

FPKIMA Newsletter

Summer 2014
Volume 1 Issue 1



**Federal PKI
Management Authority**
Enabling Trust

INSIDE THIS ISSUE

Federal Public Key Infrastructure - Federal Bridge Certification Authority	1
Choose a Signing Certificate	2
FPKI Web Crawler	3
FPKI Technical Working Group	4
Ask the FPKIMA	4

Did you know....

GSA/FAS plays a security role with your PIV card? The FPKIMA, operated by the GSA FAS, enables federated certificate-based security services (logical and physical) across federal agencies and external organizations.

Need help?

*Have Questions?
help@fpki.gov*

Federal Public Key Infrastructure – Federal Bridge Certification Authority

The Federal Public Key Infrastructure (FPKI) was created in 2000 to facilitate electronic services that need to be both secure and trusted. Some of these electronic services include: physical and logical access, information sharing, electronic document signing, and many others. The FPKI facilitates these services between Federal agencies, universities, state and local governments, commercial entities, international partners, and other communities of interest. The FPKI Management Authority (FPKIMA) operates the four Certification Authorities (CA) of the FPKI Trust Infrastructure which consists of the Federal Bridge (FBCA), Federal Common Policy (FCPCA), E-Governance (EGCA), and the SHA-1 Federal Root (SHA1 FRCA). This first in a series of four articles will focus on each CA and give a brief description and history of its operation. The first CA established by the FPKI was the FBCA.

The FBCA acts as an identity trust hub or “bridge” (a non-hierarchical model) between disparate PKI environments enabling secure peer-to-peer transactions between federal and non-federal organizations. For an affiliate to become cross-certified with the Federal Bridge it must first demonstrate compliance with the FBCA Criteria and Methodology document (Crits and Methods).

To provide trust services, the FPKI uses a set of policies and procedures based on Public Key Cryptography to authenticate users and data, protect the integrity of transmitted data, and ensure technical non-repudiation and confidentiality. These policies and procedures are documented in a Certification Policy (CP), Certification Practice Statement (CPS), and a Crits and Methods document. The CP defines the policies in use by the CA; the CPS documents the internal practices and procedures for certificate lifecycle services; and the Crits and Methods identifies the criteria for suitability and the methodology for implementing and maintaining cross-certification.

A participating Affiliate CA exchanges a cross-certificate pair with the FBCA, thus making it technically interoperable with the FBCA and all other cross-certified Affiliates. This interoperability allows cross-certified Affiliates with no direct relationship to trust digital certificates issued by any Affiliate of the FBCA.

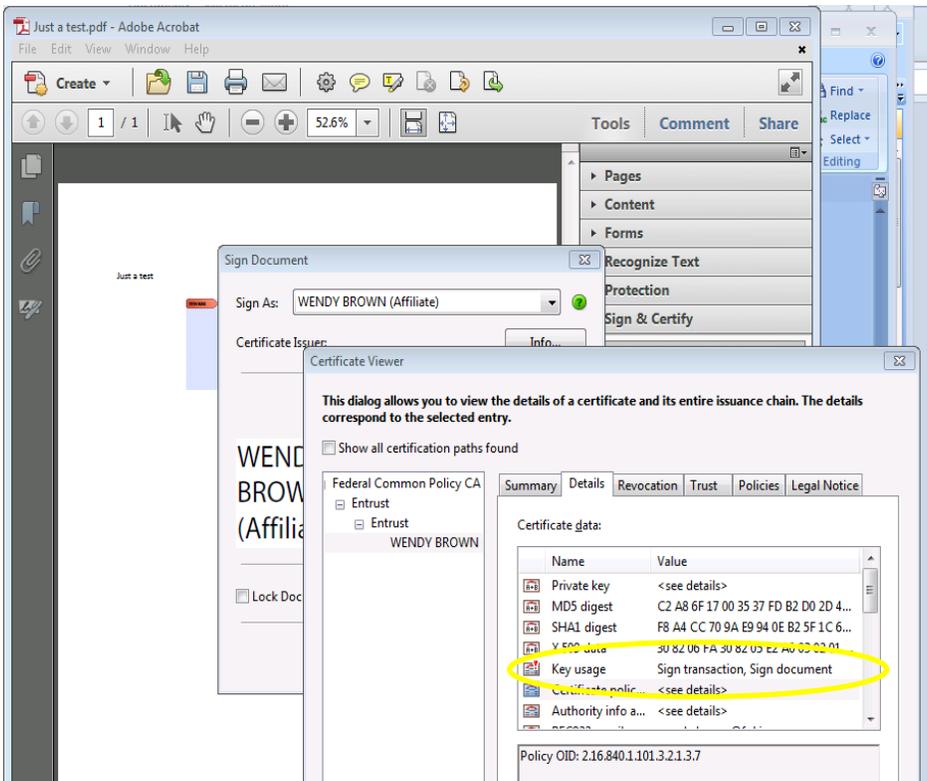
As the need for interoperability and trusted electronic services has grown, the FBCA has extended the use of secure credentials and reach of the FPKI well beyond the boundaries of the federal government. Communities of interest, such as the pharmaceutical, healthcare, and defense and aerospace industries, can now securely access, sign and share government information increasing the efficiency and security in using digital transactions.

The next article in this series will focus on the FCPCA otherwise known as the Federal Trust Anchor.

Choose the Correct Signing Certificate

One of the benefits of the PIV card is its use in electronically signing documents to ensure technical non-repudiation. A PIV card contains several different digital certificates, each with a specific purpose. The “Signature Certificate” is used to sign documents, but it is often confused with the “Authentication Certificate”. To choose the “Signature Certificate”, follow these steps:

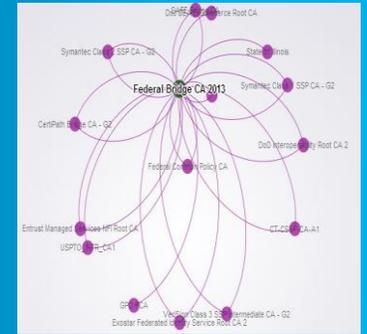
1. In Adobe Acrobat on the signature field, Click on “more info” on dialog box for “Sign As”
2. Click the “Details” tab and check the “Key Usage” field
3. Select the certificate with “Sign Transaction, Sign Document”



The FPKI Web Crawler

The FPKI Authority Information Access (AIA) Crawler application is an interactive tool used to navigate the FPKI infrastructure. It is designed to find all CA certificates cross-certified with the FBCA or certified by the FCPA and validate each certificate’s trust path to the FCPA. The tool uses the AIA and SIA extensions in the public certificates, starting at the FCPA, to find all known subordinate or cross-certified CA certificates. It then follows the certificate’s AIA chain to the trust anchor or root. The crawler operates by processing certificates in two steps.

Please see *FPKI Web Crawler* on page 3



A graphic representation of FBCA cross-certified Affiliates from the FPKI AIA Web Crawler. Dual lines indicate a two-way cross-certificate.

Federal Bridge CA 2013

Attributes
id : CN=Federal Bridge CA, 2013,OU=FPKI,O=U.S. Government,C=US

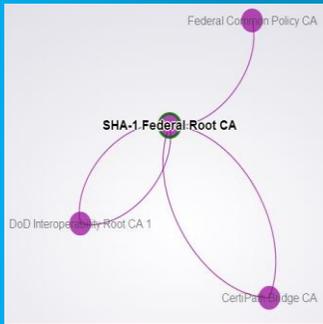
Inbound Links from :

- CertiPath Bridge CA - G2
- CT-CSSP-CA-A1
- DoD Interoperability Root CA 2
- Entrust Managed Services NFI Root CA
- Exostar Federated Identity Service Root CA 2
- Federal Bridge CA
- Federal Common Policy CA
- SAFE Bridge CA
- Symantec Class 1 SSP CA - G2
- Symantec Class 2 SSP CA - G2
- USPTO_INTR_CA1
- VeriSign Class 3 SSP Intermediate CA - G2

Outbound Links to :

- CertiPath Bridge CA - G2
- CT-CSSP-CA-A1
- DoD Interoperability Root CA 2
- DoJ DEA E-Commerce Root CA
- Entrust Managed Services NFI Root CA
- Exostar Federated Identity Service Root CA 2
- Federal Bridge CA
- Federal Common Policy CA
- GPO PCA
- SAFE Bridge CA
- State of Illinois
- Symantec Class 1 SSP CA - G2
- Symantec Class 2 SSP CA - G2
- USPTO_INTR_CA1
- VeriSign Class 3 SSP Intermediate CA - G2

FBCA cross-certified Affiliates. The FPKI Web Crawler also displays a list of Affiliates by inbound/outbound link in addition to the relationship graphic.



The Crawler can display graphic relationships of all entities certified, whether cross-certified or subordinate, with the FPKI.

Did you know....
HSPD-12 will turn 10 on August 27, 2014? The identity standard identified in HSPD-12 is the PIV card and can be used for physical and logical access. The anchor certificate on the PIV card is the FCPCA, which is managed by the FPKIMA.



The above screen shot is the opening page of the FPKI AIA Web Crawler. The center of the graph is the trust anchor of Federal Common Policy. Each dot on the graph represents a CA with a relationship to the FPKI. The FPKI has grown exponentially from its proof of concept with three Federal Agencies to a diverse and complex federated environment.

FPKI Crawler from page 2

The first process flow conducts a search for CA certificates. The search starts at the FCPCA and checks the AIA and SIA extension of each certificate and subordinate certificate until no new AIA / SIA Uniform Resource Locators (URL) are discovered. The AIA extension defines the URL of the CA's signing certificate while the SIA extension defines the URL of the subordinate public certificates.

The second process flow consists of path validation to the FCPCA. The path processing for any particular path will be ignored if the chain becomes too long, repeats itself, or ends at a root other than the FCPCA.

Multiple reports in multiple formats (html, csv and xml) are available on the Crawler website and are grouped into three categories of certificates found with: validated AIA chains, validated chains but not through AIA, and no validated AIA chains. All CA certificates are available as PKCS 7 binary files in either a single file or in multiple segment files. The crawler provides value in appreciating the complexity of the FPKI and aids those entities, relying parties, and users in understanding the growth and interoperability available to them.

FPKI Crawler - <http://fpki-graph.fпки-lab.gov>

Reports - <http://fpkiapps.icam.pgs-lab.com/fbcaApps/>

FPKI Technical Working Group

At the latest FPKI Technical Working Group (TWG) discussed two topics:

1. Acceptance of the Mount Airey Ozone Server Testing Report
 - a. The FPKIMA conducted Path Discovery and Validation (PDVAL) testing on the Mount Airey Ozone Server as a static path validator. The TWG formally accepted the testing report and, if approved by the FPKI Policy Authority (FPKIPA), will be added to the PDVAL Product List (PPL).
2. Discussion on FPKI Content Delivery Network (CDN)
 - a. The FPKIMA is exploring the use of a Content Delivery Network (CDN) service to improve availability, security and performance, but a few agencies with tight egress controls may not be able to interoperate. A hybrid model combining both CDN and maintaining the current HTTP repository for those with tight egress controls was discussed as the most likely implementation option. Further technical analysis and discussion will occur prior to implementation.

If you would like to be added in the TWG listserv, send an email to help@fpki.gov.



**Federal PKI
Management Authority**
Enabling Trust

**Need Help?
Have Questions?**

**Contact the FPKI Help
Desk**

help@fpki.gov

Did you know....

Someone could steal your password by listening to you type?

Acoustic cryptanalysis is a type of side-channel attack on Information Technology (IT) systems that exploits the high-pitched sounds our systems emit due to the vibrations of electronic components. Sound patterns can convey corresponding operations, and reveal sensitive information such as passwords and PINS for cryptographic keys.

Ask the FPKIMA



When I check the path of my certificate it says it was issued under the Netherlands Ministry of Defense, why?

- The FPKI is a large and complex federated PKI environment with many cross-certified Affiliates. This structure has the potential to create multiple paths from an end user's certificate. The path validation software used by your agency determines the route to validate a certificate to a root in your trust store and in some cases it means traversing another Entity's certificate path. The Netherlands Ministry of Defense is just one of the international partners with a trust relationship with the Federal root. The FPKI AIA Web Crawler is an excellent visual tool to see these relationships in real time (<http://fpki-graph.fpki-lab.gov>). Reports and P7B files are also available (<http://fpkiapps.icam.pgs-lab.com/fbcaApps/>)

Where can I find more information on the FPKI and FPKIMA?

- Information on the FPKI and FPKIMA can be found on the idmanagement.gov website.

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

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