FPKIMA Newsletter

Winter 2021 | Volume 7, Issue 1

Federal PKI
Management Authority
Enabling Trust

Inside This Issue

GSA ICAM Solutions and Shared Services Roadmap

This document provides a response to the Office of Management and Budget (OMB) memorandum M-19-17. The roadmap primarily focuses on the steps and actions GSA will take to provide solution offerings that enable agencies to efficiently and cost effectively implement ICAM solutions aligned with OMB M-19-17, it also identifies areas of collaboration between GSA and other agencies supporting ICAM.

A copy of the ICAM Roadmap can be found here.

FPKIMA COVID – 19 Response

The COVID – 19 pandemic has caused drastic changes within our personal and professional lives. Federal Public Key Infrastructure Management Authority (FPKIMA) was well positioned to respond. We had previously laid the groundwork to move to offline certification authorities (CAs). The Federal Bridge CA G4 (FBCAG4) was already established as an offline CA issuing 30-day CRLs. The new Federal Common Policy CA G2 (FCPCAG2) was planned to be operated offline when it was established in October. Maintaining offline CAs that are isolated from network access can improve security and integrity. Of course, a CRL can be issued early as required, i.e. with any certificate revocation.

When the pandemic hit, the team was able to update current operational practices to take the current Federal Common Policy CA (FCPCA) offline with 30-day CRLs with minimal impact. This allowed maximum telework and limited the requirement for onsite personnel. In addition, trusted role holders were grouped into teams to reduce cross contamination.

Trust Stores Removal Update

The Federal Public Key Infrastructure (FPKI) was designed to support and facilitate interoperability of Public Key Infrastructure (PKI) systems for many different uses within the Federal Government and between government agencies and partners in industry. When the FCPCA was initially established, the FPKIMA applied for its inclusion in multiple public trust stores in order to enable both the government and partners to easily trust certificates issued within the FPKI for all potential uses.

In recent years, these public trust stores have become more focused on individual use cases, most notably Transport Layer Security (TLS) certificates for server authentication of publicly trusted web sites. Trust stores controlled by the vendors of Internet browser software have modified the requirements for inclusion in these trust stores to align with Baseline Requirements developed by the CAB Forum specific to publicly trusted server authentication certificates.

Since the CAs within the FPKI support many types of certificates, most notably those associated with government personnel use with both physical and logical authentication, they may not meet the same requirements for CAs intended for the sole purpose of issuing publicly trusted server authentication certificates. For this reason, the FCPCA was never accepted in the trust store managed by Mozilla; it was removed from the Apple trust store in 2018. Discussions were held with Microsoft about removing the FCPCA from their trust store, but testing the method by which Microsoft would perform the removal demonstrated there would be a negative impact on current internal government practices.

However, the FCPCAG2 will not be included in the Microsoft Trust store as a publicly trusted root. The new root was established as of October 2020; complete migration of the FPKI to the new root should be complete by the end of May 2021. At the end of that migration, the FPKIMA will request that Microsoft remove the FCPCA entirely from the public trust store. There will be no impact to the removal at that time as all relying party applications should have successfully migrated to enterprise reliance on the new FCPCAG2.

Federal Common Policy CA Update

In **October 2020**, the Federal Government created a new FPKI Root CA. The new root is named the **Federal Common Policy CA G2** (FCPCAG2). This new CA has issued new certificates to all CAs signed by the current FCPCA. This enables all current certificates issued by them to build a path to the new root.

What will be impacted?

This change will affect all Federal agencies and will have an impact on the following services:

- Personal Identity Verification (PIV) credential authentication to the government networks
- Agency web applications implementing client authentication (e.g., PIV authentication)
- User digital signatures that leverage PIV or similar credentials
- Other applications leveraging the FCPCA as a root including Physical Access Control System (PACS) implementations

When will this change take place?

- **Between now and May 2021**, agencies will need to transition from using the old FCPCA as the root to the new FCPCG2.
- **Last week of January 2021,** the new intermediate CA certificates must be published in CA repositories.
- **February 2, 2021**, the FPKIMA team will migrate the FBCAG4 to the FCPCAG2, by publishing the cross-certificate from the FCPCAG2 to the FBCAG4 and removing the cross-certificates between the FBCAG4 and the old FCPCA.
- **May 2021**, the FPKIMA team will decommission the old FCPCA

What should I do?

To prevent issues, agencies **must** distribute the FCPCAG2 root certificate as a trusted root CA to workstations and servers.

To prepare for the FCPCA update, read the playbook here.

Who can I contact for help or more information?

Email us at fpkirootupdate@gsa.gov.

The FPKIMA is collaborating with Cybersecurity and Infrastructure Security Agency (CISA) on a series of webinars to communicate the upcoming changes and answer questions. Email fpkirootupdate@gsa.gov to join our next webinar on **January 28, 2021 at 11:00 a.m. ET**.

GSA ICAM Solutions Catalog

May 21, 2019, the Office of Management and Budget (OMB) released a new Identity, Credential and Access Management (ICAM) policy (M-19-17) which mandated that GSA publish "a consolidated catalog of existing ICAM solutions and shared services." This catalog includes ICAM solutions that can be purchased on GSA eBuy. The GSA ICAM Solutions Catalog can be found here. Additional solutions and shared services have also been included such as login.gov and max.gov.

Enterprise Single Sign On Playbook

The Playbook is designed to help agencies implement Enterprise Single Sign On (SSO) to improve service delivery efficiency and leverage federated solutions.

The draft is in a comment/review period with a publication goal of January 29, 2021.

NIST Special Publication 800-207 - Zero Trust Architecture

Published on 8/11/2020. The publication will help with the future needs of Non-Person Entity (NPE) certificate requirements. The document gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

https://csrc.nist.gov/publications/detail/sp/800-207/final

Explore the IT Security Hallway yet?

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. Sign up at https://hallways.cap.gsa.gov/

FIPS 201-3 Draft and Workshop

A draft of FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors was published 11/2/2020 with comments due on 2/1/2021. The draft revision proposes changes to FIPS 201-2, including: expanding specification on the use of additional PIV credentials known as derived PIV credentials, procedures for supervised remote identity proofing, the use of federation as a means for a relying system to interoperate with PIV credentials issued by other agencies, alignment with the current practice/policy of the Federal Government, and specific changes requested by Federal agencies and implementers.

FIPS 201-3 Workshop: A public virtual workshop was held on December 9, 2020 to present Draft FIPS 201-3. The workshop provided a broad overview of public draft FIPS 201-3 – focusing specifically on the new/updated features introduced in the draft standard. Topics include 1) PIV identity proofing and enrollment, 2) PIV card updates and associated authentication mechanisms 3) expansion of PIV credentials/authenticators in the form of Derived PIV credentials, and 4) PIV federation as a means for interagency interoperability. Federal Agencies and industry representatives were invited to the virtual event on the Draft FIPS 201-3.

The workshop was recorded, in case you missed a segment. Visit the Draft FIPS 201-3 Virtual Workshop Event page to view the recordings and access additional workshop proceedings/resources - including slides (zip file or individual presentations under the Agenda heading) and the Q&A transcript.

NIST SP800-53 Rev 5 Published

NIST SP 800-53, Revision 5 - Security and Privacy Controls for Information Systems and Organizations was published on 9/23/2020 and subsequently updated on 12/10/2020. It's been seven years since the last major update to NIST 800-53. This update will provide a solid foundation for protecting organizations and systems - including the personal privacy of individuals - well into the 21st century.

NIST SP 800-53, Revision 5 is not just a minor update but rather a complete renovation—addressing both structural issues and technical content. The update represents a multi-year effort to develop the first comprehensive catalog of security and privacy controls that can be used to manage risk for organizations of any sector and size, and all types of systems - from super computers to industrial control systems to Internet of Things (IoT) devices. The controls offer a proactive and systematic approach to ensuring that critical systems, components, and services are sufficiently trustworthy and have the necessary resilience to defend the economic and national security interests of the United States.

An update of the **FPKI 800-53 Security Controls Overlay** is in the process of final review and adjudication of comments. Once completed, the FPKI Policy Authority (FPKIPA) will apply for NIST Security Control Overlay Repository (SCOR) inclusion in the NIST library.

Federal PKI Working Group Updates

The **Certificate Policy Working Group (CPWG)** Audit and Archive Work team met throughout the quarter to make progress on potential changes to existing audit and archive policy requirements. The next steps include;

1) Participants to provide feedback on existing audit and archive policy requirements (by mid-January)
2) Work Team will adjudicate feedback by applying qualifying criteria (February)

The FPKI Technical Working Group (TWG) 2021 Meeting Schedule
In 2021, the TWG will resume quarterly meetings. Our first 2021 TWG that will be held on February 3rd will have Microsoft answering questions received through our recent survey.

Do you have a topic that you would like to be addressed during an upcoming TWG? Please send any topics or questions to fpki-help@gsa.gov.

Add these dates to your calendars and lookout for meeting specifics as it gets closer to the date of each meeting. Meetings will be held on a quarterly basis.

1) February 3rd at 1:00 p.m. to 3:00 p.m.
2) May 4th at 10:00 a.m. to 11:30 a.m.
3) August 3rd at 10:00 a.m. to 11:30 a.m.
4) November 2nd at 10:00 a.m. to 11:30 a.m.

Participation in Federal PKI working groups is limited to Federal employees, contractors, and invited guests.

Ask the FPKIMA

Can I be notified of new certificate issuances or other system notifications?

Yes! System notifications including; changes to Certificate Revocation List Distribution Points (CDP) and Online Certificate Status Protocol (OCSP) endpoints, new or retiring URIs, and signing or revoking a CA certificate are posted to the FPKI Guides System Notification page at https://fpki.idmanagement.gov/notifications/#notifications.
You can subscribe to system notification and other issues by signing up for a GitHub account and watching the FPKI guide repository at https://github.com/GSA/fpki-guides.

Where Can I Find More Information about the FPKIMA?

For more Information about the the FPKIMA, go to https://www.idmanagement.gov/fpkima/ or the FPKI Guide website at https://fpki.idmanagement.gov/.

Need Help?

Certificate doesn't validate? Unsure which certificate to use?

ASK THE FPKIMA

fpki-help@gsa.gov

Do you send digitally signed email and documents? Let us know!

The FPKIMA is currently updating our PKI use cases. One use case involves sending digitally signed emails or documents outside of the government to mission partners including U.S. or international business partners, foreign governments, or citizens. Please let us know if your agency uses a PIV card or other FPKI certificate to perform any of these actions. Send your feedback to fpki-help@gsa.gov to ensure this capability is sustained in any future enhancements.