Interagency Advisory Board

Meeting Agenda, Wednesday, May 23, 2012

1. **Opening Remarks** *(Mr. Tim Baldridge, IAB Chair)*
2. **Revision of the Digital Signature Standard** *(Tim Polk, NIST)*
3. **Update on Content and Status of FIPS 201-2** *(Hildy Ferraiolo, NIST)*
4. **The Importance, Expectation, and Value of FPKIMA** *(Chris Louden)*
5. **Use of PIV/CAC as a Payment Token in Transit Applications** *(Greg Garback, WMATA)*
6. **Closing Remarks** *(Mr. Tim Baldridge, IAB Chair)*

Federal PKI
Management Authority
Enabling Trust

GSA

FPKIMA Briefing
May 23, 2012

Chris Louden

Agenda

- Context
- PKI Enables…
- What is the FPKIMA
- Transaction Volume

Context

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

Context

- HSPD-12

  Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

Context

- Cyber Security Priorities
  1. Trusted Internet Connections (TIC)-
  2. Continuous Monitoring of Federal Information Systems
  3. **Strong Authentication**– Passwords alone provide little security. Federal smartcard credentials such as PIV (Personnel Identity Verification) and CAC (Common Access Cards) cards provide multi-factor authentication and digital signature and encryption capabilities, authorizing users to access Federal information systems with a higher level of assurance.

PKI Enables: Background

- Public Key Infrastructure (PKI)
  - Refers to the infrastructure needed to make use of Public Key Cryptography in the real world
- Public Key Cryptography
  - Asymmetric Cryptography
    - 2 Key system
    - Encrypt with one key, decrypt with the other

PKI Enables: Background

- Public Key Cryptography (Asymmetric Cryptography)
  - Everyone generates 2 Keys
  - Anything encrypted with one key is decrypted with the other
  - Publish one of the keys, call it a “Public Key”
  - Keep the other key safe, call it a “Private Key”
    - Best way to protect is to generate and store on a smart card

PKI Enables

- Encryption
  - Alice Encrypts a file using Bob's Public Key, Bob decrypts it with his Private Key
    - In practice PK used to encrypt a session key
  - Enables data privacy, ability to securely transfer files without sharing session keys

PKI Enables

- Digital Signature
  - Bob signs a file with his Private Key, Anyone can validate the signature using Bob's Public Key
    - Sign by using the private key to encrypt a hash of the document
    - Validation ensures Alice signed it and the document is unchanged
  - Enables proof of origin to mitigate phishing, mitigates data corruption/tampering, enables paper processes to move online, etc

PKI Enables

- Authentication
  - Challenge user to “prove possession of the private key”
  - Use of “Signed Authenticators”
    - Biometrics, CHUIDS, etc
  - Enables strong LOA4 authentication to physical and logical access systems, SSL, Mutual SSL/TLS

PKI Enables

- Everything depends on having the right Public Key
  - If it's not really Bob's Public Key…
  - Is Alice using Bob's public Key or an Attacker's public key?

PKI Enables: Certificate Authorities

- Certification Authorities (CAs)
  - Issue signed Certificates that bind a subject to a Public Key
    - Attest that this is really Bob's Public Key
  - Issue signed Certificate Revocation Lists (CRLs)
    - List of any certificates that shouldn't be trusted
    - Updated periodically
  - Operate Repositories
    - Contain CRLs and Certificates issued by the CA
  - CAs drive alignment and interoperability by enforcing consistent standards and policies
  - The Infrastructure in the Public Key Infrastructure

PKI Enables: Certificate Authorities

- Summary
  - Public Key Cryptography provides Encryption, Signature, and Authentication
    - Assuming you know you have the right public key
  - CAs let you know you have the right key
    - Issue signed certificates binding Bob to his public key
  - Enable Alice and Bob to *trust* each other
  - Alice and Bob trust the CA, so they can *trust* each other
  - CAs enforce consistent standards and policies, so Alice and Bob can *interoperate*
  - *Certificate Authorities Enable PKI*

PKI Enables: Certificate Authorities

- *Why* trust a CA?
  - Published Policies
    - Certificate Policy
    - (A CA can have multiple policies, identified in each certificate)
    - Certificate Profiles
  - Independent Audits
    - Confirms CA practices meet policies
- Local policies generally dictate which CAs to trust
  - Considerable diligence and expertise required to judge the trustworthiness of a CA

PKI Enables: Certificate Authorities

- *How* do you trust a CA?
  - You need the CAs public key to validate their Certificates
    - How do you know you have the right public key?
    - CAs have certificates, just like Bob
  - Who certified the CA? Who signed their certificate?
    - CAs can sign certificates for other CAs
    - Ultimately some CA starts the chain of trust
      - The root of trust for the other CAs
      - Root CAs sign their own certificates, called “Trust Anchors”
  - Trust Anchors have to be “Pre-Installed” before PK operations can work

Agenda

- ✓ Context
- ✓ PKI Enables
- ➢ What is the FPKIMA
- Value
- Infrastructure

What is the FPKI Management Authority

- Responsible for FPKI Trust Infrastructure
  - Operates Certification Authorities for the FPKI
  - Operates the Common Policy Root
  - Operates the Federal Bridge CA (FBCA)
  - Operates the SHA-1 Federal Root (SHA1 FRCA)
  - Operates the E-Governance CAs
- Major functions
  - Platform, Security, Relationship, Community, and Program Management

Common Policy Root

- Common Policy establishes rules for PIV Issuers
  - Identity Proofing, Key Sizes/Types, Algorithms, FIPS Validation, etc
- Common Policy CA certifies CAs that meet the requirements of the Common Policy
- In order to trust Bob's PIV Card…
  - Check Bob's certificate
  - See if Bob's CA has a certificate from the Common Policy Root

Common Policy Root

- FIPS 201-1:
  - **Section 4.2.2, *Asymmetric Signature Field in CHUID*:** "The public key required to verify the digital signature shall be provided in the certificates field in an X.509 digital signature certificate issued under [COMMON]…"
  - **Section 4.4.2, *Biometric Data Representation and Protection*:** "The X.509 certificate containing the public key required to verify the digital signature shall be issued under [COMMON]…"
  - **Section 5.4.2, *PKI Certificate*:** "All certificates issued to support PIV Card authentication shall be issued under the id-CommonHW policy and the id-CommonAuth policy[5] as defined in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON].*"

Common Policy Root

- Verifying that a card is a real PIV Card requires validating certificates from the Common Policy Root
- Validating certificates from Common requires:
  - Getting Common's certificates from the Repository
  - Getting Common's CRLs from the Repository
    - Updated every 12-18 hours
  - Having the Common Policy Trust Anchor installed

Common Policy Root: Trust Store Status

Vendor	Application Submitted	Application Accepted as complete by Vendor	Vendor Processing of Application	Vendor Approved Certificate Inclusion	Distribution Date	Comments
Microsoft	✓	✓	✓	✓	22-Mar-11	
Adobe	✓	✓	✓	✓	15-Apr-11	
Mozilla	✓	✓				Ready for public discussion beginning 10-May-12
Apple	✓	✓	✓	✓	1-Feb-12	
Java	✓					All required documentation has been submitted. Awaiting a response from Java.
Opera	✓	✓				Opera has acknowledged receipt of the supplemental application package.
Chrome Browser	N/A	N/A	N/A	N/A	N/A	Chrome Browser uses the trust store of the OS rather than distributing its own.
Chrome OS	N/A	N/A	N/A	N/A	N/A	Chromium OS source code leverages Mozilla NSS Library; includes Mozilla Public Distribution of Root CA Certificates

Common Policy Root: Mobile Trust Store Status

Vendor	Application Submitted	Application Accepted as complete by Vendor	Vendor Processing of Application	Vendor Approved Certificate Inclusion	Distribution Date	Comments
Android						Researching
iPhone	✓	✓	✓	✓	1-Feb-12	
iPad	✓	✓	✓	✓	1-Feb-12	
Blackberry						Researching
Windows Phone 7						Microsoft is in the process of updating their application process for Mobile platform.
PKard	✓	✓	✓	✓	3-Mar-12	App to use smart card with iPhone

FPKIMA Certification Authorities (CAs)

- Federal Bridge CA (FBCA)
  - FBCA was 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

FPKIMA Certification Authorities (CAs)

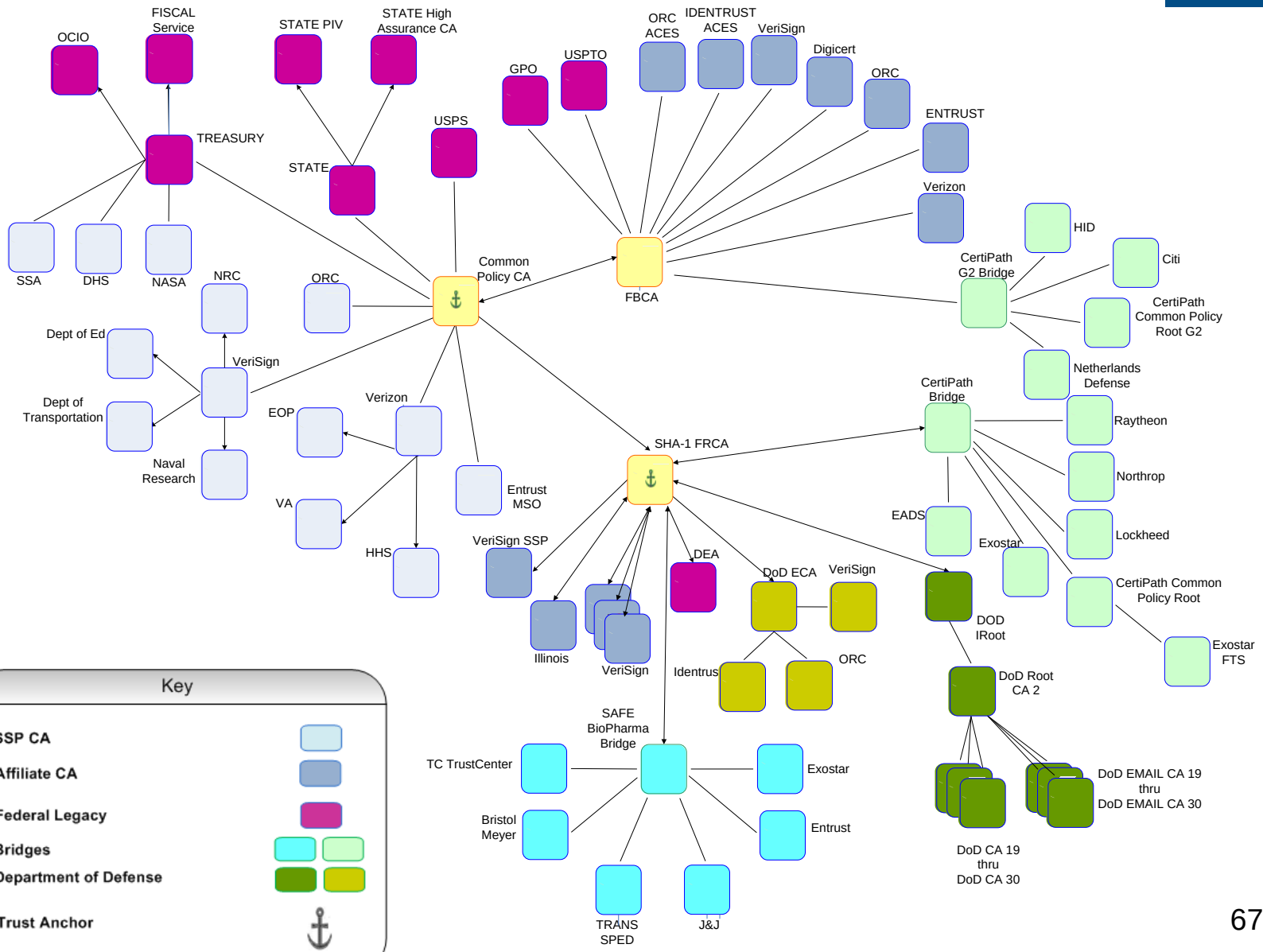
- SHA-1 Federal Root CA (SHA1 FRCA)
  - SHA1 FRCA has been established for organizations that are not yet capable of implementing the SHA-256 algorithm in their environment
  - Starting 1 Jan 2011, the Federal Public Key Infrastructure Policy Authority (FPKIPA) prohibits the use of the SHA-1 algorithm for CAs signing Personal Identity Verification (PIV) Cards, and strongly discourages its use for any digital signatures
  - FPKIMA implemented new Trust Infrastructure CAs, which use the SHA-256 signature hashing algorithm, for transitioning the FPKI community away from SHA-1
  - “PIV-like” credentials are issued and managed in the SHA1 FRCA environment, but are not true PIV
  - SHA1 FRCA will expire and be decommissioned by 31 Dec 2013

FPKIMA Certification Authorities (CAs)

- E-Governance CAs (EGCA)
  - EGCA issues PKI certificates to approved Credential Service Providers (CSPs), at assurance levels 1 or 2, and to Federal Relying Party (RP) applications to enable mutual trust through mutual authentication
  - Two separate CAs support each of the two certificate types: EGCA CSP2, and EGCA Apps
  - EGCA CSP2 and EGCA Apps have issued three current certificates each
  - A third EGCA was established in support of the newly developed E-Governance Trust Services (EGTS)
  - EGTS includes new certificate types for supporting Backend Attribute Exchange (BAE) and digitally-signed metadata

Federal PKI Management Authority
Enabling Trust

Trust Relationships



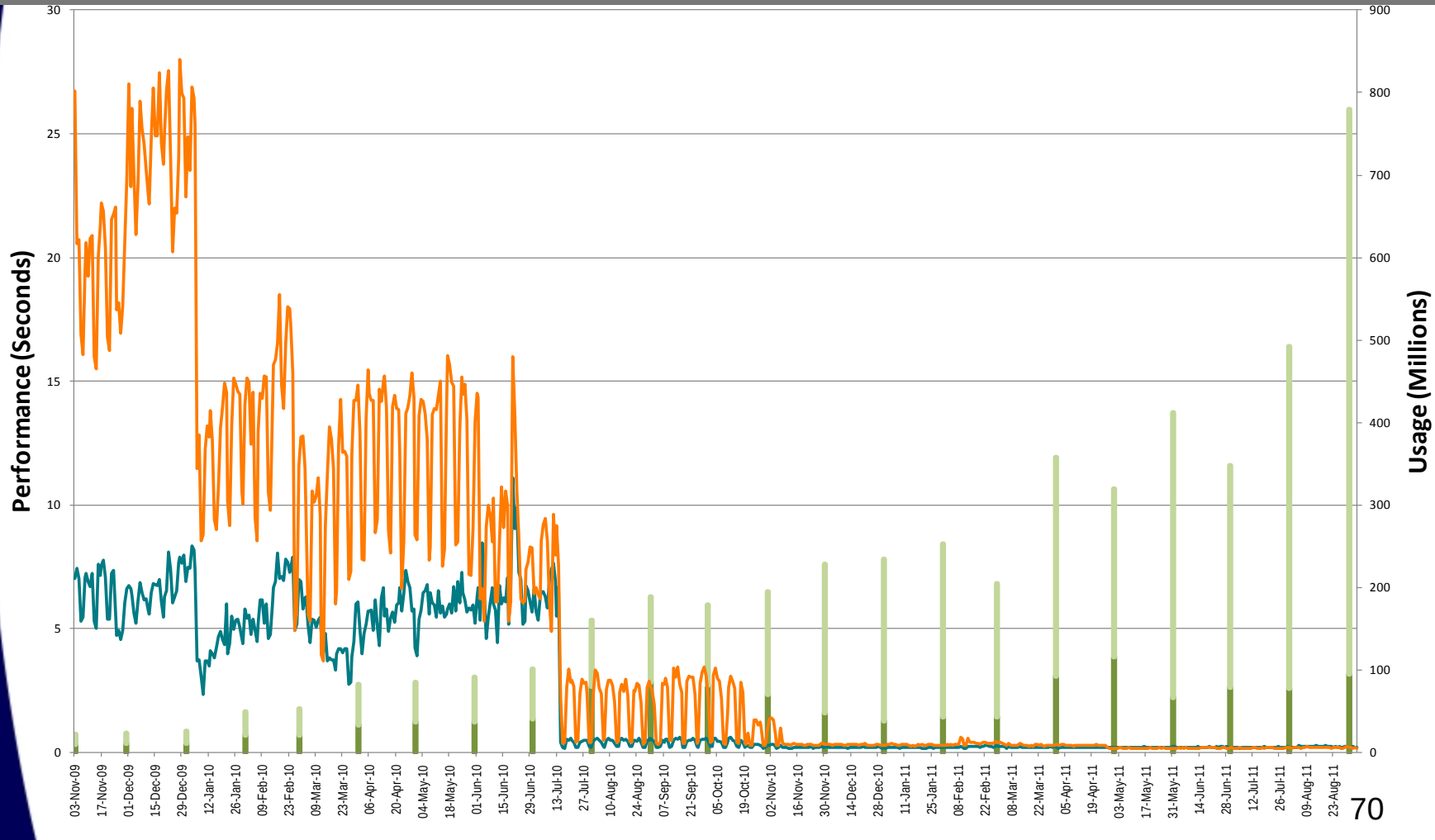
Repository Services

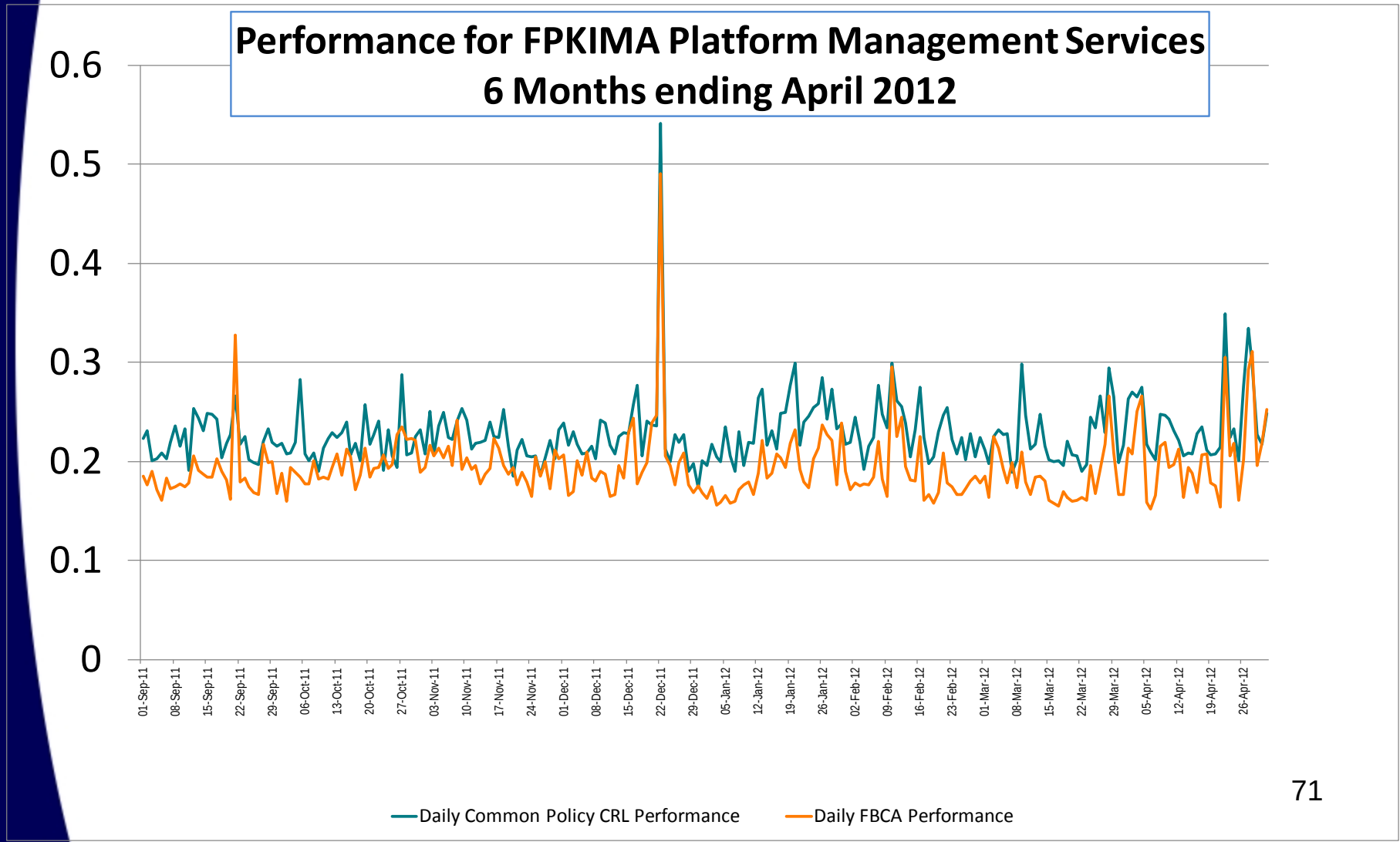
- High-availability repository services
  - 99.5% availability per the Federal PKI Policies
  - Fault-tolerant networking and content delivery
  - Load balancing and redundancy
  - Multi-protocol support for repository access (e.g., http, ldap, dsp)

Current State of The FPKIMA Program-Metrics

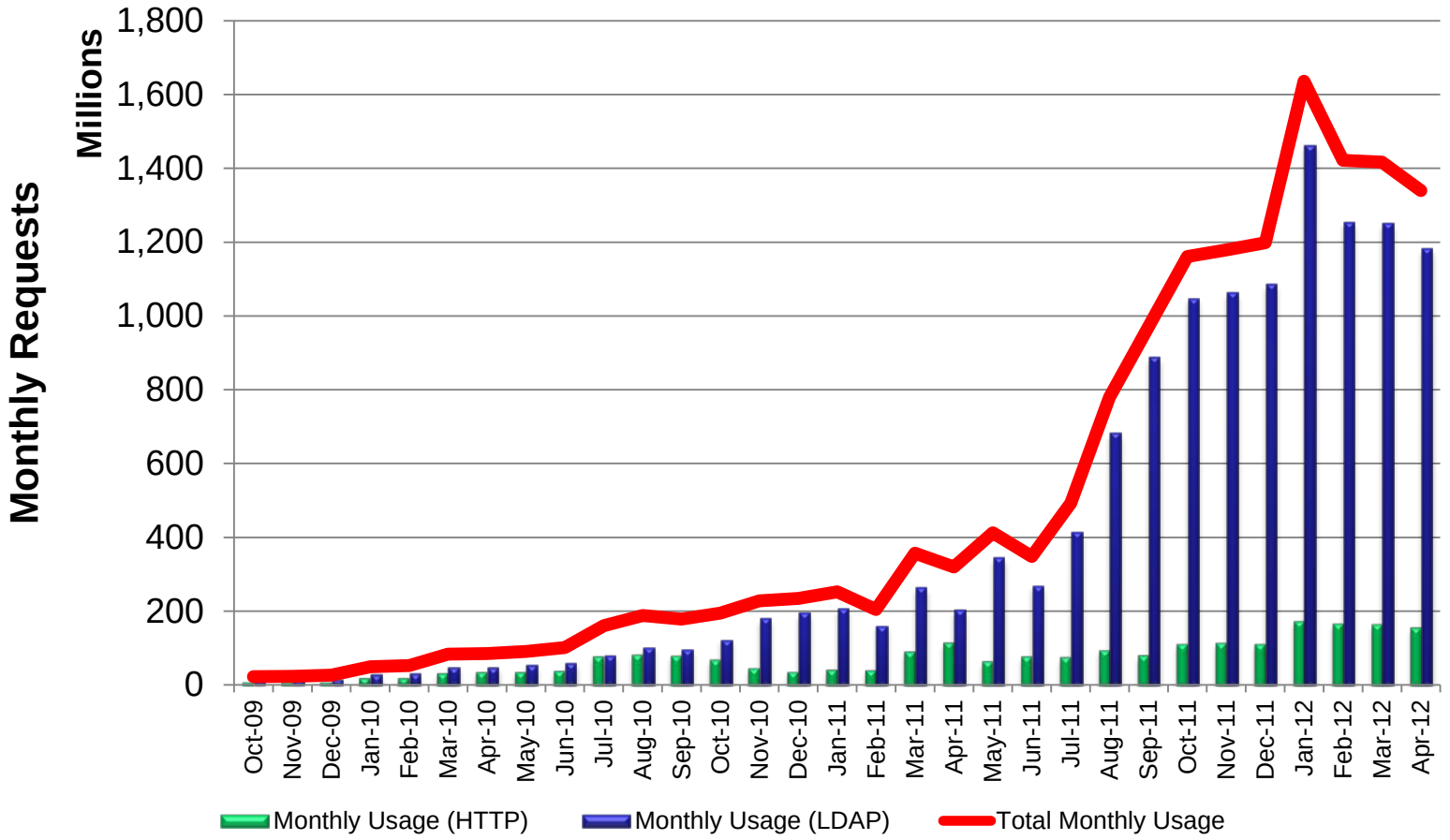
- Increased Usage
  - ✓ Before Re-design: less than **100 Million** monthly usage requests
  - ✓ FPKIMA Platform Management Services monthly usage has increased **1600%** over the last three years as PIV Usage increases
  - ✓ In Jan 2012, there were over **1.6 billion** requests
- Improved Performance
  - ✓ Before Re-design: response time was between **20** to **30** seconds
  - ✓ As usage continues to increase, Response Time for both the Common Policy and Federal Bridge since Aug 2011 is less than 1/3 of a second (Average government benchmarks performance 2.7 seconds)
- As usage continues to increase the FPKI Trust Infrastructure has sustained nearly 100% availability

Technology Refresh



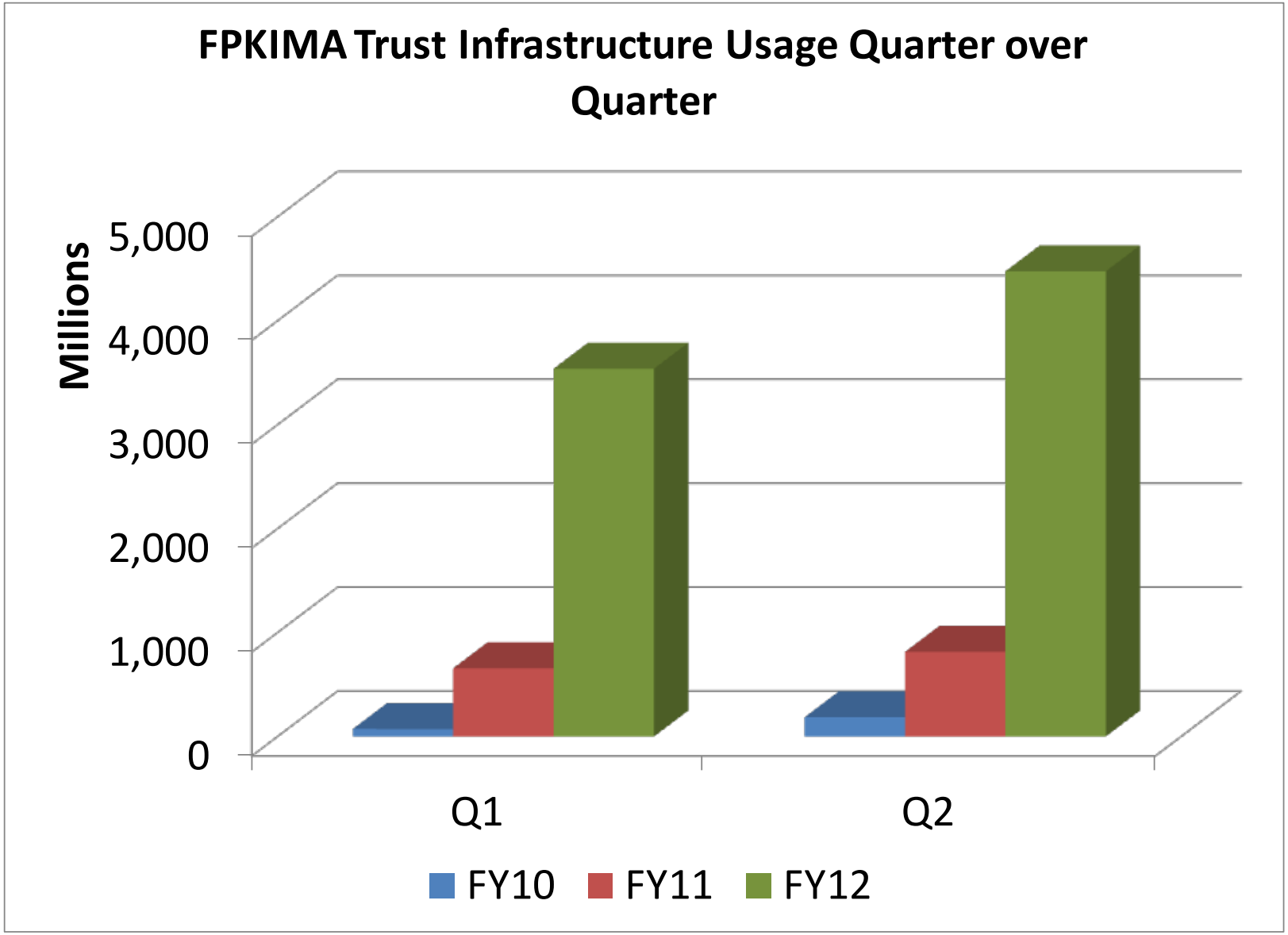

Performance for FPKIMA Platform Management Services
6 Months ending April 2012
0.6
0.5
0.4
0.3
0.2
0.1
0
01-Sep-11
08-Sep-11
15-Sep-11
22-Sep-11
29-Sep-11
06-Oct-11
13-Oct-11
20-Oct-11
27-Oct-11
03-Nov-11
10-Nov-11
17-Nov-11
24-Nov-11
01-Dec-11
08-Dec-11
15-Dec-11
22-Dec-11
29-Dec-11
05-Jan-12
12-Jan-12
19-Jan-12
26-Jan-12
02-Feb-12
09-Feb-12
16-Feb-12
23-Feb-12
01-Mar-12
08-Mar-12
15-Mar-12
22-Mar-12
29-Mar-12
05-Apr-12
12-Apr-12
19-Apr-12
26-Apr-12
Daily Common Policy CRL Performance
Daily FBCA Performance

FPKIMA - Repository Usage



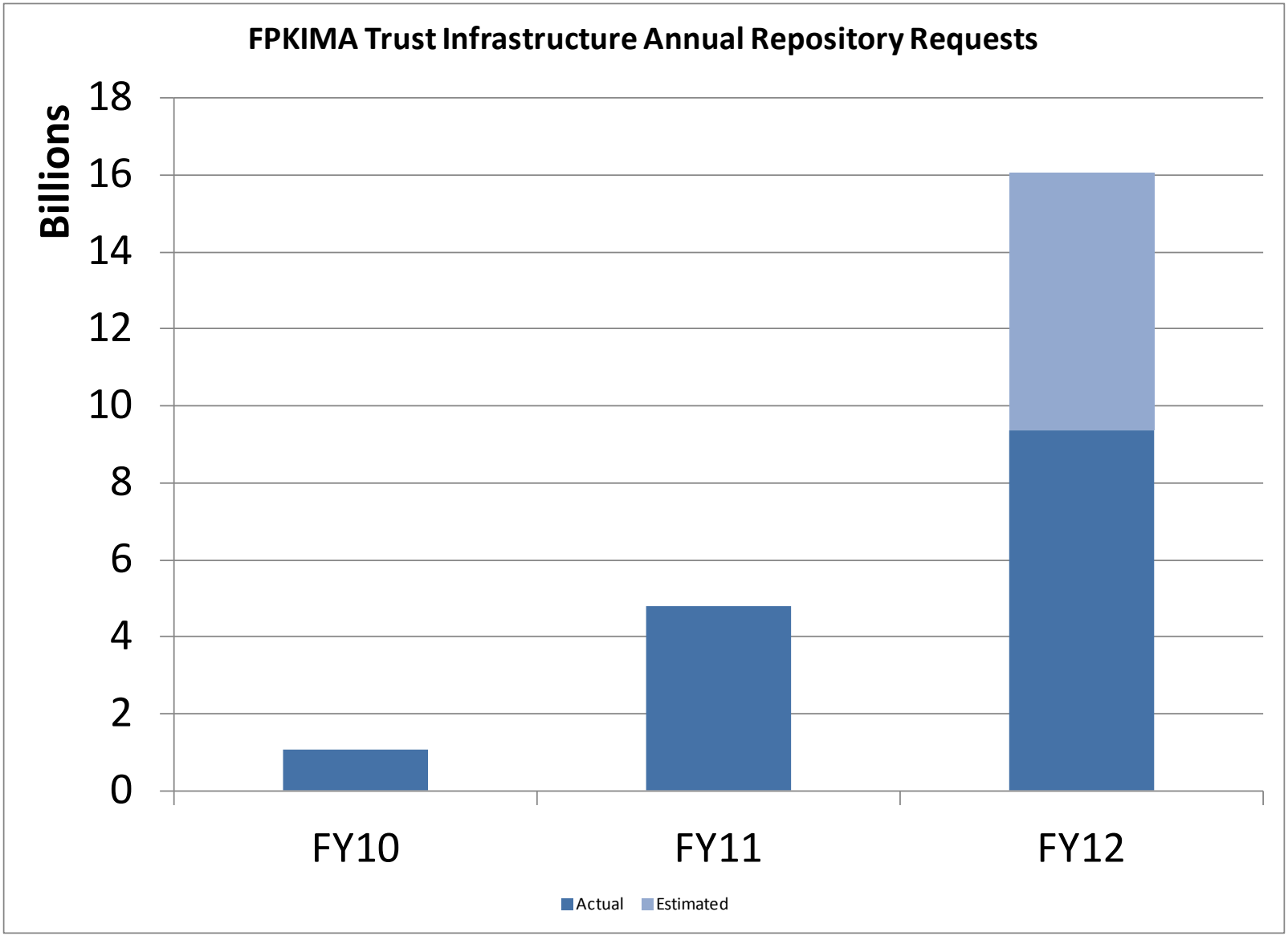
Federal PKI
Management Authority
Enabling Trust

GSA



Federal PKI
Management Authority
Enabling Trust

GSA



Questions?

FPKIPA-MA@listserv.gsa.gov