

FPKIMA Newsletter

Fall 2016
Volume 3 Issue 3



**Federal PKI
Management Authority**
Enabling Trust

INSIDE THIS ISSUE

National Cyber Security Awareness Month	1
Shaping the National Cyber Landscape	2
Home Grown Cyber Initiatives	3
FPKI Working Group Updates	4
Ask the FPKIMA	4

It's Official!

The OMB Circular A-130 Managing Information as a Strategic Resource has been officially updated.

Federal PKI plays a prominent role by integrating requirements to help agencies improve their security posture.

Some of the most important changes include identifying the GSA

FPKIMA as the operator of the Federal PKI Trust

Anchor and all agency PKI issued in accordance with FPKI policy must validate

to a Federal PKI Trust Anchor. Use of the FPKI ensures your agency is meeting federal security guidelines. Go to

<http://go.usa.gov/xKJMu> for more information.

National Cyber Security Awareness Month

National Cyber Security Awareness (NCSAM) month is in full swing for the month of October with the federal government leading the way! Each week in October featured a variety of themes with different federal agencies hosting cyber awareness events to inform, educate, and protect both government and citizens. One week featured articles “From the Break Room to the Board Room” with the most prominent advice to recognize and avoid phishing attacks, make passwords more complex, and report suspicious activity.

Luckily, the federal government has the Federal Public Key Infrastructure (PKI) to thwart the majority of cyber related attacks through use of the Personal Identity Verification (PIV) card and other Federal PKI credentials. For example:

- 1) **Phishing Emails and Social Engineering** - A phishing email is an official or authentic-looking email with links to malicious sites or with malicious attachments that steal personal, financial, or organization information.

How To Protect Your Agency - Use a PIV or PIV-Interoperable (PIV-I) card to send digitally signed emails and ask your business partners to do the same. A digitally signed email authenticates the sender and provides assurance it was sent from a trusted source or person. The Federal PKI has a home for both federal and citizen users! Using a PIV, PIV-I or other Federal PKI credential to send and receive digitally signed email can significantly decrease the threat of phishing and other email-based attacks. In addition, a digital signature provides an integrity check that ensures the content was not altered during delivery (e.g., a malicious attachment added).

- 2) **Password Attacks and Network Intrusions** - Password guessing, password cracking, unsecure password update methods, and other forms of potential password compromise put an agency’s network and internal assets at risk.

How to Protect Your Agency - Stop using passwords and start using PIV, PIV-I or other Federal PKI credentials to enable your enterprise and web portals for two factor authentication. Don’t know how? Looking for guidance? Join the Federal PKI implementation team, an open collaboration forum to create, post, and update Federal PKI implementation guidance, at <https://github.com/GSA/fпки-guides> or <https://gsa.github.io/piv-guides/>.

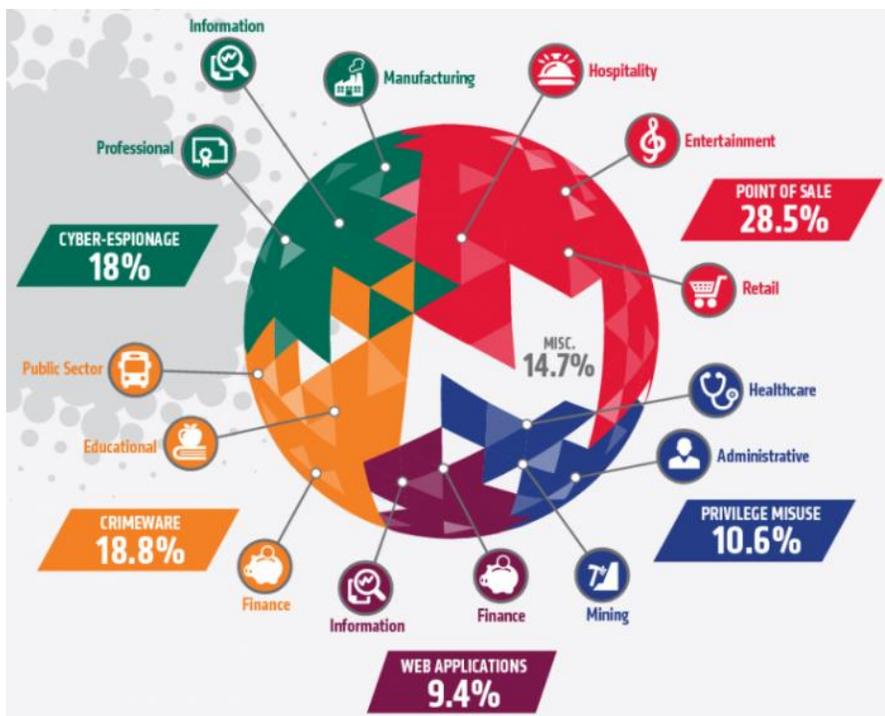
Federal PKI can solve many cyber-related issues such as secure tunneling or virtual private networks, single sign-on, and access control. The Federal PKI supports PIV for federal employees and contractors and PIV-I or other software-based PKI solutions for short-term employees and external business partners who may not qualify for a PIV card. Have questions, concerns, or requirements? Ask the FPKIMA! Send an email to fpkima-ma@listserv.gsa.gov and find the solution that best fits your application or agency’s needs in meeting federal cyber requirements and mandates.

Shaping the National Cyber Landscape

Federal Outreach Efforts to Secure Cyberspace

Cybersecurity has and will continue to be an important topic from the break room to the board room as more physical assets become digitized. The Cybersecurity National Action Plan issued by the White House in February 2016 outlined both federal and national actions to secure cyberspace as described below.

1. Enable Multi-factor authentication access for web based accounts - According the Verizon Breach Report, 9.5 percent of cyber-attack patterns originate through a web application from compromised credentials. Using strong authentication, such as multifactor or two-factor, adds an additional layer of security beyond a username and password to protect credentials. Enable strong authentication if it is offered and go to <https://www.lockdownyourlogin.com/> to learn more.



Cyber Threat Vectors by Industry (Source: Tripwire.com and Verizon Breach Report)

2. The Federal Trade Commission (FTC) relaunched identityTheft.gov to serve as a one-stop shop for victims of identity theft. The site provides a personal recovery plan, pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors.
3. The Small Business Administration partnered with the FTC, NIST, and the Department of Energy to offer small business cybersecurity training. For more information, go to: <https://www.sba.gov/managing-business/cybersecurity>.

Securing cyberspace is a national challenge and the Federal Government is taking near-term actions to align with a long-term cyber strategy.

NIST Releases Cryptographic Standard Guide

NIST released two special publications on the directives, policies, and mechanisms for using cryptographic standards in the Federal Government. NIST SP 800-175A and 175B outline the background and tools an agency can use to protect sensitive, but unclassified data both at rest and in transit. For more information, see NIST 800-175A

<http://go.usa.gov/xKJz2> or NIST 800-175B <http://go.usa.gov/xKJzZ>

Are you a NCSAM Champion?

The National Cyber Security Alliance is a public-private partnership promoting cyber security awareness for all users. They sponsor a NCSAM Champion program for companies, schools, nonprofits, government, and individuals to represent their cyber awareness contributions. For more information, go to

<https://staysafeonline.org/ncsam/champions/>

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 work 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>

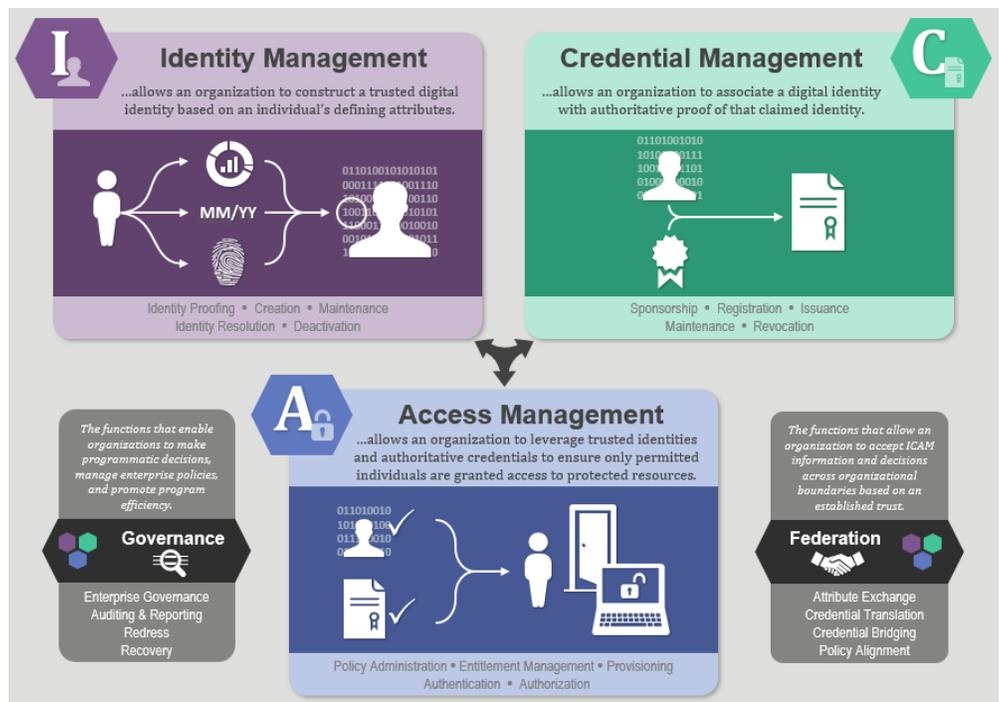
OMB Memo 16-24
 Newly released OMB Memo 16-24 revises the policy on the role and designation of the Senior Agency Official for Privacy (SAOP). This memo gives more power to the SAOP in agency privacy policy making, compliance, and risk management. Read the memo for more information:
<https://go.usa.gov/xKJaf>

Home Grown Cyber Initiatives

Federal PKI as the Cybersecurity Foundation

Protecting federal physical and digital assets is more important today than ever. Strong authentication of users and devices with a foundation in the Federal PKI reduces risk and increases return on investment. The Federal PKI has internal and external credential solutions for all agency identity management needs. The Federal PKI can solve the following use cases and many others:

- Software based authentication using FPKI approved external citizen credentials (See GSA eOffer / eMod <http://eoffer.gsa.gov/>).
- Strong authentication using PIV for cross-agency authentication (see OMB Max.gov <https://login.max.gov/>).
- Strong authentication using PIV-I for business partner access (see DoD JPAS <https://jpasapp.dmdc.osd.mil>).
- Digitally signed and encrypted email to and from both federal and business partners.
- Digitally signed document recognition for both federal and citizen signers.
- Document and digital artifact encryption.



FICAM Business Architecture (Source: GSA FICAM)

The Federal PKI is a solution that aligns with each Federal Identity, Credential, and Access Management (FICAM) architecture area and ensures automatic compliance with multiple federal laws and mandates. Does your agency have an identity management use case that is not met by the Federal PKI? Need guidance on how to accept Federal PKI PIV, PIV-I or approved citizen credentials? Increasing risk and cost in maintaining external user credentials? Ask the FPKIMA (FPKIPMA@listserv.gsa.gov) how the Federal PKI can be fully leveraged for agency needs.

FPKI Working Group Updates

The Technical Working Group (<https://go.usa.gov/x3tEm>) held its quarterly meeting to discuss the following topics:



**Federal PKI
Management Authority**
Enabling Trust

1. **Use of AnyEKU** - The Microsoft Trusted Root Program released a new requirement that no certificates should assert the AnyEKU extension which is a catch all extension to allow any type of usage. The group discussed impact and potential risk of completely removing use of the AnyEKU.
2. **64-Bit Serial Entropy** - Industry PKI has a new requirement for 64-bits of serial number entropy in all certificate serial numbers. The group discussed current product limitations and risks the requirement attempt to mitigate.
3. **HTTP Cache Control Headers for PKI Artifacts** - HTTP cache control headers can be used to set the level of how often PKI artifacts should be retrieved. Some Federal PKI issuers have large certificate revocation lists downloaded thousands of time a day which may impact application or server performance and potentially the user's experience from due to time out errors. Setting a HTTP Cache Control header requirement in is one potential solution to increase performance and decrease errors.
4. **Weak Key / Random Number Generator Checks** - This was a follow-up discussion on tools, techniques, and methods to identify weak random number generators and weak key. No current products or services perform this type of check and it may become a new requirement to meet Industry PKI standards.

Participation in Federal PKI working groups is limited to federal agencies and Federal PKI affiliates. Please send any questions to FPKI-Compliance@gsa.gov.

Ask the FPKIMA



What is a Publicly Trusted PKI Certificate? Is it Different than My PIV Card?

Public PKI trust is created by PKI Root Certificate distribution from a software vendor's trusted root program. The main trusted root programs are operated by Microsoft, Apple, Mozilla, Oracle (Java), Adobe, and Google (Chromium-based browsers and Android). Each vendor program is operated independently, but follow a set of agreed upon industry PKI baseline requirements. A publicly trusted PKI certificate is one issued by a PKI Root Certificate that is included in one of the trusted root programs. To be completely trusted, the Root must be in all programs or else a user may experience errors between software vendors (e.g., a security error appears in Google Chrome but not Apple Safari). The Federal PKI has a Root in three of the seven trust stores so while a PIV card is publicly trusted by some, it is not trusted by all. The Federal PKI is working diligently to meet all public trust requirements and to have a Root Certificate accepted in all trusted root programs.

Where Can I Find More Information on the FPKIMA?

FPKIMA information can be found on the idmanagement.gov website:
<https://go.usa.gov/x3tPF>.

Need Help?

Contact the FPKIMA
fpki-help@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/>