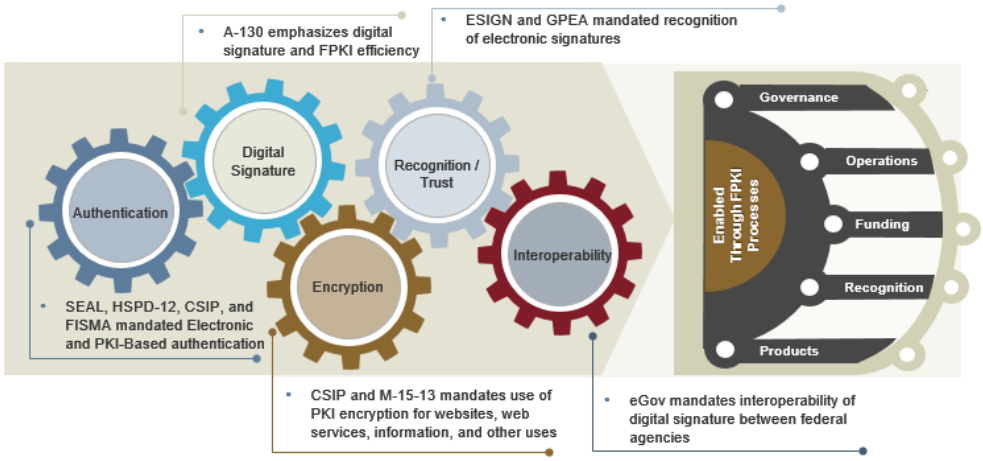
FPKIMA Newsletter

Winter 2017
Volume 4 Issue 2

Federal PKI Management Authority
Enabling Trust

How Do You Use the Federal PKI?

The Federal PKI was designed to meet multiple federal mandates as an efficient and secure means to conduct digital business. Even though the Federal PKI has existed since the late 1990's, it was officially mandated in the E-Government Act of 2001 (eGov Act). The General Services Administration (GSA) was tasked, as part of the act, to establish a Federal Bridge Certification Authority for digital signature interoperability between preexisting Federal Agency PKIs. As the years rolled on, digital signature interoperability led to authentication with the issuance of Homeland Security Presidential Directive 12 (HSPD-12) and encryption with the Office of Management and Business (OMB) Memo 15-13 *Policy to Require Secure Connections Across Federal Websites and Web Services*. The Federal PKI Management Authority (FPKIMA) conducted a policy analysis and found nine main policy drivers which aligned with five core PKI use cases outlined in the graphic below.



Federal PKI Mandates Aligned with PKI Use Cases and Enabling Processes

One of the more interesting policy drivers is around recognition or trust of electronic signatures (digital signature being the most secure form of electronic signature). The Electronic Signature in Global and National Commerce Act or ESIGN was enacted in 2000 to help increase the use of electronic records and signatures in interstate and foreign commerce. Electronic signature recognition has not been fully realized yet, but the Federal PKI supports this capability by ensuring it integrates national and international standards for digital signature interoperability and is included in Application Trust Store Programs. An Agency that interacts with foreign governments or companies may take advantage of this capability by accepting digitally signed documents instead of traditional paper and pen methods. The same holds true for domestic companies interacting globally through using the PIV-I and other approved Federal PKI credentials.

Is your agency using the Federal PKI for something other than the five core use cases or following a federal-wide policy not identified by the FPKIMA? Tell us (FPKI@GSA.gov) so we can add it!

Inside This Issue

Updated PIV Guide Website

The GSA FICAM Office has released an updated PIV Guide website under the new https://piv.idmanagement.gov. The PIV Guide is your one-stop shop for all things policy and technical to implement a PIV infrastructure. It is a community-driven resource on PIV details, certificate trust, network authentication, developer guides, user guides, and much more. Visit it today and join the Federal PKI development team by submitting your own content!

Nationally Recognized

Federal PKI Use In and Around the Government

The Federal Bridge's mission is to act as an interoperability hub for the Federal Government; state and local governments as well as private companies can take advantage of it too. Some benefits of the Federal PKI for global and national ecommerce include:

1) **A contract clause for secure authentication or digital signature**. Does your agency or company have a requirement for strong assurance of people or documents? Use Federal PKI credentials as a contract clause to ensure you are using the strongest form of digital identity that aligns with NIST requirements. GSA Access Certificate for Electronic Services (ACES) business representative certificates and PIV-I were both specifically designed as high assurance citizen credential. The Federal PKI is also natively trusted by Microsoft, Apple, and Adobe for authentication and digital signature. Federal PKI credentials are also trusted throughout the European Union (EU) and European Economic Area through the SAFE Bio-Pharma program and meet the strict EU requirements for legal digital signatures. One example is the Department of Defense (DoD). They require all business partners who do not qualify for a CAC card to use an external PKI credential issued from an approved Federal PKI partner. This ensures that external PKI providers meet NIST standards for high assurance credentials before accessing or sharing DoD information.
2) **A single credential for use with Business to Government (B2G) interaction.** Is your company required to submit regulatory or other types of documents for government compliance? Hopefully you are already using a Federal PKI credential to authenticate and digitally sign your submissions. Federal Drug Administration, Drug Enforcement Agency, Government Publication Office, and Patent and Trademark Office are just a few of the agencies who rely on Federal Bridge credentials to decrease the cost of paper submissions. Still submitting paper-based forms? Wish you could digitally sign them? Tell the FPKI (FPKI@GSA.gov) so we can help!
3) **A single credential for use with state and local governments.** The Federal PKI is not just for the Federal Government; state and local governments can take advantage of the Federal PKI too! The Florida Department of Transportation, City of Tallahassee (FL), West Virginia Department of Environmental Protection, and the Virginia eNotary program are a few of the state and local governments utilizing Federal PKI for digital signature. Virginia recently passed a new digital identity management law (https://go.usa.gov/xXNpB) with the ultimate goal of realizing truly interoperable digital identities based on a strongly validated credential (e.g., similar to a state issued HSPD-12 credential, but the credential is issued by any trusted identity provider if it meets certain criteria).

The Federal PKI was designed and built for authentication, encryption, and digital signature needs of the Federal Government. Does your agency use external credentials or username and password for citizen-based access? Make sure you are using an approved Federal PKI external credential to mitigate access risk! Send an email to the FPKI (FPKI@GSA.gov) to find out.

Contribute Content to the FPKI Guides on Github!

The Federal PKI is looking for user guides, best practices, and implementation guidance on the Federal PKI. Examples include updating trust store configurations, parsing certificate information, identifying Federal PKI CAs and other useful information. Do you have useful guidance that has helped your agency? Post it as an issue or open a branch on the FPKI Guide Github site. Check it out today! https://github.com/GSA/fpki-guides

It's Official!

The National Institute of Standards and Technology (NIST) officially supports RSA key sizes larger than 2048 including 4096 bit keys. What does this mean to you? Not much unless you are operating a root PKI then it is totally big news. This change is already reflected in NIST Special Publication 800-131A revision 1 and will be included in FIPS 186-4 in the near future. More information at https://go.usa.gov/xXNdG.

Increase Data Security with the Federal PKI

The Federal PKI is one of the most effective tools available to ensure confidentiality, integrity, and availability of government electronic data. The Federal PKI takes the effort out of identifying implementation standards and ensures vendors and other federal agencies are operating securely. For example, both DoD and DEA require external users to acquire Federal PKI PIV-I, software PKI or other approved credentials before either gaining access or submitting official documents. To learn more, go to https://go.usa.gov/x3tRm

U.S. CERT Alert

U.S. CERT released an alert on HTTPS interception software potentially weakening TLS security. If not deployed properly, the products could give a false sense of security and potentially break otherwise good TLS connections. Read the alert for more information; https://go.usa.gov/xXNfY.

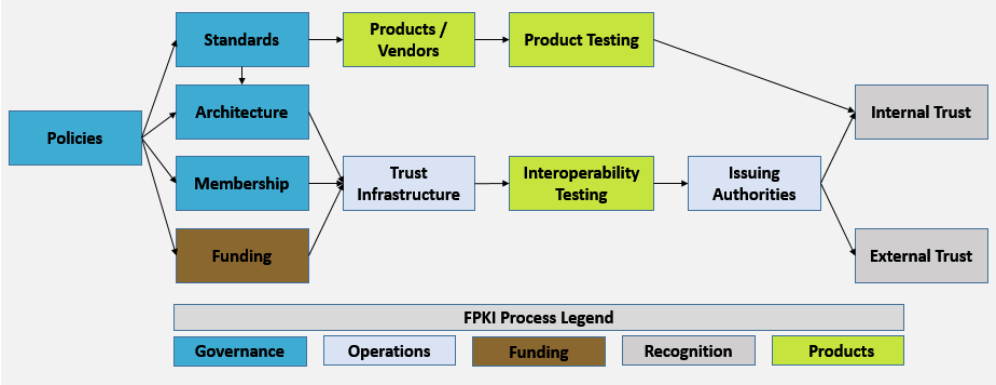
Federal PKI Supply Chain

The Ingredients to Delivering Trusted Credentials

The trust created by the Federal PKI is not a simple process. It takes federal-wide interaction to ensure it meets the latest federal and international standards, functions as designed, and will remain trusted after credential issuance. The FPKIMA analyzed the Federal PKI as a holistic system from policy to user and found there were five distinct processes and twelve activities, as shown in the figure below.

The Federal PKI Governance process is defined by the following activities:

1. Policies (Public Laws, Executive Orders, OMB memos and others)
2. Standards (NIST, IETF, ISO/ITU, and PKI audit standards)
3. Architecture (service management, planning, hierarchy, and strategy)
4. Membership (Trust Infrastructure, SSPs, Non-Federal, and Federal issuers)



The Federal PKI Supply Chain – Enabling Processes and Activities

Funding is received through both appropriated and cost recovery mechanisms and involves holistic funding of the supply chain components. Products are the technical application of the Federal PKI and include both Products / Vendors and Product & Interoperability Testing. Federal PKI Operations is the actual PKI infrastructure which includes the FPKI Trust Infrastructure (FPKIMA) and Issuing Authorities (Shared Service Providers, GSA Managed Service Offering (MSO), Federal Issuers, and Non-Federal Issuers). Recognition is the most crucial part; this includes both the External trust by relying parties outside of the Federal Government (such as application trust stores, industry groups, and citizens) and Internal Trust by relying parties inside of the Federal Government (including federal agencies, federal websites, and cross-agency digital signatures).

Each process and activity is vital to ensure a trusted Federal PKI credential is both issued properly and enabled for recognition by internal and external relying parties. The Federal PKI has been successful in matching equal parts business and technology to realize its mandated value. Continued success relies on identifying and understanding future PKI use cases and how best to integrate them. It requires national and international collaboration for the Federal PKI to remain a relevant, secure shared service for the Federal Government. How is the Federal PKI doing in meeting its mandated value? Did we miss something in our process or activity analysis? Let us know! Email the FPKI (FPKI@GSA.gov) to start the conversation.

FPKI Working Group Updates

The Certificate Policy Working Group met in March to discuss the following topics:

1. **Change Proposals** – A number of change proposals were reviewed or discussed. Once finalized they will be submitted for a vote by the Federal PKI Policy Authority (FPKIPA). The change proposals include:
    - Require FPKIPA Notification in FPKI Affiliate Infrastructure Changes
    - Restrict Use of Test, Pre-Production or Similar Names in Production Environment
    - Expired Card Stock Use After Approved Product List Removal
    - Security Incident Notification Requirements
    - Limit FPKI Affiliate Logical Relationship to One Path
2. **CPWG Meeting Approach** – A suggestion was made to integrate best practices from similar industry based meetings to include new initiatives having committed volunteers, rotating the secretariat function, and a more data/requirements driven approach.
3. **Annual Audit Review Requirements Comment Adjudication** – The CPWG adjudicated comments on the new annual audit requirements.

The FPKI Technical Working Group is scheduled to meet in April to discuss Derived PIV Technical Implementation Challenges. Participation in Federal PKI working groups (https://go.usa.gov/x5bFy) is limited to federal agencies and Federal PKI affiliates. Please send any questions to FPKI@GSA.gov.

Ask the FPKIMA

Where can I find information on all the Federal PKI Certification Authorities (CAs)?

The Federal PKI Graph (https://fpki-graph.fpki-lab.gov) is the best resource to find information on all Federal PKI CAs and a majority of Federal PKI Affiliate CAs. It is a graphical representation of the Federal PKI with Federal Common Policy in the center of the graph.

There are also machine readable resources on the Federal PKI Crawler website (https://fpki-graph.fpki-lab.gov/crawler). It includes graph output in CSV, HTML and XML. It also contains P7B files which include different certificate configurations of all certificates under Federal Common Policy and then specific Federal PKI and Federal PKI Affiliate CAs. Is there something missing? Need other kinds of Federal PKI information? Please contact the FPKI so we can help (FPKI@GSA.gov).

Where Can I Find More Information on the FPKIMA?

FPKIMA information can be found on the idmanagement.gov website: https://go.usa.gov/xr2rR.

Federal PKI Management Authority
Enabling Trust

Need Help?

Contact the FPKIMA
FPKI@GSA.gov

Explore the IT Security Hallway yet?

The GSA Acquisition Hallway aims to help federal acquisition official's work smarter, faster, and better by connecting experts from across the government. The IT Security Hallway on the Acquisition Gateway helps Federal Government buyers from all agencies find and share the latest information on IT Security acquisition information. The Acquisition Gateway features information on government-wide contract vehicle comparisons, acquisition best practices, market research tools, prices paid data, and other useful tools and features. The website is open to federal and non-federal users with full site access for federal acquisition employees and approved contractors. Sign up at https://hallways.cap.gsa.gov/