

# FPKIMA Newsletter

Winter 2015  
Volume 2 Issue 1



**Federal PKI  
Management Authority**  
Enabling Trust

## INSIDE THIS ISSUE

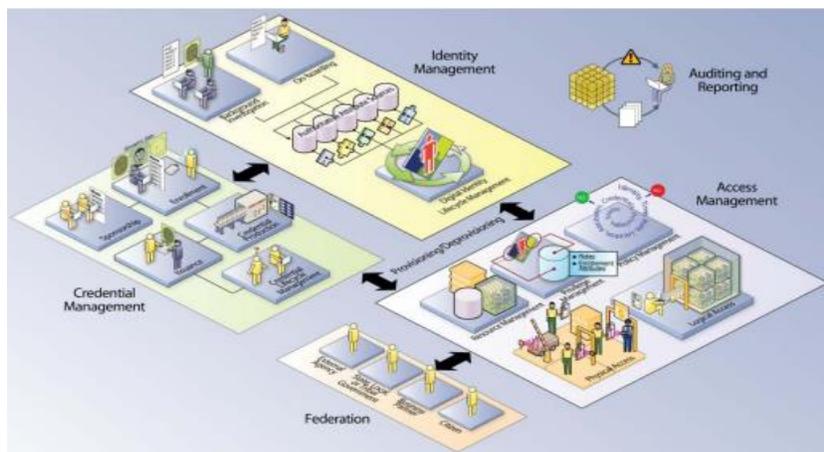
Federal Public Key Infrastructure Interoperability .....	1
Repository Response Improvements .....	2
News from the FPKI.....	3
FPKI Technical Working Group .....	4
Ask the FPKIMA .....	4

*The National Institute of Standards and Technology (NIST) released a draft of its Guide to Cyber Threat Information Sharing for public comment. "The goal of the publication is to provide guidance that improves the efficiency and effectiveness of defensive cyber operations and incident response activities, by introducing safe and effective information sharing practices." Cyber threat information sharing is a mature capability of the NIST Cybersecurity Framework and this draft publication will help both Federal and commercial partners successfully implement for effective practices.*

## Federal Public Key Infrastructure Interoperability

One key to a successful federated trust mechanism is its ability to grow and mature. The Federal Public Key Infrastructure (FPKI) has shown this ability as it has expanded from one certificate policy (CP) and Certification Authority (CA) to over four CAs. Previous articles in this series explained the mission and purpose of the Federal CAs, but not how they interoperate. This article focuses on and explains how FPKI interoperability has led to Federal success.

Organizations use unique internal policies and procedures to manage the identities of their employees and collaborating groups. These policies and procedures do not easily or efficiently align with policies and procedures used by other organizations. Federated PKI trust mechanisms, such as the Federal Bridge and other bridges it partners with, allow trusted interoperability between disparate systems, greatly facilitating a digital government. Inter-organizational trust is readily extended to all individual credentials within a federated organization, whether they are used to enable secure e-mail exchange, provide digital signatures, or access control activities.



*FPKI is required for multiple service areas of the FICAM Roadmap*

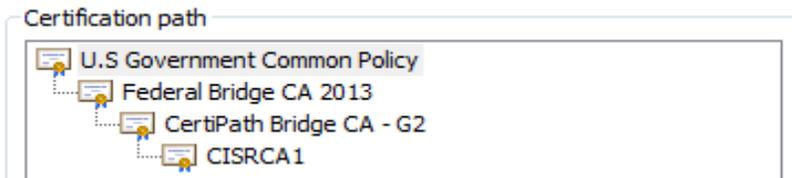
For the Federal community, the move to the Federal Common Policy CA (FCPCA) as the trust anchor for PIV cards has simplified the cross-organizational trust model, since all trust has been placed in the single policy and its root CA. The FCPCA trust anchor has been added to commercial product Root Stores further facilitating federated trust, both within the Federal community and between the Federal community and its external partners.

The FPKI has much to celebrate as a technology that is gaining importance and criticality to new digital government initiatives. The FPKI is intrinsically tied to the modern fabric of Federal IT and is the foundation of Federal identity management. As more agencies and industry use the FPKI through the use of PIV, PIV-I, and CAC, the realized value of the FPKI increases greatly.

## Repository Response Improvements

### Improve Slow Performance by Removing Expired Certificates

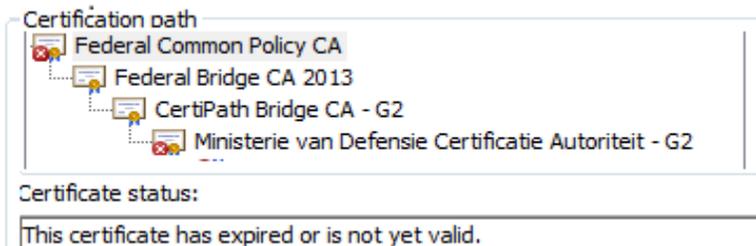
In order for a PKI certificate to provide essential security services, such as authentication, confidentiality, and integrity, the Relying Party (RP) application must be able to verify the certificate is current and issued from a trusted source. The trust source not only includes the issuing CA, but also the trusted path from the end-entity certificate. If the RP doesn't already hold an assured copy of the issuing CAs public key, then it may need to build a certificate path to a CA it is configured to trust.



Example of Path Validation using Microsoft CAPI

If the RP application is not configured with all the CA certificates it will trust, it builds the certificate path by dynamically discovering certificates in the path based on information in the Authority Information Access (AIA) extension in each certificate in the path starting with the end-entity certificate. The AIA contains the location of where to find certificates issued to the issuing CA until it reaches the final CA that is configured as a trust anchor. In the case of the FPKI, the FCPCA is configured as the trust anchor.

***“The fewer expired and revoked certificates encountered during the path discovery process, the more efficient the process becomes.”***



Example of Path Validation with Expired Certificates in the Path

At a minimum, certificate path validation requires that the RP application verify each certificate in the path contains a validity period that includes the current time (is neither expired or has a validity period starting in the future), and is not currently revoked. Additional checks include:

- 1) Verifying the signature on the certificate is valid
- 2) Verifying each certificate is issued by the CA whose name is the subject of the certificate until a self-signed trust anchor is reached
- 3) Validating Policy and Name Constraints are not violated
- 4) Verifying acceptable Certificate Policies are asserted

By removing expired certificates from your repository, it increases the speed of the path validation process for RP applications in verifying end entity certificates.

*Looking for Cybersecurity information for your small business and agency partners?*

*NIST recently issued a new guide that tailors basic information on cybersecurity to the specific needs of small business and agencies to help them in planning for and managing secure information systems. NIST Interagency Report (NISTIR) 7621 presents major area mitigation that small organizations should address to provide security for their information, systems, and networks.*

*More information is available at <http://www.itl.nist.gov/lab/bulletns/b-11-09.pdf>*

## News from the FPKI

### FPKI Monthly Statistical Report Enhancements

The FPKIMA has initiated an enhancement project to make the Monthly Statistical Report more relevant for troubleshooting availability and interoperability issues of the FPKI environment. Starting with the November 2014 report, the FPKIMA began monitoring all locations listed in a Certificate Distribution Point (CDP) extension to include both LDAP and HTTP Certificate Relocation List (CRL) locations. Very few Affiliates still support directory chaining and future statistical reports will reflect this transition. Since the new monitoring has been implemented, two HTTP CRL issues have already been identified and resolved.

Approximate CRL Availability:

FPKI Entity	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	Average
CertiPath Bridge CA	100.0	100.0	-	-	-	-	100.00
CertiPath Bridge CA - G2	100.0	100.0	-	-	-	-	100.00
DigiCert Federated ID CA-1	100.0	100.0	-	-	-	-	100.00
DoD Interoperability Root 1	99.9	100.0	-	-	-	-	99.97
DoD Interoperability Root 2	99.9	100.0	-	-	-	-	99.95
Department of State AD Root CA	100.0	100.0	-	-	-	-	100.00
Entrust Managed Services Root CA	100.0	100.0	-	-	-	-	100.00
Entrust Managed Services NFI Root CA	100.0	100.0	-	-	-	-	100.00
Exostar Federated Identity Service Root CA	100.0	100.0	-	-	-	-	100.00
FPKI EGovApp	100.0	100.0	-	-	-	-	100.00
FPKI EGovCSP2	100.0	100.0	-	-	-	-	100.00
FPKI EGTSCA	100.0	100.0	-	-	-	-	100.00
FPKI FBCA	100.0	100.0	-	-	-	-	100.00
FPKI FBCA2013	100.0	100.0	-	-	-	-	100.00
FPKI FCPCA	100.0	100.0	-	-	-	-	100.00
FPKI SHAIFRCA	100.0	100.0	-	-	-	-	100.00
GPO PCA	92.9	99.6	-	-	-	-	96.26
IdenTrust ACES	100.0	100.0	-	-	-	-	100.00
IdenTrust Global Common Root CA	100.0	100.0	-	-	-	-	100.00
ORC NFI CA	100.0	100.0	-	-	-	-	100.00
SAFE Bridge CA	99.9	100.0	-	-	-	-	99.96
Symantec Class 1 SSP CA	100.0	100.0	-	-	-	-	100.00
Symantec Class 2 SSP CA	100.0	100.0	-	-	-	-	100.00
Treasury Root CA	100.0	100.0	-	-	-	-	100.00
USPTO	100.0	100.0	-	-	-	-	100.00
Verisign Class 3 SSP Intermediate CA	100.0	100.0	-	-	-	-	100.00
Verisign SSP Intermediate CA - G3	100.0	100.0	-	-	-	-	100.00
Verizon CT-CSSP-CA	100.0	100.0	-	-	-	-	100.00
Verizon Betrusted Production SSP CA	100.0	99.7	-	-	-	-	99.83

HTTP CRL Repository Sample from the December 2014 Statistical Report

### FPKI Industry Day

The FPKIMA is planning to hold an Industry Day to increase awareness about the services, capabilities, and business value provided by the FPKI across the Federal Government and to individual federal agencies, state government agencies, and industry.

In addition to vendor displays, it will also provide information about the roadmap of future services and capabilities the FPKI can offer to meet emerging needs in key areas such as Cybersecurity, Identity Management, Mobility, Device Authentication and Management, and Mobile Workforce. Send an email to [help@fpki.gov](mailto:help@fpki.gov) for more information.

Looking for a tool to help navigate the FPKI?

Check out the FPKI AIA Web Crawler, a graphical tool with publicly available reports on all certified and cross-certified Affiliates of the FPKI.

<http://fpki-graph.fпки-lab.gov>

Looking for security training to complement your cybersecurity skills? Check out the National Initiative for Cybersecurity Careers and Studies (<http://niccs.us-cert.gov/>) for new ideas. It is a one stop shop for cybersecurity related resources.

## FPKI Technical Working Group

The FPKI Technical Working Group (TWG) held a December meeting to discuss an Extended Key Usage (EKU) certificate profile change request and weakness in random number generator anomalies.

- The EKU Change Request is a compromise from the earlier certificate profile discussion that would have mandated all end-entity certificates contain EKUs to limit their use to intended capabilities. This compromise allows issuing CAs to include the EKU without asserting anyEKU which allows end-entity certificates to be used for any purpose, intended or not. Discussion on EKU use is ongoing and an EKU Test Report is being drafted based on member requirements and testing.
- Department of the Treasury presented a presentation on random number generator (RNG) anomaly detection using greatest common divisor and collision detection methods. The conclusion, based on academic research, was RNG anomalies are a real threat and steps should be taken to detect if certificates are being issued with flawed RNGs.

For more information or to be added in the TWG listserv, send an email to [help@fpki.gov](mailto:help@fpki.gov).

## Ask the FPKIMA



### Who Manages and Operates the FPKI?

- The Federal PKI Management Authority (FPKIMA) is the operational authority of the FPKI. The FPKIMA manages the FPKI Trust Infrastructure, which includes the CAs and repositories that provide centralized trust services to the FPKI community, on a day-to-day basis in accordance with the FPKI CPs and CPS' approved by the FPKIPA. The FPKIMA is a GSA office that operates under the direction of the FPKIPA and is responsible for the operations, communications, testing, helpdesk, and incident response management of the FPKI.
- The Federal PKI Policy Authority (FPKIPA) is the governing authority of the FPKI. The FPKIPA is an interagency working group that develops digital certificate standards for trusted identity authentication across federal agencies and between federal agencies and external organizations. The FPKIPA governs the FPKI by setting FPKI operational policy (CP/CPS), approving cross-certification, monitoring compliance, and directing the FPKIMA. Its voting members are limited to federal agencies operating a PKI or using a Shared Service Provider (SSP), but other agencies and industry can participate as observers.

### Where Can I Find More Information on the FPKI and FPKIMA?

- Information on the FPKI and FPKIMA can be found on the [idmanagement.gov](http://idmanagement.gov) websites below:

FPKI - <http://idmanagement.gov/federal-public-key-infrastructure>

FPKIMA - <http://idmanagement.gov/federal-public-key-infrastructure-management-authority>



**Federal PKI  
Management Authority**  
Enabling Trust

### Need Help?

Contact the FPKI Help  
Desk

[help@fpki.gov](mailto:help@fpki.gov)

### Did you know...?

*It is helpful to quantify PKI Return on Investment (ROI) in terms of increased protection for government assets; greater efficiencies in doing business; and reduced costs. It can be demonstrated that improving trust in the exchange of sensitive information results in lower cost, more streamlined communications, and accelerated process improvements, in part because digital transactions vastly reduce paper use. Use of the FPKI can increase an Agency's overall IT ROI.*