

Interagency Advisory Board

Meeting Agenda, March 23, 2011

1. **Open Remarks** (*Mr. Tim Baldrige, IAB Chair*)
2. **Impact of M-11-11 on PACS** (*Ron Martin, HHS*)
3. **FIPS 201-2 Update** (*Bill MacGregor, NIST*)
4. **Status Brief on ICAM Roadmap** (*Shelly Hartsook, Deloitte*)
5. **Status of FPKI Management Authority** (*MA Team, GSA*)
6. **Closing Remarks** (*Mr. Tony Cieri*)



Federal PKI
Management Authority
Enabling Trust

GSA

Interagency Advisory Board
March 23, 2011

FPKI Management Authority Report



Federal PKI Management Authority

- **Who Is The Management Authority?**
 - Organizationally, the FPKIMA is a program that operates under GSA's OGP, but follows policy and guidance from a variety of organizations and entities, with the primary two being the ICAM and FPKIPA.
 - Operationally, the FPKIMA is responsible for managing the Common Policy root that is relied on for PIV card use; the FBCA that interface federal government with industry making possible secure on-line business, and other certification authorities and services that support IDM solutions.



Federal PKI Management Authority

Enabling Trust



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

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

FPKI PA
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

FPKI MA 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.

FPKI MA Primary Functions:
Fundamental building blocks of the program

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

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



Agenda

- Performance and Capacity Planning
- SHA-2 Transition Report
- FPKI Technical Working Group Report

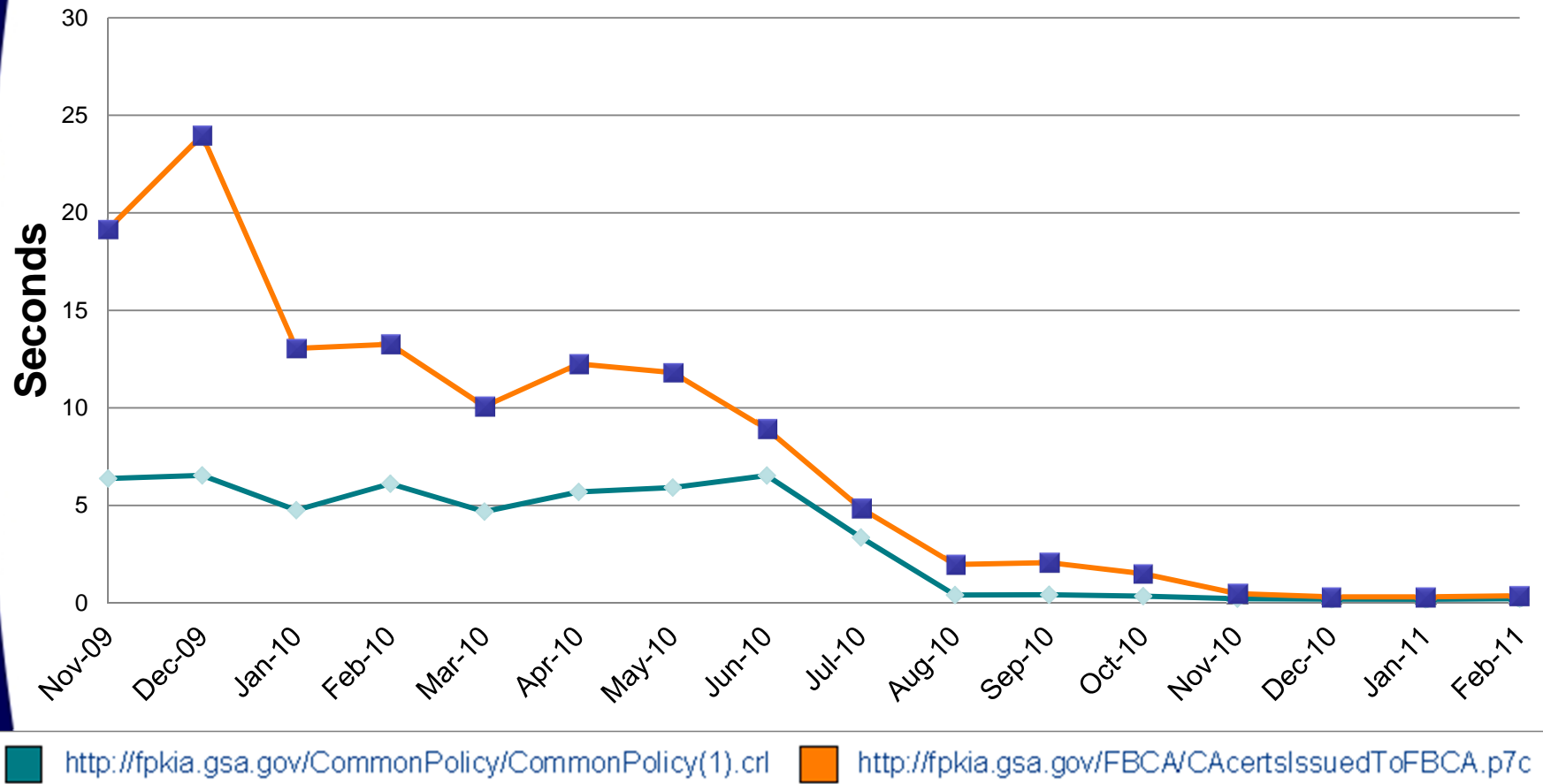


Performance & Capacity: Background

- **Performed a Holistic Redesign**
 - Complete infrastructure and technology refresh
 - Upgrade of data centers, servers, software, networking, etc
 - Some legacy elements co-exist with target in an integrated design
 - Incremental deployment concurrent with development
- **Increased Network Capacity with Demand**
 - Started 2010 with 1.5Mbps
 - Ended 2010 with 110Mbps effective:
 - Site 1: 90 Mbps (100Mbps with 10Mbps reserved for VPN)
 - Site 2: 20 Mbps (30Mbps with 10Mbps reserved for VPN)
 - Site 2 upgrade to 100Mbps in process

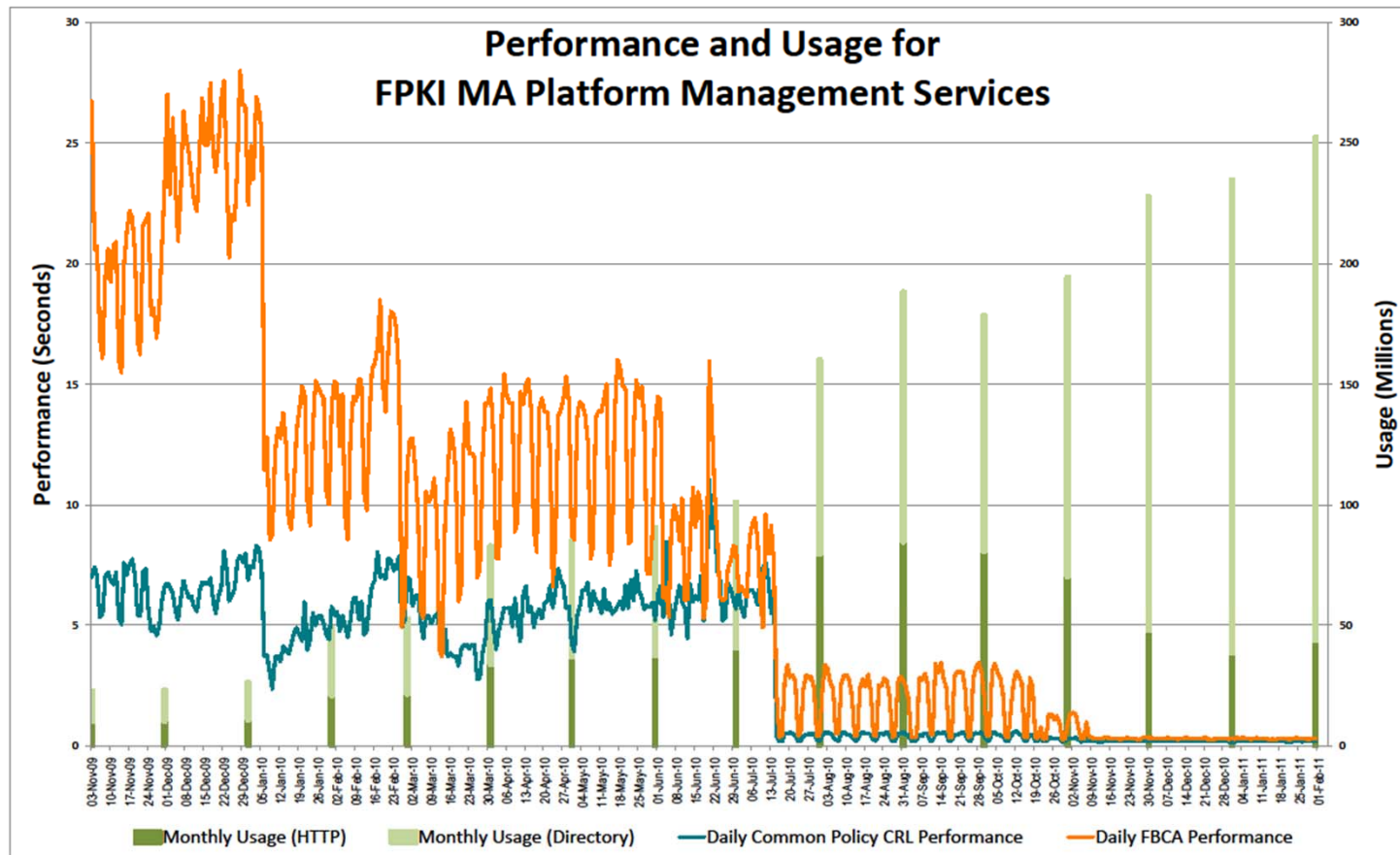


Performance: Average Response Time





Performance: Detailed Performance and Usage





Performance: Summary

- ~3,190% increase in speed for CPCA crl (31.9x)
 - 6.38s (Oct 2009) to 0.20s (Dec 2010)
- ~6,180% increase in speed for FBCA p7c (61.8x)
 - 19.17s (Oct 2009) to 0.31s (Dec 2010)
- ~1,040% increase in traffic served (10.4x)
 - 22.5M (Oct 2009) to 234.4M (Dec 2010)
- December 2010 availability > 99.9%
 - CPS requires 99% and less than 0.5% scheduled downtime



Capacity Planning

- **Operational Management**
 - Capture and Analyze Metrics
 - Performance and usage measurements
 - Usage analytics, e.g. requestor, client type, geo-location
 - Grow Capacity
 - Maintain reserve capacity to cover growth
 - Maintain reserve capacity to cover site outages



Capacity Planning (cont.)

- **Research**
 - Load testing of repository components
 - Establish acceptable loads on components
 - Determine need for component upgrades to support loads
 - Load Management Technologies
 - Public Content Delivery Networks (CDNs), e.g. Akamai
 - Alternative client behaviors, e.g. caching



Federal PKI
Management Authority
Enabling Trust

GSA

Questions?

Giuseppe Cimmino
giuseppe.cimmino@pgs.protiviti.com
703-299-4722

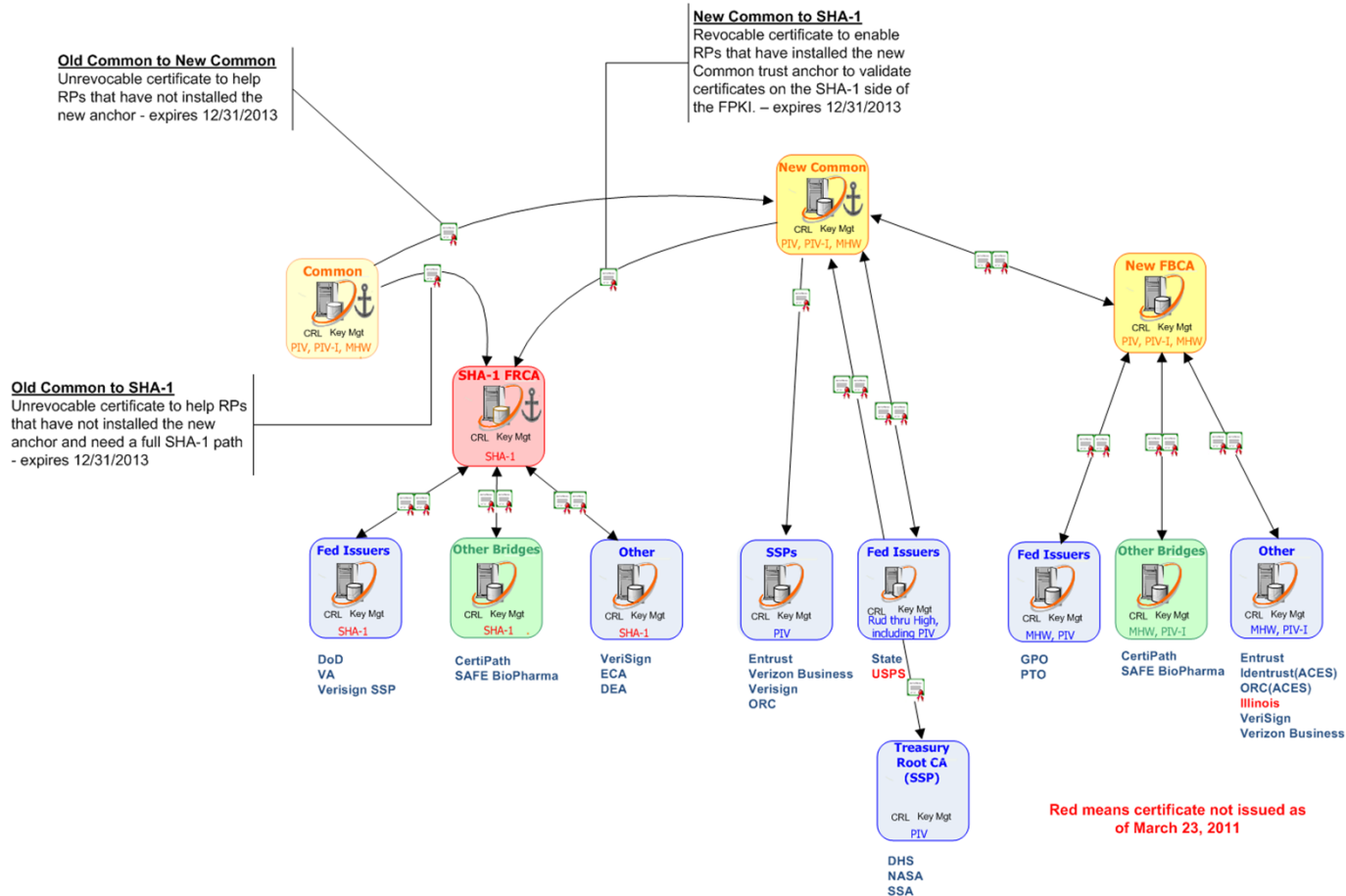


SHA-2 Transition Report

- ✓ Performance and Capacity Planning
- SHA-2 Transition Report
- FPKI Technical Working Group Report

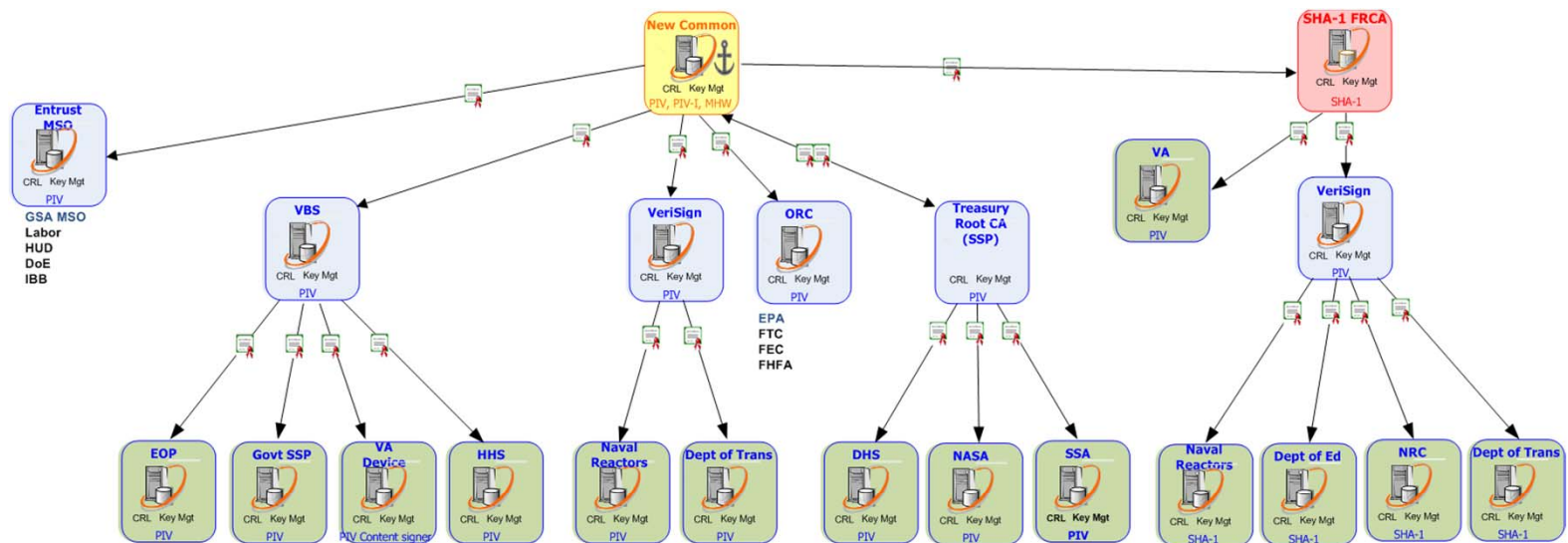


SHA-2 Transition Report: Current Trust Infrastructure





SHA-2 Transition Report: Current SSP Support



Key	
FPKI SHA-256 Infrastructure CA	Yellow
FPKI SHA-1 Infrastructure CA	Red
SSP CA or SSP Intermediate CA	Blue
Agency specific Subordinate CA	Green



SHA-2 Transition Report: Common CA Distribution

Vendor	Status	Status Date	Distribution Date
Microsoft	Completed	N/A	03/2011
Adobe	Completed	N/A	04/2011
Mozilla	In Queue for Public Discussion	02/2011	
Apple	Application Submitted	01/2011	
Java	Application Submitted	03/2011	
Opera	Planned		



SHA-2 Transition Report: AIA Crawler Introduction

- **Purpose:**
 - Discover and Path-Validate all CA Certificates Cross Certified with the Federal Common Policy (SHA-256) CA
 - Authority Information Access (AIA)
 - Subject Information Access (SIA)
- **Results available at:**
 - <http://http.icam.pgs-lab.com/AIACrawler/>



SHA-2 Transition Report: AIA Crawler Processing

- Retrieve all CA Certificates Found via AIA, SIA
- Perform Path Validation for each CA Certificate
 - Attempt to Discover Paths Using AIA or General Search
- Perform FBCA Policy Validation
 - PKIX Validation of each FBCA Certificate Policy
 - 2.16.840.1.101.3.2.1.3.1 - .8, .12 - .27
 - Assurance (Test, Basic to High), Common Policy, PIV-I, SHA-1
- CA Certificate Grouping
 - Use Certificate DN to Categorize by US Government Agency, State, or Commercial Company



SHA-2 Transition Report: AIA Crawler Result Formats

- **Federal Common Policy Tree**
 - Creates Tree, From Federal Common Policy
 - Lists all CA certificates discovered which path-validating via AIA directly to Federal Common Policy
 - List each of their Subordinate CAs
 - Output currently as CSV Spreadsheet
 - Output will be visual display
- **Crawler Output (HTML)**
 - For Each CA Certificate
 - PKIX Path Validation Result to Federal Common Policy: via AIA, General Search, or no valid path found
 - Lists only Shortest paths to Federal Common Policy
 - Lists Validating policies and certificate details



SHA-2 Transition Report: AIA Crawler Result Formats

- **Certificate Lists (P7B)**
 - All CA Certificates for loading into Certificate Store or View
 - CA Certificate Groups
 - Subordinates Only
 - Full Path to Federal Common Policy
- **CA Certificates Found at URL (CSV, XML)**
 - For Each AIA and SIA URL
 - CA Certificates Retrieved
 - XML contains PEM-encoded certificate
 - CA certificates may appear in multiple locations
 - Lists Retrieval error, if any
- **All CA Certificates (CSV)**
 - For Each CA Certificate:
 - Name/CN, Issuer CN, Serial, Not After, DN, Issuer DN
 - Signature Algorithm: SHA-1 or SHA-256
 - Specifies AIA or General Path Length
 - Lists OCSP, CRLDP, AIA, SIA URLs and Errors



Federal PKI
Management Authority
Enabling Trust

GSA

Questions?

Wendy Brown
wendy.brown@pgs.protiviti.com
703-299-4705

Sandy Metzger
sandy.metzger@pgs.protiviti.com
703-299-4719



FPKI TWG Report

- ✓ Performance and Capacity Planning
- ✓ SHA-2 Transition Report
- FPKI Technical Working Group Report



FPKI TWG Report: Informational

- FPKI TWG reconvened March 17, 2011
- Purpose - Advancing PKI technology through community collaboration and technical analysis of proposed modifications to the Trust Infrastructure
 - Technical participants from the FPKI community
- FPKI TWG Current Topics:
 - FPKI Test Environment
 - High-level strategies for future PKI transitions
 - Time stamping
- TWG meetings will be held quarterly
- Minutes will be posted at:
http://www.idmanagement.gov/fpkima/drilldown.cfm?action=fbca_twg



Federal PKI
Management Authority
Enabling Trust

GSA

Questions?

Wendy Brown

wendy.brown@pgs.protiviti.com

703-299-4705