FPKIMA Newsletter

Spring 2021 | Volume 7, Issue 2

Federal PKI Management Authority
Enabling Trust

Inside This Issue

New Playbook Site

The new site for Federal Identity, Credential, and Access Management (FICAM) Playbooks is now live. This is consolidating all existing FICAM and Federal Public Key Infrastructure (FPKI) playbooks to this new page to help you find answers and content faster. Please bookmark this URL for future reference. https://playbooks.idmanagement.gov/

Federal Common Policy CA Update

In **October 2020**, the Federal Government created a new FPKI root certification authority (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

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 to FCPCAG2 update, read the playbook here.

The intermediate CAs with certificates issued by the current FCPCA were issued new certificates by the new FCPCAG2 to support the migration to the new Federal Public Key Infrastructure (FPKI) trust anchor. Depending on agency configurations, you might need to distribute these certificates to systems and applications. We recommend also distributing the new intermediate certificates issued by the FCPCG2; more information can be found on this page.

Who can I contact for help or more information?
Contact the FPKIMA to answer your questions. Email fpkirootupdate@gsa.gov.

NIST Test PIV Cards V2

NIST published the NISTIR 8347 NIST Test Personal Identity Verification (PIV) Cards Version 2 on 4/2/2021. In order to facilitate the development of applications and middleware that support new PIV cards, NIST developed a set of test PIV cards and a supporting PKI. This set of test cards includes not only examples that are similar to cards issued today but also examples of cards with features that are expected to appear in cards that will be issued in the future. This document provides an overview of the test cards, the infrastructure that has been developed to support their use, and detailed specifications for each test card and for each certificate issued by the test PKI.

Adobe Approved Trust List

The FCPCAG2 has now been added to the Adobe Approved Trust List (AATL). What is the AATL? It is a program that allows millions of users around the world to create digital signatures that are trusted whenever the signed document is opened in Adobe Acrobat or Acrobat Reader software. Essentially, both Acrobat and Reader have been programmed to reach out to a web page to periodically download a list of trusted "root" digital certificates. Any digital signature created with a credential that can trace a relationship ("chain") back to the high-assurance, trustworthy certificates on this list is trusted by Acrobat and Reader.

Why is this feature important? When you receive a digitally signed document, both Reader and Acrobat ask three key questions to validate the signature:

1. Is the digital certificate that signed the document still valid? Has it expired or been revoked?
2. Has the document been changed since it was signed? Has the integrity of the document been affected? If there are changes, are they allowed changes or not?
3. Finally, does this certificate chain up to a certificate listed in the Trusted Identity list? If so, the signature will be trusted automatically.

The answers to the first two questions are handled by Acrobat and Reader based on an analysis of the information contained within the certificate and the signed document itself. However, it's the answer to the third question that has always posed a challenge to the electronic signatures marketplace. How do you know if you can trust a digital signature? What aspects of the signer's digital certificate/credential should be noted? How important is verifying the signer's identity, and how critical is the storage of the signing key itself?

Adobe understands that the relying party must be free to make its own trust decisions based on its unique circumstances. However, Adobe AATL is a way to help relying parties make this determination and in so doing make the process of using digital signatures that much easier.

Note: The FPKIMA is aware of a current issue with how Adobe products handle self-issued certificates in a certificate path, so it is possible they may show an issue with certificates issued prior to the August 2019 re-key of Entrust-issued certificates.

Ontology for Authentication

NISTIR 8344 Ontology for Authentication. This is an effort to define authentication by examining mechanisms used to prove position or membership; analyzing existing methods, tools, and techniques; and developing an abstract representation of authentication features and services. The need for strong authentication continues to increase. To understand the intricacies of what authentication means the establishment of a set of concepts and categories in a subject area or domain that shows their properties and the relations between them and authentication can better manage the requirements placed upon both systems and users. This document includes a survey of authentication mechanisms, establishing the need and basis for authentication metrology, as well as key factors in determining strength and management requirements when assessing an authentication system suitable for the associated risks in a given environment.

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.

Publication was completed in February 2021.

https://playbooks.idmanagement.gov/docs/playbook-sso.pdf

Request for Topics

Do you have a topic or a question that you would like to be covered in an upcoming newsletter? Please send any topics or questions to fpki-help@gsa.gov.

SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST 800-171

This publication provides federal agencies with recommended enhanced security requirements for protecting the confidentiality of CUI.

Digital Worker Identity Playbook

The Playbook is a practical guide to manage digital worker identities.

Publication was completed in January 2021.

https://playbooks.idmanagement.gov/docs/playbook-digital-worker.pdf

Recent TLS Articles of Note

Nearly half of malware now use TLS to conceal communications

As more of the Internet uses Transport Layer Security (TLS), analysis of detection telemetry shows the volume of TLS encrypted communications by malware has doubled in a year.

While HTTPS helps prevent eavesdropping, man-in-the-middle attacks, and hijackers who try to impersonate a trusted website, the protocol has also offered cover for cyber criminals to privately share information between a website and a command and control server – hidden from the view of malware hunters.

"It should come as no surprise, then, that malware operators have also been adopting TLS ... to prevent defenders from detecting and stopping deployment of malware and theft of data," said the Sophos group.

Malware communications fall into three main categories: downloading more malware, exfiltration of stolen data, or command and control. All these types of communications can take advantage of TLS encryption to evade detection by defenders, the security company said.

According to Sophos, a year ago 24% of malware was using TLS to communicate but today that proportion has risen to 46%. Sophos said a large portion of the growth in overall TLS use by malware can be linked in part to the increased use of legitimate web and cloud services protected by TLS as unwitting storage for malware components, as destinations for stolen data, or even to send commands to botnets and other malware.

NSA Urges System Administrators to Replace Obsolete TLS Protocols

The National Security Agency (NSA) is lighting a fire under system administrators who are dragging their feet to replace insecure and outdated TLS protocol instances.

The agency recently released new guidance and tools to equip companies to update from obsolete older versions of TLS (TLS 1.0 and TLS 1.1) to newer versions of the protocol (TLS 1.2 or TLS 1.3).

TLS (as well as its precursor, Secure Sockets Layer or SSL) was developed as a protocol aimed to provide a private, secure channel between servers and clients to communicate. However, various new attacks against TLS and the algorithms it uses have been revealed – from Heartbleed to POODLE – rendering the older versions of the protocol insecure.

You can read more about the NSA cybersecurity program here or go directly to the document here.

Addressing Visibility Challenges with TLS 1.3

Addressing Visibility Challenges with TLS 1.3 White Paper was published on 2/24/2021 and comments closed on 3/29/2021. NIST recognizes the challenges associated with compliance, operations, and security when enterprises employ encrypted protocols, in particular TLS 1.3, in their data centers. This project will use commercially available technologies to demonstrate a range of approaches for enabling necessary intra-enterprise access to unencrypted/decrypted information.

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 FPKI Technical Working Group (TWG) 2021 Meeting Schedule
In 2021, the TWG will resume quarterly meetings. The first 2021 TWG that was held on February 3rd with Microsoft answering questions received through the FPKIMA recent survey. During and following the meeting additional questions along with example CAPI logs were received from members. The upcoming meeting will have Microsoft answering those additional questions.

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) May 4th at 1:30 p.m. to 3:00 p.m.
2) August 3rd at 10:00 a.m. to 11:30 a.m. (times are subject to change)
3) November 2nd at 10:00 a.m. to 11:30 a.m. (times are subject to change)

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://playbooks.idmanagement.gov/fpki/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/ficam-playbooks.

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://playbooks.idmanagement.gov/fpki/.

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.