

FPKIMA Newsletter

Summer 2015
Volume 2 Issue 3



**Federal PKI
Management Authority**
Enabling Trust

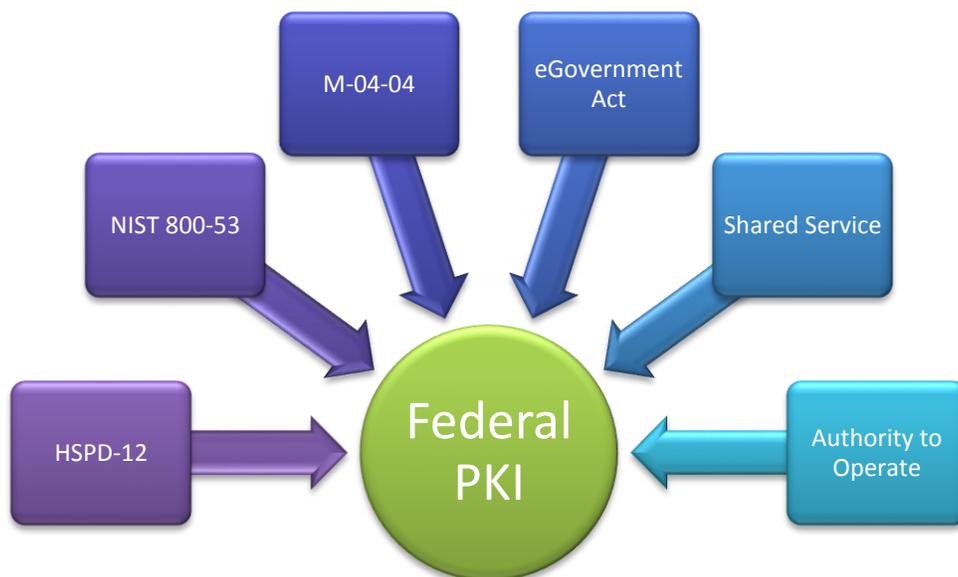
INSIDE THIS ISSUE

Federal PKI, the Government PKI Standard	1
The AAA's of Logical Security	2
Types of Secure Socket Layer (SSL) Certificates	3
FPKI Technical Working Group	4
Ask the FPKIMA	4

In response to the Office of Personnel Management (OPM) breach, the Office of Management and Budget (OMB) gave agencies 30 days to take immediate and specific actions to further improve the security of systems and data. As part of the "CyberSprint," the FPKIMA is assisting GSA to identify gaps in Federal PKI services. If your agency has identity and authentication needs that are not being met, let us know! Send an email to fpki-help@gsa.gov

Federal PKI, the Government PKI Standard

One of the often overlooked benefits of the Federal PKI is the government's ability to point to one standard or requirement for PKI-based authentication. This is an amazing benefit for acquisition, technology, and executive-level professionals when making critical access management decisions. The Federal PKI takes the work out of identifying implementation standards, ensuring vendors and other federal agencies are operating their PKI in a secure manner, and guaranteeing availability of Federal PKI Trust Infrastructure services upon which HSPD-12 Personal Identity Verification (PIV) cards rely.



The Federal PKI is a single requirement federal agencies can use when writing contract vehicles for identity and authentication services

The Federal PKI encompasses services for federal and nonfederal subscribers. For example, the Department of Defense requires any industry partner's PKI to be cross-certified with the Federal Bridge and the Drug Enforcement Agency (DEA) requires any PKI-based electronic prescription to validate across the Federal Bridge. In both cases above, industry PKI partners apply for cross-certification with the Federal Bridge so they can issue a comparable credential which is trusted by either federal or industry relying party applications.

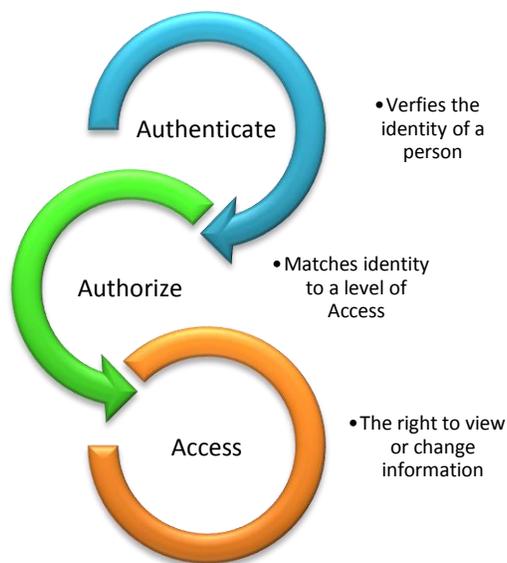
Part of ensuring industry PKIs offer a comparable credential is the Federal PKI compliance team validating that the level of assurance matches the high government standard. Is your agency leveraging the Federal Bridge for citizen access? For more information on who issues Federal Bridge credentials including the PIV-Interoperable (PIV-I) hardware token, go to <http://idmanagement.gov/federal-public-key-infrastructure>.

The AAA's of Logical Security

Authentication, Authorization, and Access

It is sometimes easy to forget the power of a PKI credential if an application is not configured properly. Specifically, in the Federal PKI, federal agencies may be apprehensive about using the Federal PKI for citizen access because of a common misunderstanding of what a Federal PKI credential grants. If a web server is configured properly, the only thing a PKI credential should grant is authentication or the ability to logically validate a user's identity.

Authentication is derived from the Greek word, *authentikos*, meaning real or genuine. In the federal government, authentication is the process of verifying a claimed identity is genuine and based on valid credentials; this can be accomplished through a variety of mechanisms including challenge/response (knowledge based questions), time-based code sequences (RSA key), biometric comparison or PKI. The federal government relies on the FPKIMA to ensure the PKI certificates on a user's PIV card or Common Access Card (CAC) can be easily validated.



Federal relying parties should utilize the FPKI for federal employee and citizen access to their web-based applications

Once an identity is authenticated, an authorization decision can be made to grant or deny requests for obtaining and using information. The data owner will make the authorization decision to allow access to their information using a risk-based decision process. The higher the risk, the higher level of identity assurance. A Federal PKI credential does not automatically authorize the credential owner to access internal databases or change permissions. The data owner determines who should have access to information and what the user is entitled to do with it. The Federal PKI credential is another tool for a federal agency to use to logically validate a user's identity and provides stronger assurance than a username and password.

Did you know?

The FPKIMA hosts a Technical Working Group (TWG) to develop and discuss the technical future of the Federal PKI. If your agency is not participating your agency's needs may not be heard. Send an email to fpki-help@gsa.gov to join.

OMB released Memo 15-13 "Policy to Require Secure Connections across Federal Websites and Web Services" or the HTTPS Memo on June 8, 2015.

This memo requires publicly accessible federal websites and web services to only provide service through a secure connection or HTTPS. Take your security a step farther by using Federal PKI SSL Certificates. Federal PKI offers automatic compliance with HSPD-12 and multiple e-government acts. Need more information? Send an email to fpki-help@gsa.gov.

Types of Secure Socket Layer Certificates

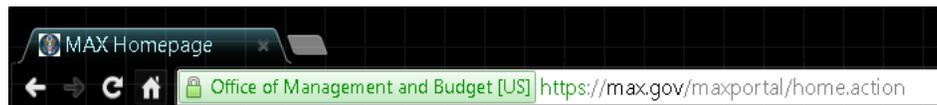
What the Green Address Bar Really Means

With the recent release of the OMB HTTPS Memo, many federal agencies are scrambling to secure their public websites. What is HTTPS and why does the address bar sometimes turn green in color? HTTPS utilizes the Secure Socket Layer (SSL) or Transport Layer Security (TLS) which are internet protocols to establish a secure channel between a user/client and a server. Although SSL and TLS are used synonymously, TLS is the SSL successor which allows the server and client to authenticate each other and to negotiate an encryption algorithm before sending data which does not happen with SSL. SSL/TLS utilizes digital certificates for a user to authenticate the website and then creates an encrypted channel for safe website browsing. The intent of the digital certificate is to certify the website owner's identity and address have been validated by a third party. The added benefit of using digital certificate also helps to mitigate the threat of website spoofing while creating an encrypted channel to securely share information between a user and a website.



Standard SSL Certificate Example

Major browser vendors such as Microsoft (Internet Explorer), Google (Chrome), and Apple (Safari) are working together to help users identify SSL by adding visual cues in the address bar. The easiest way to identify if a website is using SSL is to look for the "HTTPS" in front of the website address in addition to the use of a padlock and different colors in the address bar. Browsers are also using other tools such as a yellow triangle over the padlock to show there may be an issue with the SSL certificate.



Extended Validation SSL Certificate Example

There are currently two major types of SSL certificates: standard SSL and extended validation or EV SSL. A standard SSL certificate requires some level of identity proofing of the organization and the server. An EV SSL certificate is intended to give the user more confidence in the validation and ownership of a website. This validation also includes posting public audit records and including the organization name in the address bar and certificate. Depending on the browser, the address bar may be totally green (Internet Explorer) or contain a green box preceding the website address (Chrome) to indicate an EV SSL certificate.

The next time you are surfing your favorite website and are about to input your credentials, notice if they are using SSL. If not, ensure you are on the correct website by putting an "HTTPS://" in front of the website address.

The new Federal Information Technology Acquisition Reform Act or FITARA has been described as the most far-reaching IT reform legislation since the Clinger-Cohen Act of 1996. The GSA Information Technology Services (ITS) Division, which the FPKIMA falls under, is working on new initiatives and strategies to improve government-wide IT acquisitions across the government and add value without further agency investment. The newest initiative agencies can currently leverage is the Common Acquisition Platform or CAP which is a government-wide acquisition collaboration tool to drive smarter acquisition through greater knowledge on government buying power. For more information, go to <https://hallways.cap.gsa.gov/>

FPKI Technical Working Group

The FPKI Technical Working Group (TWG) held a July meeting to discuss the Microsoft Certificate Reputation Program and SSL wildcard certificates. Highlights include:

- Microsoft presented an information brief on the Microsoft Certificate Reputation program. The program consists of three parts: 1) a trusted root store (which includes the Federal Common Policy), 2) an intermediate certificate blacklist, and 3) a smart screen feature built into Internet Explorer to capture and analyze SSL certificates. The intent of the program is to protect the user from fraudulent websites while also notifying certification authorities of compromised certificates.
- The Department of Homeland Security (DHS) presented an information brief on new system requirements of Microsoft SharePoint 2013. One requirement of SharePoint 2013 is to use SSL wildcard certificates which alleviate the need to issue hundreds of individual certificates to each SharePoint server or farm. The current Federal Common Policy Certificate Policy (CP) is vague concerning SSL and device certificates, but does not specifically state a wildcard is not allowed. The consensus of the TWG was to make a request to the Federal PKI Policy Authority (FPKIPA) to update the Federal Common Policy CP to address and improve the certificate policies around SSL and device certificates.

For more information about the FPKI TWG, send an email to fpki-help@gsa.gov.



**Federal PKI
Management Authority**
Enabling Trust

Need Help?

Contact the FPKIMA

fpki-help@gsa.gov

Did you know...?

The National Institute of Standards and Technology (NIST) has published a new standard for protection of controlled unclassified information (CUI) on nonfederal information systems? NIST Special Publication (SP) 800-171 is a tailored version of NIST 800-53 for use by nonfederal organizations that process, store, transmit, or receive CUI data from federal agencies. This can include state and local governments to contractor owned information systems. The new CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements to extend the protection of CUI data to nonfederal systems. For more information, go to http://www.nist.gov/itl/csd/20150618_sp800-171.cfm

Ask the FPKIMA



What is a Common Derived Credential and Derived PIV?

A derived credential, as explained in NIST special publication 800-63-2, is a credential that leverages the identity proofing and vetting of a current valid credential. When applied to PIV, the identity proofing and vetting of the PIV card is used to issue a Common Derived PIV credential. For all intents and purposes, a Common Derived PIV credential is a PIV credential and, when used, can be reported as “PIV-enabled” to meet the goals set forth in HSPD-12.

The current focus of the Common Derived PIV credential is for network authentication with mobile devices where a PIV card is not practical. For more information on Common Derived PIV compliant hardware and software, check out the FIPS 201 Evaluation Program which contains the Approved Product List (APL) for FPKI and PIV compliant hardware and software (<http://www.idmanagement.gov/ficam-testing-program>).

Where Can I Find More Information on the FPKIMA?

FPKIMA information can be found on the [idmanagement.gov](http://www.idmanagement.gov) website:

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