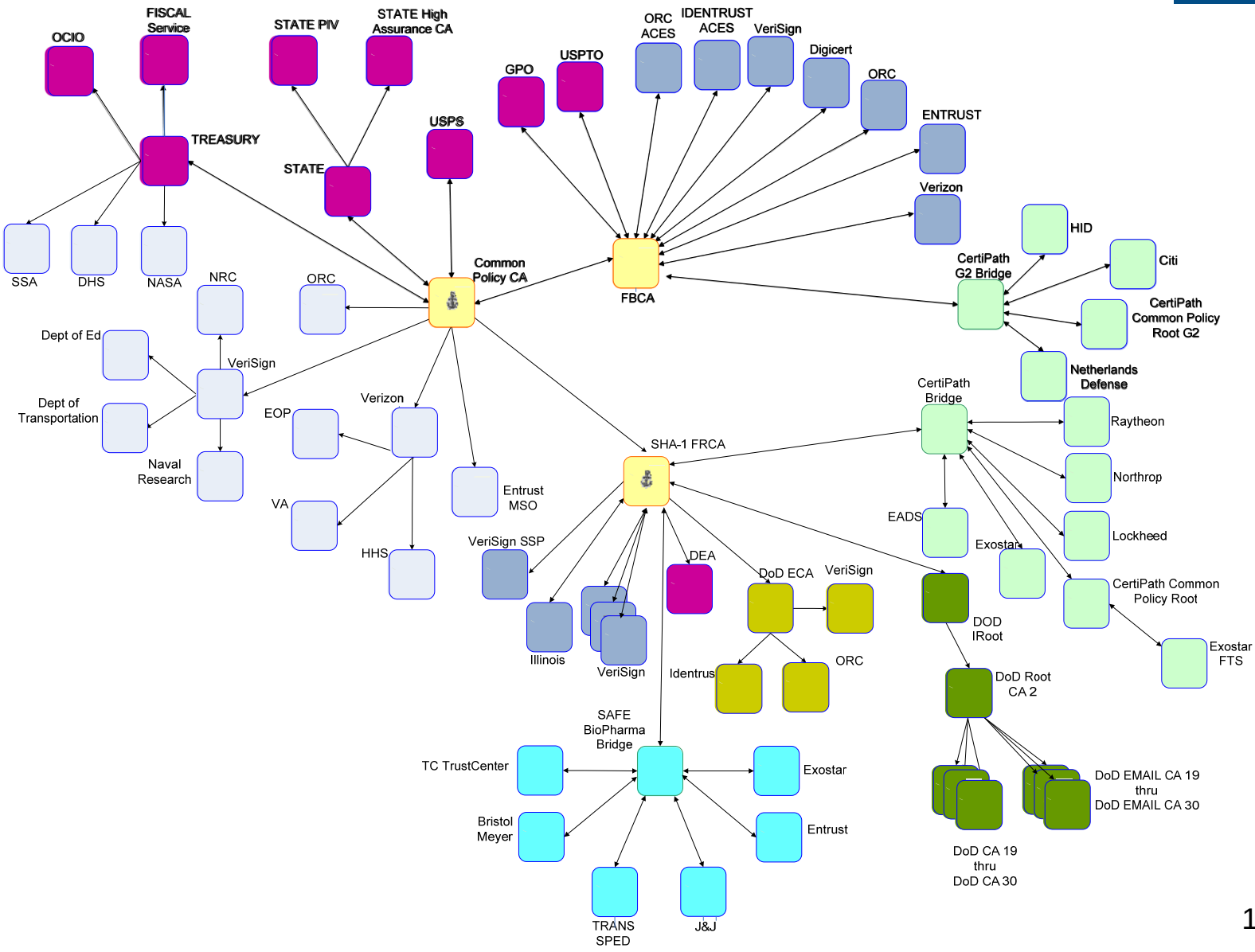
- Common Policy Root CA
  - Trust Anchor for PIV and the US Federal Government

Shared Service Providers

- Issue PIV credentials to federal employees, federally-owned devices, and federal contractors.
- Issue certificates in accordance with the Common Policy Certificate Policy.

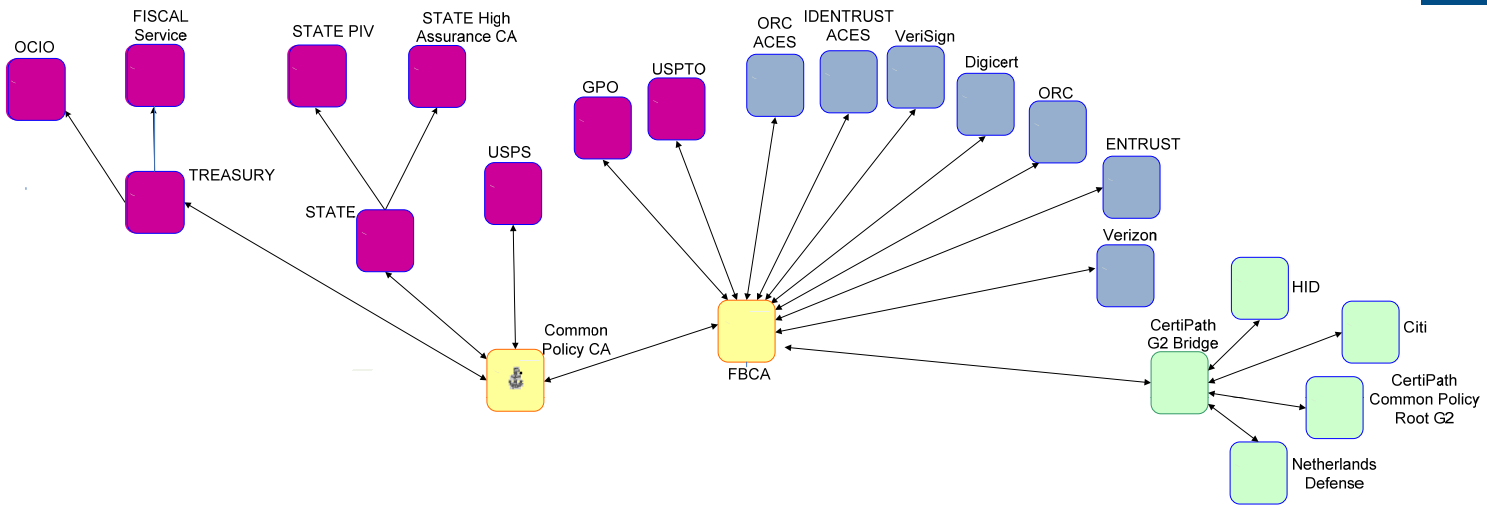
Federal PKI Management Authority
Enabling Trust

The Federal PKI (cont.)



Federal PKI Management Authority
Enabling Trust

The Federal PKI (cont.)



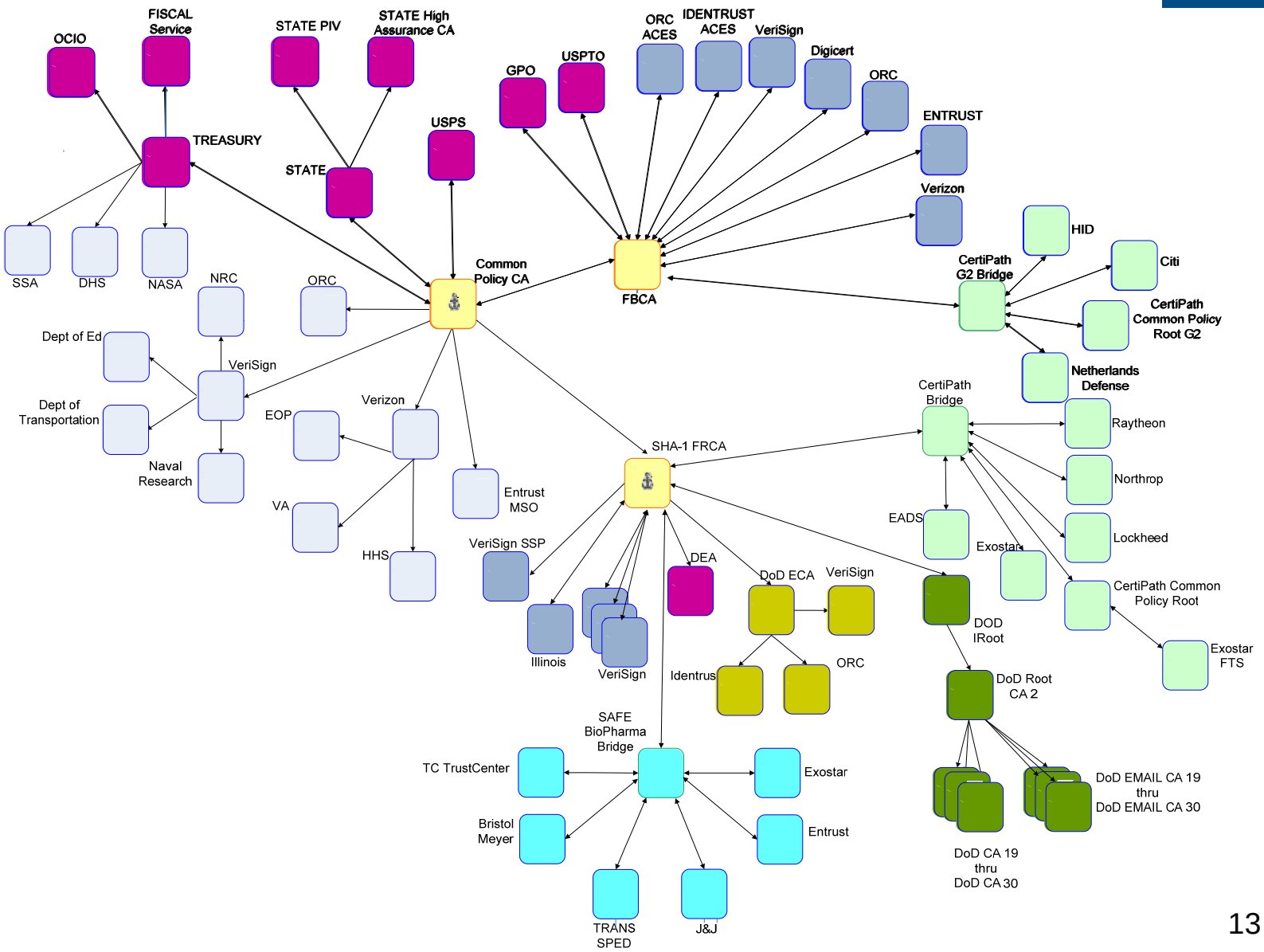
- Federal Bridge CA
  - Maps trust between Affiliate PKIs
  - Maps trust between PIV and PIV-I

Affiliates

- Legacy Federal Agencies
- Industry sector Bridges
- PIV-I issuers
- Commercial PKIs

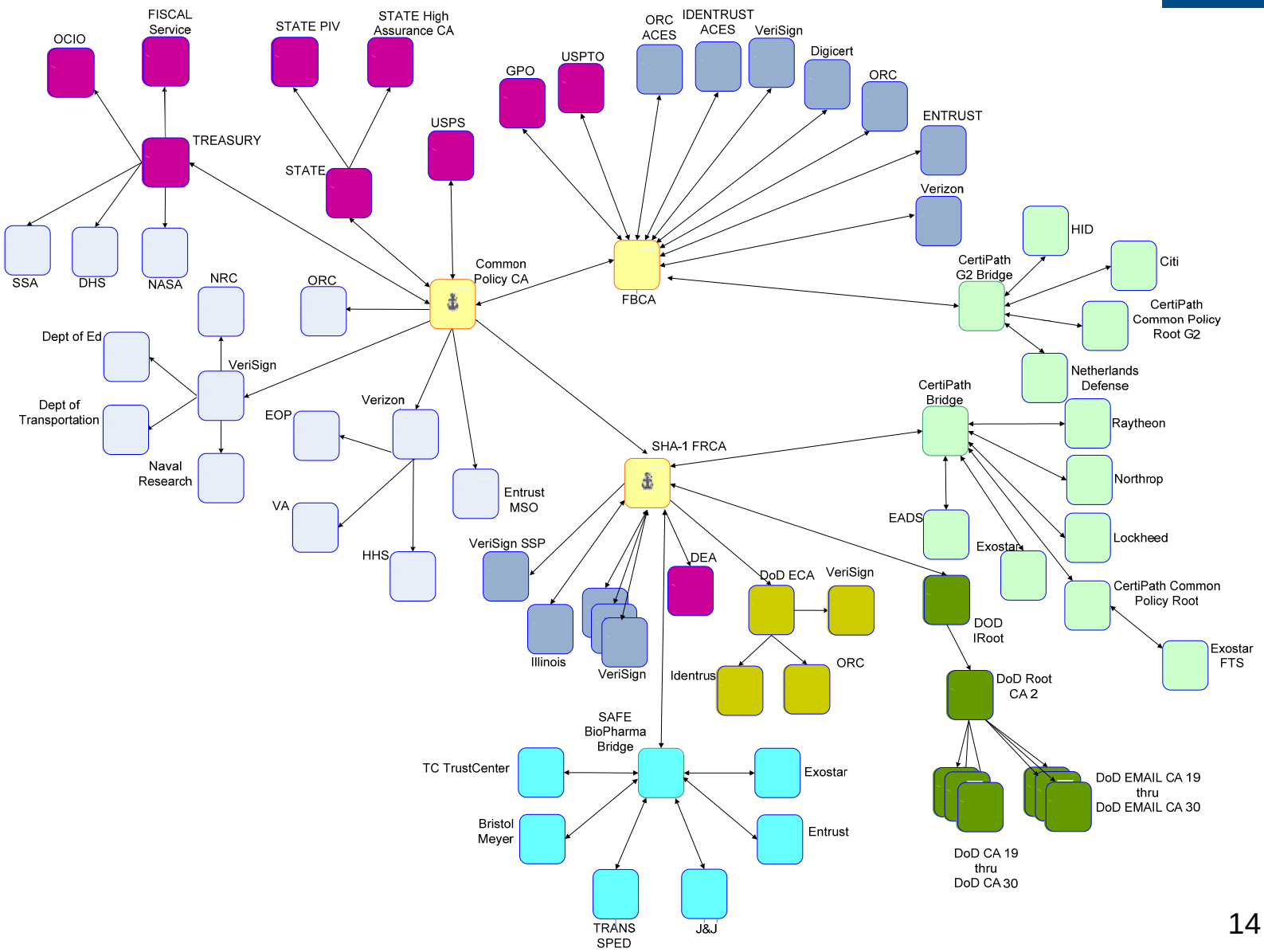
Federal PKI Management Authority
Enabling Trust

The Federal PKI (cont.)



Federal PKI Management Authority
Enabling Trust

The Federal PKI (cont.)



Federal PKI Management Authority
Enabling Trust

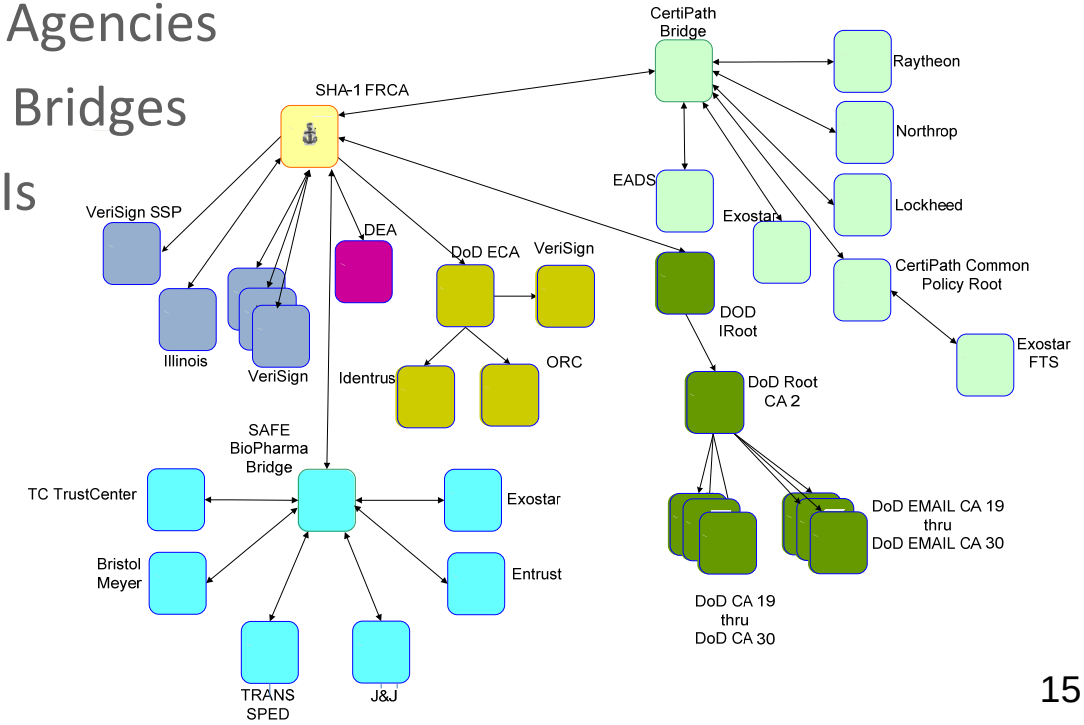
The Federal PKI (cont.)

GSA

- SHA-1 Federal Root CA
  - Provides a SHA-1 Trust Anchor
  - Maps trust similar to FBCA
  - Ends 12/31/2013

SHA-1 Partners

- Legacy Federal Agencies
- Industry sector Bridges
- Commercial PKIs



Federal PKI Management Authority
Enabling Trust

GSA

Agenda

- FPKIMA Background
  - ✓ What is the FPKI
  - What we do
  - c. What we do
  - d. What we protect
- II. Why Does US-CERT Care?
- III. Incident Response Use Cases
- IV. Looking Forward

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.
- FPKIMA Program Manager resides within GSA's Federal Acquisition Service (FAS), Office of Integrated Technology Services (ITS), Security Services Division headquartered in Fairfax, VA.
- Find us at:

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

Federal PKI Management Authority
Enabling Trust

GSA

Who We Are – The Big Picture

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
- ENFORCE
- 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	Community	Program Management
Manage systems and services	Implement policy and security controls to protect platform	Board, manage, and support entities	Collaborate and test solutions for the advancement of the trust infrastructure	Provide program oversight and control

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

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

Federal PKI Management Authority
Enabling Trust

GSA

Agenda

- FPKIMA Background
  - ✓ What is the FPKI
  - ✓ Who we are
  - What we do
  - d. What we protect
- II. Why Does US-CERT Care?
- III. Incident Response Use Cases
- IV. Looking Forward

What We Do – Infrastructure Management

- Perform Infrastructure (IT Service) Management
  - Manage the FPKI Trust Infrastructure CAs and their repositories.
    - Federal Bridge CA (FBCA)
    - Common Policy CA (FCPCA)
    - SHA-1 Federal Root CA (SHA-1 FRCA)
    - E-Governance CAs (EGCA)
  - Network Operations
  - Monitoring and Reporting
  - Operate the FPKI Service Desk
    - FPKIPA-MA@listserv.gsa.gov
    - 1-888-754-1229 (1-888-PKI-1A2Z)

What We Do - Certificate Services

- Manage the full life cycle of digital certificates issued by the FPKI Trust Infrastructure:
  - Certificate Issuance (Scheduled)
  - Certificate Renewal/Modification (Scheduled)
  - Certificate Revocation (Scheduled or Immediate)
  - Certificate and CRL Publication
  - Quality Assurance of:
    - Requests
    - Issued Certificates

What We Do - Repository Services

- Manage directory servers and network devices that enable relying parties both within and external to the FPKI Community to locate certificate status information for certificates issued:
  - Within the Federal Government
  - Outside the Federal Government
    - State, local and tribal governments
    - Commercial bridges: SAFE-BioPharma & CertiPath
    - Foreign entities

What 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
  - ✓ What is the FPKI
  - ✓ Who we are
  - ✓ What we do
  - What we protect
- II. Why Does US-CERT Care?
- III. Incident Response Use Cases
- IV. Looking Forward

What We Protect - Context

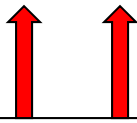
- Cyber security attacks are commonplace
- Identity Theft is commonplace
- Attacker sophistication is increasing
  - Advanced Persistent Threat
  - Organized Crime
  - Cloud based “attack for hire”
  - PKI elements being attacked

What We Protect – Higher Assurance

Authentication Assurance Levels (per OMB M-04-04)

"A breech (false positive authentication) at each assurance level has ramifications"

OMB M-04-04 Risk Impacts	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**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



FPKIMA Root CA and CRLs enable these higher assurance levels

Federal PKI Management Authority
Enabling Trust

GSA

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
- ENFORCE
- 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	Community	Program Management
Manage systems and services	Implement policy and security controls to protect platform	Board, manage, and support entities	Collaborate and test solutions for the advancement of the trust infrastructure	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

We protect sensitive artifacts …

Federal PKI Management Authority
Enabling Trust

GSA

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

ICAM	FPKIPA	GSA
Fostering effective identity and access management government-wide and between external business partners, by enforcing digital certificate standards for trusted identity authentication	Enforce digital certificate standards for trusted identity authentication across the federal agencies and …usiness partners	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	Community	Program Management
Manage systems and services	Implement policy and security controls to protect platform	Board, manage, and support entities	Collaborate and test solutions for the advancement of the trust infrastructure	Provide program oversight and control

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

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

… and foundational trust. As well as …

Federal PKI Management Authority
Enabling Trust

GSA

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

ICAM	FPKIPA	GSA
Fostering effective identity and access management government-wide and between external business partners, by enforcing digital certificate standards for trusted identity authentication	Enforce digital certificate standards for trusted identity authentication across the federal agencies and between external business partners	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

Platform Management	Security Management	Relationship Management	Community	Program Management
Manage systems and services	Implement policy and security controls to protect platform	Board, manage, and support entities	Collaborate and test solutions for the advancement of the trust infrastructure	Provide program oversight and control

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

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

… Affiliate PKI's…

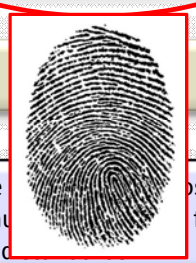
Federal PKI Management Authority
Enabling Trust

GSA

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

ICAM	FPKIPA	GSA
Fostering effective identity and access management government-wide and between external business partners, by enforcing digital certificate standards for trusted identity authentication	Enforce digital certificate standards for trusted identity authentication across the federal agencies and between external business partners	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 and between external business partners through the execution of digital certificate policies and…

FPKIMA Primary Functions: Fundamental building blocks of the program

Platform Management	Security Management	Relationship Management	Community	Program Management
Manage systems and services	Implement policy and security controls to protect platform	Board, manage, and support entities	Collaborate and test solutions for the advancement of the trust infrastructure	Provide program oversight and control

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

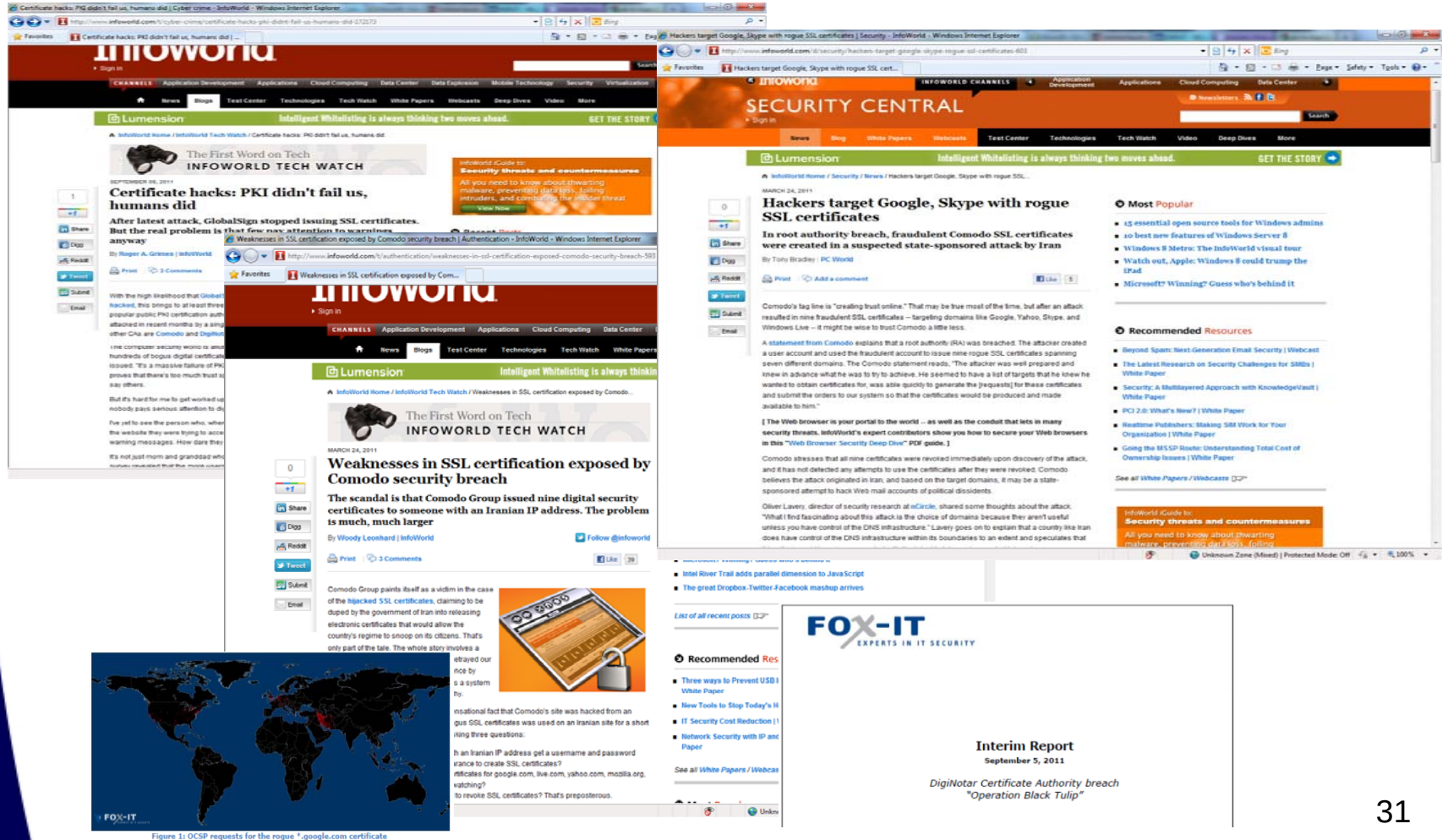
Certificate Services	Privacy Protection	Boarding	Thought Leadership	Planning
Repository Services	Physical & Logical Protection	Policy Compliance	Technical Exploration	Communications
Configuration Management	Monitoring & Reporting	User Support	Testing	Performance Reporting
Monitoring & Reporting	Security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

… and Authentication Assurance.

Federal PKI Management Authority
Enabling Trust

GSA

Cost of Broken Controls? Broken Trust.



Federal PKI Management Authority
Enabling Trust

GSA

What We Protect - Cost of Broken Protection

- **U.S. Government Sensitive Artifacts compromised?**
  - Disruption in government services and business
  - Adverse effect on individual privacy
  - Denied access to government facilities once PIV is omnipresent
  - Denied access to official systems

- **Foundational Trust 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

What We Protect - Cost of Broken Protection

- **Protection of Affiliates Undermined?**
  - Disruption of Affiliate PKI's trust chains
  - Re-establish a new Federal Root CA
  - Revocation and re-issuance of cross certificates to Federal agencies and Shared Service Providers
  - Chaos in electronic-government solutions until resolved

- **Authentication Assurance 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

Federal PKI Management Authority
Enabling Trust

GSA

Agenda

- ✓ FPKIMA Background
- ➢ Why Does US-CERT Care?
  - ➢ Policy Drivers
  - b. APT Drivers
  - c. FPKI Usage Statistics
- II. Incident Response Use Cases
- III. Looking Forward

Why Does US-CERT Care? – Policy Drivers

- The FPKI is a far-reaching trust fabric
  - Criticality
    - Facilitates trust within government and by non-government entities
    - Provides credential provisioning or authentication services to a wide variety of consumers
    - Provides high assurance and reliability for commercial and other public entities through mechanisms such as the Federal Bridge CA and Common Policy CA
  - Impact
    - Significant impact on a multitude of business processes.
    - Daily business activities leverage it for identity and access management.
  - Increasing Dependence
    - Repository traffic will increase
    - More agencies and applications will become dependent on the certificate service backbone

Why Does US-CERT Care? – FPKI Policy Drivers

- Federal mandates for implementing e-government and electronic signature technology. For example:
  - Government Paperwork Elimination Act of 1998
  - E-Sign Act of 2000
  - E-Government Act of 2002
  - Homeland Security Presidential Directive (HSPD 12)
  - OMB Memorandum 04-04
  - OMB Memorandum 05-05
  - OMB Memorandum 11-11
  - NIST SP 800-63
  - FIPS 201
  - OMB Van Ruenkel Memorandum of October 2011

Why Does US-CERT Care? – FPKI Security Drivers

- Policy drivers
  - FISMA
  - OMB Circular No.A-130, Appendix III
  - Federal PKI policies
- Security Policies
  - GSA IT Security Policy
  - FPKIMA Security Policy
  - PKI Security Profile

Federal PKI Management Authority
Enabling Trust

GSA

Agenda

- ✓ FPKIMA Background
- ➢ Why Does US-CERT Care?
  - ✓ Policy Drivers
  - ➢ APT Drivers
  - c. FPKI Usage Statistics
- II. Incident Response Use Cases
- III. Looking Forward

Why Does US-CERT Care? – APT Drivers

- GAO reports that security incidents among 24 key agencies increased more than 650% in the last five years
- New vulnerabilities may compromise FPKI CAs and allow adversaries to issue PIV or PIV-I ***forgeries that could be undetectable*** by federal agencies and other relying parties
- White House Cyber Security Priorities
  - Trusted Internet Connections
  - Continuous Monitoring of Federal Information Systems
  - Strong Authentication

Federal PKI Management Authority
Enabling Trust

GSA

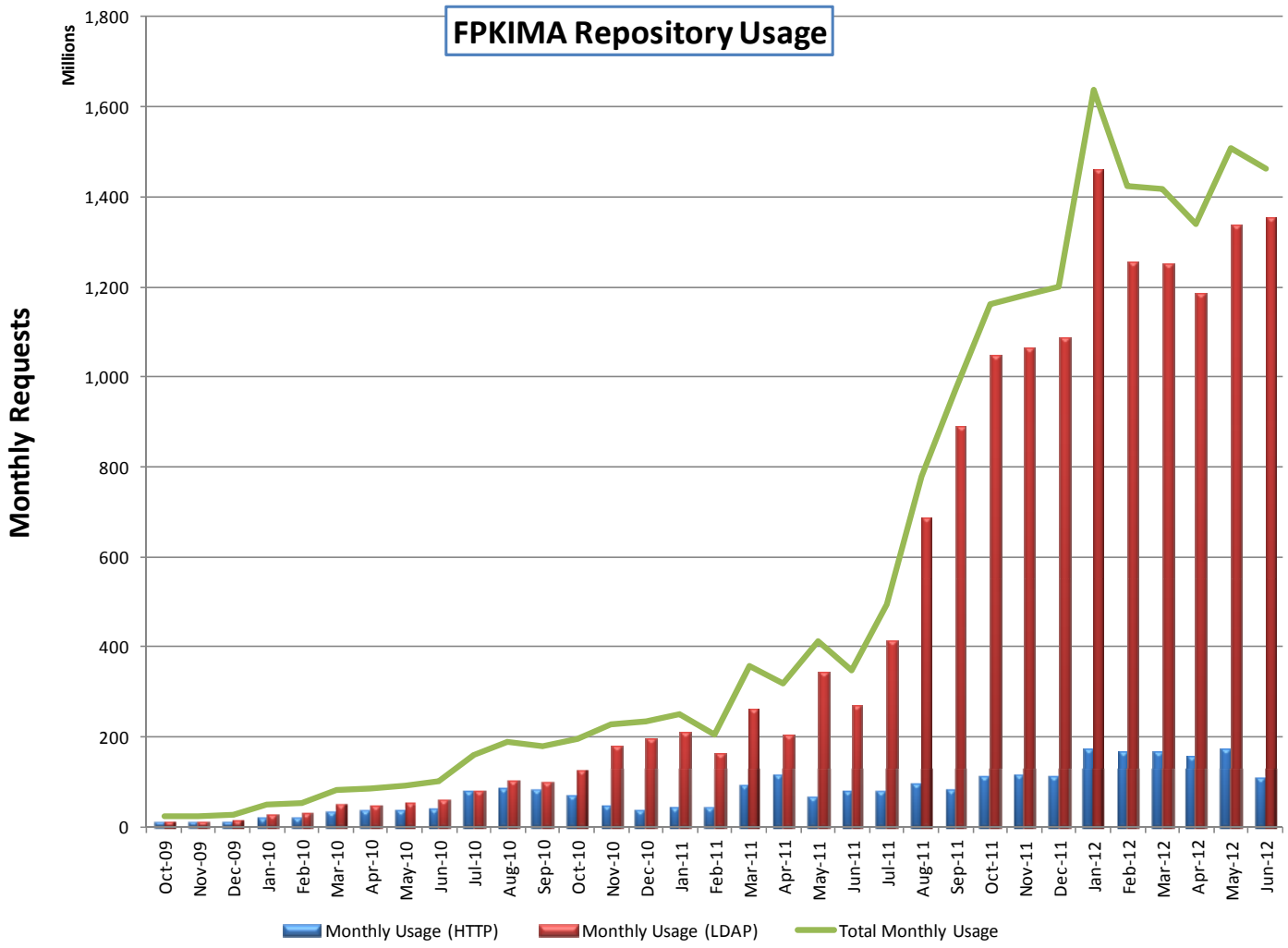
Agenda

- ✓ FPKIMA Background
- ➢ Why Does US-CERT Care?
  - ✓ Policy Drivers
  - ✓ APT Drivers
  - ➢ FPKI Usage Statistics
- II. Incident Response Use Cases
- III. Looking Forward

Federal PKI Management Authority
Enabling Trust

GSA

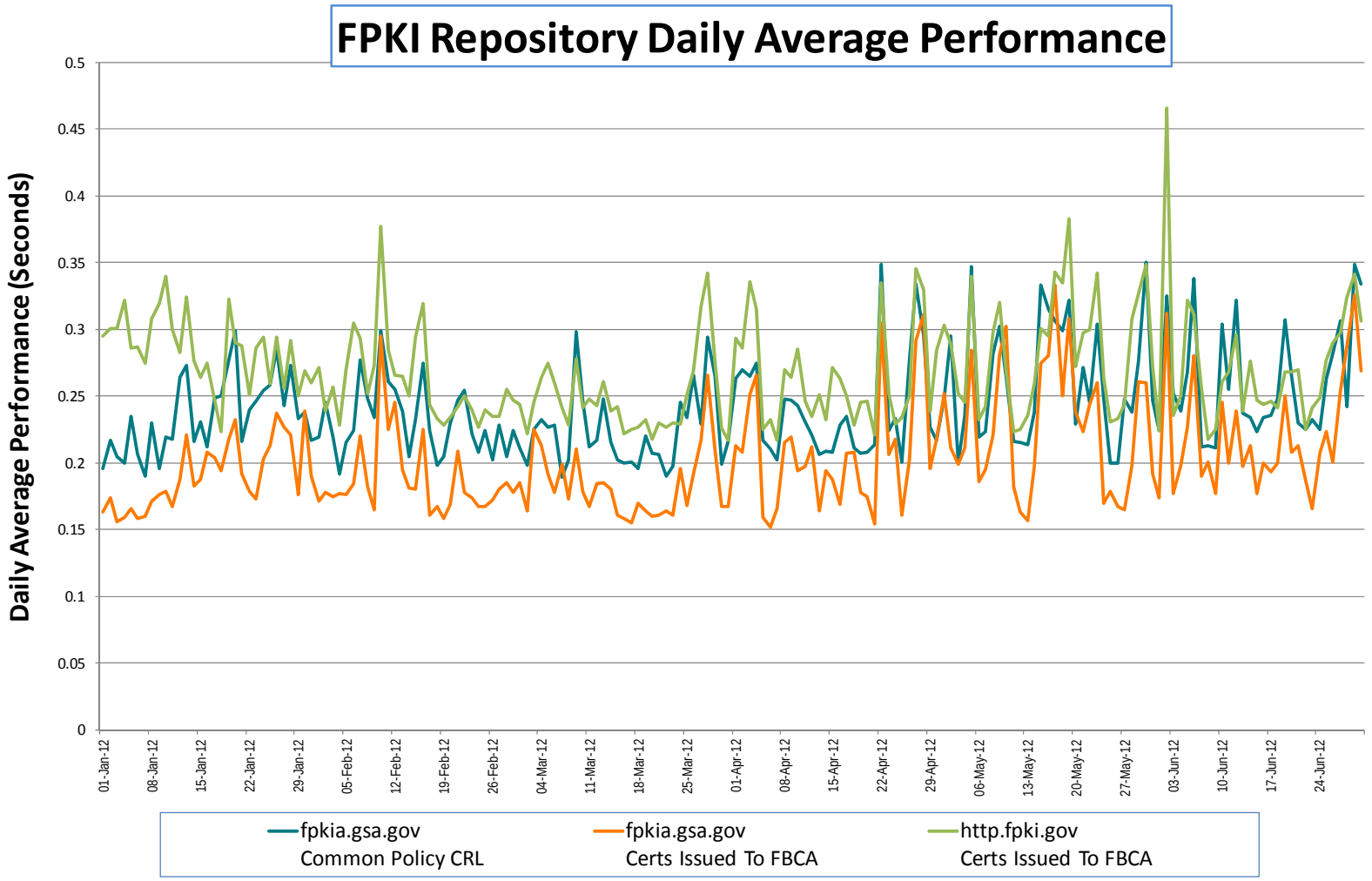
FPKI Usage Statistics – Platform Usage



Federal PKI Management Authority
Enabling Trust

GSA

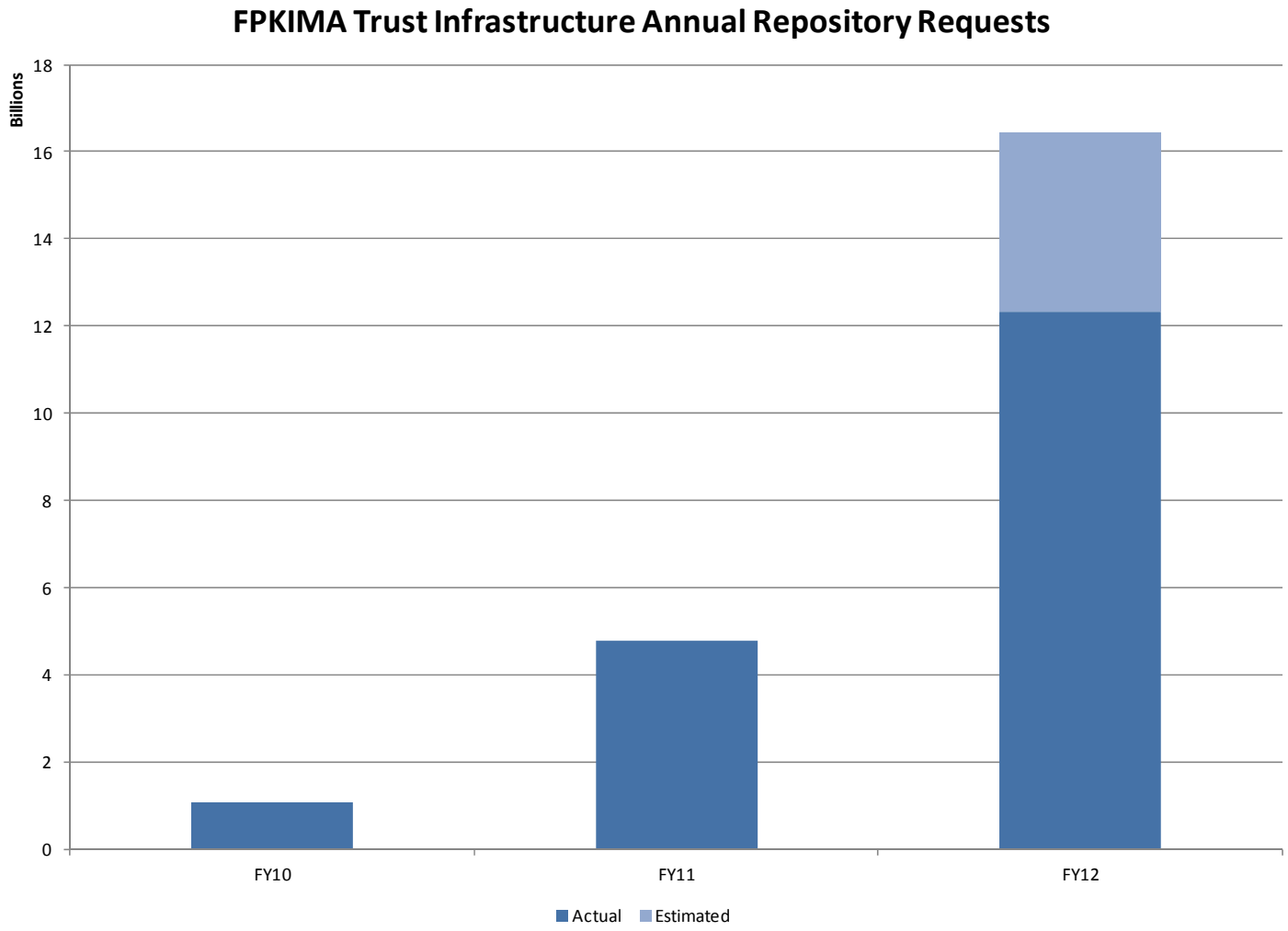
FPKI Usage Statistics – Platform Performance



Federal PKI Management Authority
Enabling Trust

GSA

FPKI Usage Statistics – Repository Requests



Agenda

- ✓ FPKIMA Background
- ✓ Why Does US-CERT Care?
- ➢ Incident Response Use Cases
- IV. Looking Forward

Incident Response #1: Flame Malware (aka Skywiper)

- Attacks computers running Microsoft Windows operating system
  - Per NSA: highly-sophisticated, multi-functional malware
  - Signed by a fraudulent Microsoft code-signing certificate, which makes Flame look like a valid Microsoft executable
    - Leverages the weak MD5 hash algorithm and unintended code-signing extension
    - Implemented a new variation of prefix-chosen collision attack to create a new certificate that appears to be a valid Microsoft code-signing certificate
- The fake certificate did not have any of the normal extensions such as AIA, CRLDP, or OCSP.
  - Therefore, it appears that operating systems were not performing revocation checking while validating the signature on the Flame malware.
- Warrants NSA Guidance
  - Information Assurance Directive No. IAA-003-2012
  - "it is likely that this malware will be reverse engineered and re-purposed against new targets"

Incident Response #1: Flame Malware (con't)

- A Flame-like attack on the FPKI Trust Infrastructure or FPKI Community PKIs could undermine trustworthiness - the essence of the FPKI
  - Certificates may have to be revoked (perhaps en masse), which would preclude logical and physical access for example
  - G2G, B2G, and C2G objectives could be negatively impacted
  - Cost of recovery could be significant
- Propagation of guidance to the FPKI Community. For example:
  - Implement Microsoft patches that address Flame
  - Follow NIST Guidance regarding key length
  - Ensure all certificates have a valid CRLDP / OCSP
  - Validate the CA signature of Certificate Revocation Lists
  - Review all application, browser, and operating system certificate trust stores for MD5. Then work with vendors to get all of these revoked and removed from the trust store as soon as possible

Incident Response #2: DigiNotar

- DigiNotar was a Dutch CA that suffered an attack that resulted in fraudulent certificates being issued.
  - SSL certificates
  - Including ones for Google.com, Yahoo.com, and Mozilla.com domains
- The fraudulent Google.com certificates were used for man-in-the middle attacks against Google services
- DigiNotar issued certificates in several contexts
  - In its own name (DigiNotar Root CA)
  - For use by the Dutch government's PKI Program
    - These DigiNotar certificates chained to the Dutch government's Root CA
- The Dutch Government used the DigiNotar certificates to validate identities of many of its web sites or other customers in their PKI Program

Incident Response #2: DigiNotar (con't)

- All major browser vendors had to issue updates that removed DigiNotar from their browser trust stores, which prevented end users from accessing web sites relying on DigiNotar-issued certificates
  - Non-government web sites
  - Dutch Government web sites providing various government services
- DigiNotar went bankrupt – within three months of initial breach
  - Loss of trust in its certificates
    - removal from browsers
    - Dutch government decision to terminate them as a CA
  - Uncertainty of cost to recover

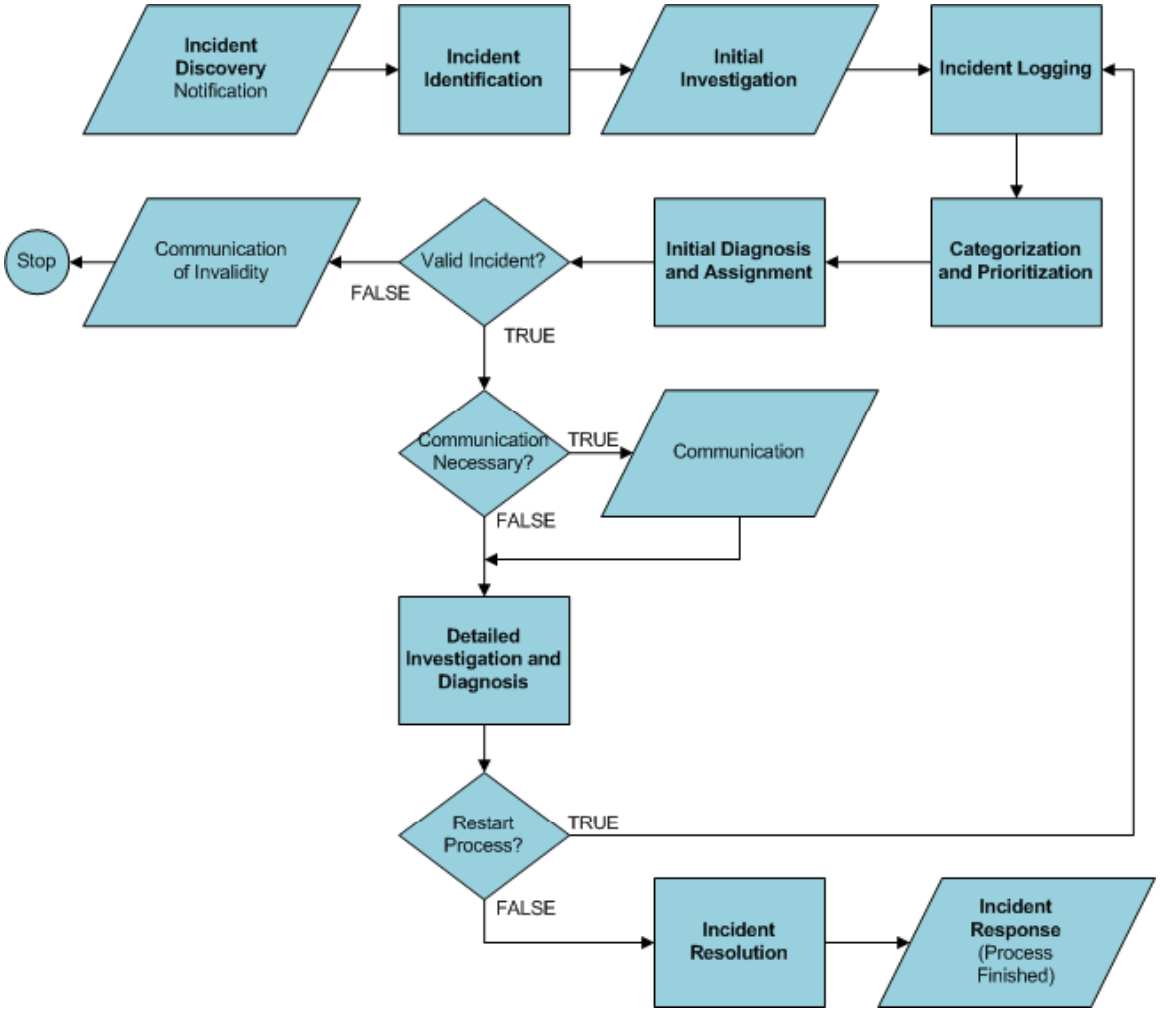
Incident Response #2: DigiNotar (con't)

- The DigiNotar incident is an import lesson for the FPKI
- Issuance of fraudulent certificates within the FPKI could have similar consequences
  - Loss of trust in issued certificates, which means revocations and loss of physical and logical access for example.
  - Increased threat of attacks throughout the community, which means confidentiality, integrity, and availability are at increased risk
  - Costs to recover
  - Diminished reputation
- Upon being alerted of the DigiNotar incident, the FPKI:
  - Began researching and analyzing the incident
  - Immediately notified the FPKI Community to not trust the DigiNotar Root CA by actively managing the PKI Trust Stores in browser products

Incident Response #3: Hypothetical FPKI Breach

- A new vulnerability compromises FPKI CAs
  - Federal agency CAs issuing PIV Cards; and/or
  - Non-federal CAs issuing PIV-I Cards
- The breach allows the attacker to issue PIV or PIV-I forgeries
  - Relying Party physical and logical assets may be at risk
  - End user information may be at risk
- Upon detection, the FPKI Community Incident Management Process is initiated. This includes
  - Incident Notification
  - A message alert at time of discovery
  - Summary message within 24 hours

Incident Response #3: Hypothetical FPKI Breach (con't)



Incident Response #3: Hypothetical FPKI Breach (con't)

- Upon diagnosis – immediate action is taken to:
  - Revoke certificates as necessary
  - Apply remediation steps to eliminate the breach/vulnerability
  - Issue new legitimate certificates as necessary
  - Identify lessons learned for future use

Agenda

- ✓ FPKIMA Background
- ✓ Why Does US-CERT Care?
- ✓ Incident Response Use Cases
- ➢ Looking Forward

Looking Forward - What We Need from US-CERT

- Provide feedback as to whether a need exists for a "PKI Desk"
  - Perhaps the FPKIMA provides
- If/When US-CERT conducts cybersecurity exercises, include an FPKI Scenario

Looking Forward - What The FPKIMA Is Doing

- Increased coordination and communication within the FPKI Community and with external security sources such as security organizations and vendors
- Continuous Monitoring
  - Quarterly FISMA Assessment and Vulnerability Scans
- Advanced Persistent Threat (APT) Counter Measures
  - Coordination with US-CERT
  - Security Operations Center (SOC) Foundations
- Pursuing additional FISMA security controls

Looking Forward - What The FPKIMA Is Doing (cont.)

- Internal Monitoring
  - Provide real-time log aggregation, analysis and alerting of anomalies
- External Monitoring
  - End user performance and availability
  - Availability checks across multiple protocols
  - CRL expiration checks
- Reporting
  - Performance from external monitoring
  - Usage from internal monitoring

Federal PKI
Management Authority
Enabling Trust

GSA

Learning Objectives Review

1. We described the Federal Public Key Infrastructure (FPKI) and discussed its importance
2. We explained the mission of the Federal Public Key Infrastructure Management Authority (FPKIMA)
3. We provided scenarios of recent attacks by the advanced persistent threat against certification authorities (CAs) world-wide
4. We outlined the FPKIMA's incident response capabilities and how they relate to US-Cert

QUESTIONS?

Federal PKI Management Authority
Enabling Trust

GSA

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

John DiDuro

FPKIMA Security Team Lead

Protiviti, Inc.

D: 703-299-4718

C: 202-345-3412

john.diduro@gsa.gov

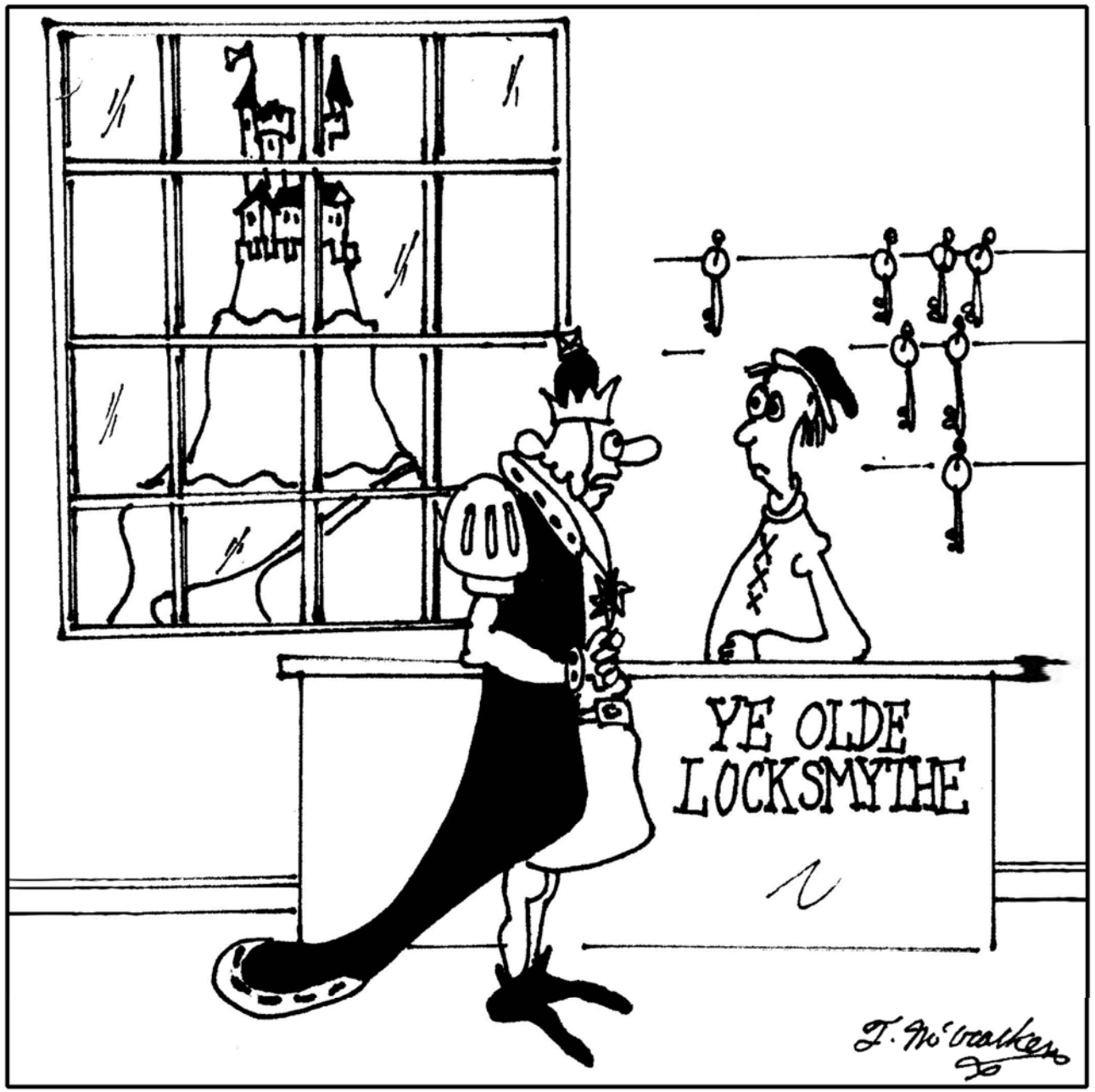
India Donald

FPKIMA Security Analyst

Protiviti, Inc.

D: 703-299-4726

india.donald@fpki.gov



"I lost my key to the kingdom."