

FPKIMA Newsletter

Fall 2015
Volume 2 Issue 4



**Federal PKI
Management Authority**
Enabling Trust

INSIDE THIS ISSUE

National Cyber Security Awareness Month	1
PKI Attack Vectors	2
News From Around the Federal PKI	3
FPKI Technical Working Group	4
Ask the FPKIMA	4

The Office of Management and Budget (OMB) is proposing for the first time in 15 years an update to Circular No. A-130, Managing Information as a Strategic Resource. A-130 provides general policy for the planning, budgeting, governance, acquisition, and management of Federal information resources. A new appendix specific to security and PKI has been added as well. For more information on the proposed revisions and how to submit comments, go to <https://a130.cio.gov/>

National Cyber Security Awareness Month

Recognizing the importance of cyber security to our nation, President Obama designated October as National Cyber Security Awareness Month. It is designed to engage and educate the public and private sectors through different activities and awareness campaigns with the overall goal to increase awareness on staying protected while connected and improving resiliency during a national cyber-incident.

Together, the Federal Government and its commercial partners are driving private and public knowledge and sharing on cyber security issues and threats, creating a safer and more resilient digital life for Americans. Examples include:

Federal PKI Management Authority (FPKIMA) - To help increase understanding and use of the Federal PKI, the FPKIMA published two user guides on the technical overview and trust store management. See page 3 for more information.

Department of Homeland Security (DHS) - DHS is a National Cyber Security Awareness Month champion with weekly information campaigns to drive public knowledge of cyber security. “Stop.Think.Connect” is a national public awareness campaign aimed to increase the understanding of cyber threats and empower the American public to be safer cyber civilians. For more information, go to <http://www.dhs.gov/national-cyber-security-awareness-month>.

Department of Energy - The Energy Office of the CIO recently hosted a number of government-only cyber-related presentations highlighting cyber policy development and practices, emerging threat identification and strategy, individual cyber responsibility, supply chain risk, technical innovation and workforce development.

National Institute of Science and Technology (NIST) - NIST, in coordination with DHS and DoD, continues to lead the implementation of the National Initiative for Cybersecurity Education (NICE) by both government and industry. NIST NICE is designed to accelerate learning and cyber skill development, nurture the diverse cyber learning community, and guide cyber career development and workforce planning. NIST has published distinct user guides for academia, employers, and government to tailor specific skills (<http://csrc.nist.gov/nice/>).

Federal Bureau of Investigation (FBI) - The FBI continues to implement public-private cyber information sharing partnerships and report on cyber success stories. For more information on the FBI’s cyber information sharing program, go to <https://www.infragard.org/>.

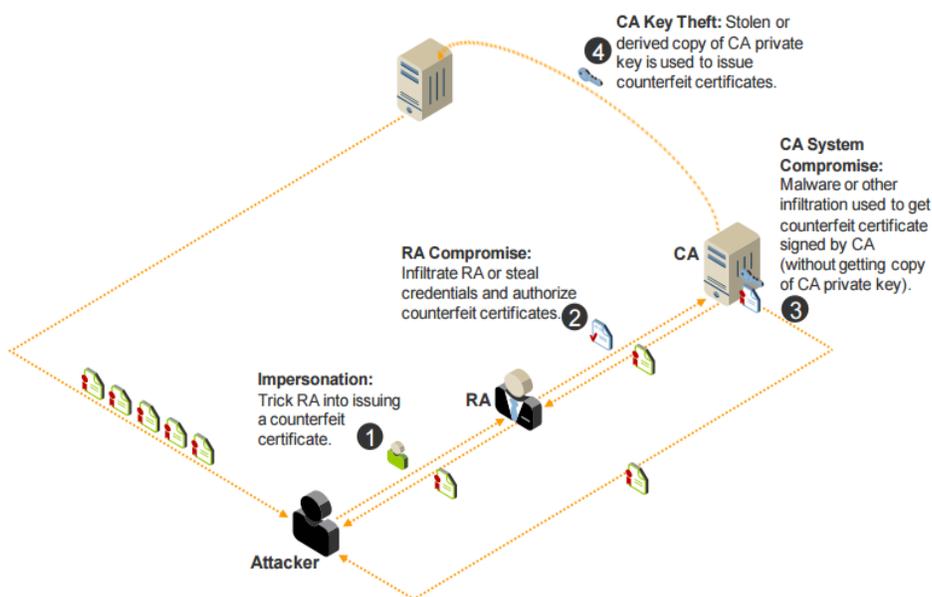
Small Business Administration (SBA) - The SBA unveiled a brand new website as a resource for small business owners to discover online courses, training opportunities, blogs and webinars, as well as cyber security information tips and best practices. Learn more at <https://www.sba.gov/cybersecurity>.

PKI Attack Vectors

General Classes of Attacks on CA Operations

The Federal Government relies on PKI as the foundation for physical and logical access control, but, in general, these systems are a high value target for cyber-attacks. Four general classes of attacks exist.

- 1) **Subject:** A subject is a person, organization, group, or device that is issued a certificate and whose identity is verified. The level of identity vetting is usually aligned with a level of assurance by asserting a specific certificate policy. A subject can impersonate another individual and present fraudulent documents to trick a Registration Authority (RA) into issuing a certificate. This is often mitigated through verifying the submitted subject information against two forms of identification which is also verified.
- 2) **Registration Authority:** An RA validates the identity of the person or the device, the device's owner, and device's address (i.e., fully qualified domain name). The RA function may be outsourced to an approved third party or performed by the same organization operating the CA. As an intermediary, an RA can be infiltrated to send fraudulent information to the CA causing it to issue a certificate. This is often mitigated through RA system segmentation and multi-factor authentication to the RA application.



Multiple Attack Vectors Exist to Compromise a PKI (Source: NIST)

- 3) and 4) **Certification Authority (CA):** The CA is the actual software issuing certificates and certificate revocation lists. CA Key Theft through unsecure or compromised private key protection or a CA system compromise through malware or other methods are the most common classes of attack against a CA. These attacks are often mitigated through an air-gapped CA system, multi-factor authentication, and FIPS 140 approved cryptographic devices.

For more information, see NIST ITL Bulletin for July 2012 (<http://csrc.nist.gov/publications/PubsITLSB.html>).

The Federal PKI has updated their help desk and compliance emails!

Use fpki-help@gsa.gov for any help desk related questions

Go to the following for compliance questions or to submit audit paperwork
fpki-compliance@gsa.gov

What is DigitalGov?

DigitalGov is a platform to drive best practices in providing federal information and services to the public anywhere and anytime. It is designed to help agencies integrate digital services and drive open information sharing by finding and sharing resources, championing repeatable digital solutions, and opening federal information to the public. To understand how DigitalGov might be able to help your organization or see some of their latest projects, go to <http://www.digitalgov.gov/>

Did you know...?

A PKI has two essential business functions:

- 1) Secure operation of a Certification Authority*
- 2) Generate and publish certificate and revocation data*

The foundation of trust in a digital certificate relies on the secure operation of the issuing authority.

Secure CA operations require dual party control from vetted trusted roles for certificate activities. This operation must also occur in a secure area or facility.

Certificate data must be readily available in a repository or directory for trusted certificate validation. Revocation data must be regularly published to alert relying parties and applications of any certificate which is revoked and should no longer be trusted. Repositories containing certificate and revocation data must be highly available.

News From Around the Federal PKI

New User Guidance Published

In trying to meet the needs of the Federal PKI community, the FPKIMA is proud to announce two new user guides have been published. Each guide was developed to address specific requests from the community.

1) FPKI Trust Infrastructure Overview

The Federal PKI has grown into a diverse PKI ecosystem of hundreds of CAs for federal and state government agencies as well as foreign and US commercial participating PKIs. The purpose of this document is to provide a technical overview of the Federal PKI Trust Infrastructure and its PKI operations to include the value of PKI, certificate policies, certificate policy mapping, and other common questions on the FPKI.

2) FPKI Trust Store Management Guide

Ensuring proper certificate validation is one of the essential business functions of a PKI. To aid relying parties in properly validating certificates, the purpose of this guide is to provide exact steps to find and download the FPKI trust anchor certificate and certificate bundles. This includes how to install them through a variety of different means and methods gathered from government and commercial partners. This is an evolving guide as we continue to gather more methods and application specific steps.

The FPKI user guides described above can be found here (<http://www.idmanagement.gov/federal-public-key-infrastructure-management-authority>). Both are also meant to be living documents with continual updates made by interested parties. We are working to implement an open source version of the document following the best practices for open source in government created by the GSA Office of Citizen Services and Innovative Technologies (<https://www.digitalgov.gov/>). In the meantime, please send any comments, questions, or improvements to fpki-help@gsa.gov.

ICAM Information Sharing Day 2015

The Fall 2015 ICAM Information Sharing Day and Vendor Expo was held October 1st at GSA's 1800 F Street NW location. The day's motto was "Make a Connection!" and the event focused on the theme of working collaboratively across the Federal Government and with private partners to advance ICAM priorities.

The agenda touched on a variety of ICAM policy and technology topics such as shared services, enterprise access management, physical security, and attribute exchange. Speaker presentations are available to Federal government employees and contractors as well as non-federal employees performing Federal activities on the OMB MAX website (a Max.gov account is needed to access the material) (<https://community.max.gov/pages/viewpage.action?title=ICAM+Day+2015&spaceKey=Egov>)

FPKI Technical Working Group

The FPKI Technical Working Group (TWG) held an October meeting to discuss the standard certificate validation policies related to server certificate validation protocol (SCVP) and audit log processing standards. Highlights include:

- GSA's FICAM Testing Program presented a brief to update the group on the Logical Access Control System (LACS) category which includes the latest SCVP testing requirements and profile. For more information on the FICAM Testing Program or the HSPD-12 Approved Product List (APL) go to <http://www.idmanagement.gov/aproved-products-list>.
- Treasury hosted an open discussion on the need for standard certificate validation policies to help relying parties properly validate an FPKI certificate. Suggested improvements included creating a validation profile for PIV and PIV-I, formal guidance to help relying parties set up PKI trust stores to validate FPKI certificates, better defined policies to differentiate people from device certificates, and a policy to designate the Federal Common Policy CA as the federal trust anchor for all PKI.
- An FPKI auditor described a potential policy gap in log processing procedures. The current certificate policy for the Federal Bridge and common policy is ambiguous around how logs should be controlled and examined. A questionnaire was distributed to determine if the policy should be updated and if a best practice document should be drafted.

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



Ask the FPKIMA

Where can I find FPKI certificate status information?

FPKI certificate status information is stored in an online repository and can be accessed through two methods: a directory or HTTP access. A directory is used to store identity information in a hierarchical structure indexed by a unique identifier called a Distinguished Name or DN. The directory information can be viewed through a Lightweight Directory Access Protocol (LDAP) application.

HTTP access is a web-based file system that stores certificate revocation and validation information. The FPKI HTTP access system also stores bundles of certificates issued to and from the FPKI Trust Infrastructures CAs. The certificate bundles are stored in a machine readable encoded file with a ".p7c" file extension. On a Microsoft system, changing the file extension to ".p7b" allows the file to be opened in a graphic user interface. The content and location of the FPKI repositories is in a digitally signed document on idmanagement.gov (<http://idmanagement.gov/documents/urls-federal-pki-management-authority-fpkima-repositories-federal-bridge-ca-federal-common>).

Where Can I Find More Information on the FPKIMA?

FPKIMA information can be found on the idmanagement.gov website: <http://idmanagement.gov/federal-public-key-infrastructure-management-authority>



**Federal PKI
Management Authority**
Enabling Trust

Need Help?

Contact the FPKIMA

fpki-help@gsa.gov

Did you know...?

The Identity Ecosystem Steering Group (IDESG), a non-profit organization of industry, academia, and government partners created under the National Strategy for Trusted Identities in Cyberspace (NSTIC), has completed an Identity Ecosystem Framework (IDEF). It is a policy foundation and first step towards NSTIC's vision of widespread, trusted identity exchanges using federated methods that are secure, interoperable, privacy-enhancing and easy to use. The framework consists of three core documents that describe the identity ecosystem and the requirements, use cases, best practices, and approved standards for compliance. For more information, go to <http://www.idesg.org/IdentityRevolution>.