FPKIMA Newsletter

Spring 2018
Volume 5 Issue 3

Federal PKI
Management Authority
Enabling Trust

Inside This Issue

Office of Federal CIO Public Working Space

The Federal CIO Council has a public working space at https://policy.cio.gov. Anyone can view draft, final, archived, and other resources. For example, the new draft Identity Policy is currently available for comment or you can view an archived collaborative project on a new policy schema. Check out the public working space, leave a comment or idea, and follow the ongoing discussion of IT policy development in the Federal Government!

OMB Identity Policy

The Office of Management and Budget (OMB) in coordination with the Federal CIO Council published a new draft Identity Policy. The new "*Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management*" offers many improvements and continued direction in securing federal systems. While still a draft policy and many elements could change, the policy is written in three sections:

1) Implementation of effective Identity, Credential and Access Management (ICAM) governance
2) Modernization of agency ICAM and capabilities
3) Agency adoption of ICAM shared solutions and services

In addition to the above three areas, it also expands on government-wide ICAM responsibilities, rescinds previous OMB Identity Policies, and updates requirements on multi-factor authentication, encryption, digital signature, acquisition, recognition, and interoperability.

Implementation of Effective ICAM Governance

This section focuses on effective ICAM Governance and the continued implementation of a cross-section ICAM office or team comprised of representatives from around an agency. Representatives should include IT, security, human resources, general counsel, privacy, and component organizations. In addition to incorporating NIST 800-63-3 processes, the policy aims to align and incorporate agency ICAM capabilities with both Enterprise Risk Management (ERM) and the Continuous Diagnostics and Mitigation (CDM) program.

Modernization of Agency ICAM and Capabilities

To improve modernization, agencies shall reduce overlapping and redundant solutions while promoting interoperability of existing and future solutions through Application Programming Interfaces (API).

Agency Adoption of ICAM Shared Solutions and Services

Federal-wide shared services provide the most cost-effective solutions for the government. This section includes support for federal identity shared services and aligning identity assurance and authentication for consumers and mission partners with NIST 800-63-3.

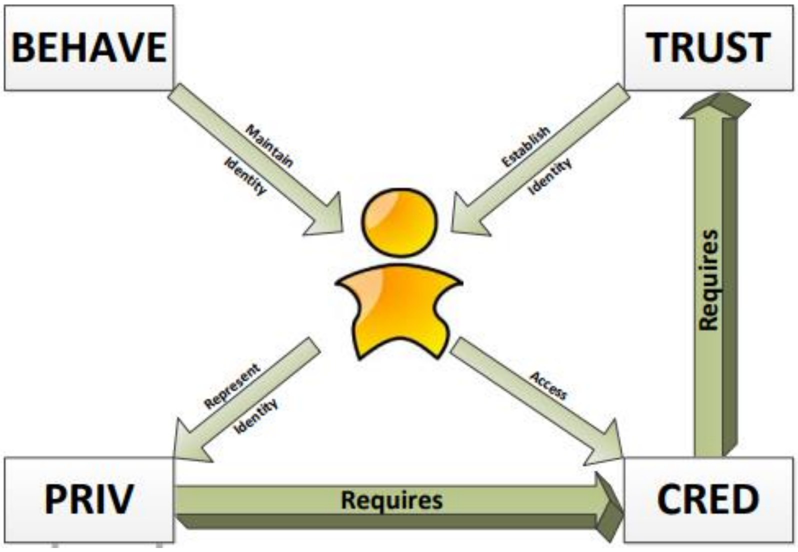
This is a draft policy and subject to change but gives an indication of the evolving federal identity landscape. This draft policy also rescinds former key pieces of identity policy such as M-04-04 "*eAuth Guidance for Federal Agencies,*" M-05-05 "*Electronic Signatures,*" M-06-18 "*Acquisition of HSPD-12 Products,*" M-11-11 "*Continued Implementation of HSPD-12,*" and "*Requirements for External Identity Credentials,*" The draft Policy is available at https://policy.cio.gov/identity-draft/ with a discussion forum is available at https://github.com/ombegov/policy-v2/labels/identitydraft.

Federal PKI and CDM Compliance

How FPKI Credentials Fit in the CDM Program

Continuous Diagnostic and Mitigation (CDM) is a federal-wide program providing adequate, risk-based, and cost-effective network monitoring and access control solutions. The overarching goal, like identity management, is to ensure the right things (people and devices) have the right access at the right time. The CDM Program treats the government as one enterprise with the Department of Homeland Security (DHS) Network Operations Center providing network monitoring and remediation. CDM implementation is divided into three phases:

1) Manage the assets (What is on the network)
2) Manage people and services (Who is on the network)
3) Manage events (What is happening on the network)



Trust, Behave, Cred, and Priv Linkage to the User (Image courtesy of DHS)

Where Does the FPKI Fit into CDM?

CDM phase 2 includes managing things (people and devices) on your network. The phase 2 security capabilities include:

1) **Trust** - Helps agencies verify fitness determination before granting access.
2) **Behave** - Locks accounts for users who do not complete or pass awareness, role, and accept rules of behavior.
3) **Credential** (CRED) - An issued credential is properly bound and valid before granting physical or logical access to federal assets.
4) **Privilege** (PRIV) - Credential privileges are reviewed and corrected on a reoccurring basis.

The FPKI fits with the TRUST, CRED, and PRIV security capabilities. For people, all PIV cards require a background investigation (TRUST) and follow federal policy for strongly binding the user to the credential. For devices, agencies must verify they control the device or domain before issuing a device certificate. Need help implementing FPKI or PIV credentials to meet CDM requirements? See the FPKI Guides page or PIV Usage Guides page on how to configure and use the FPKI.

Are You Following the Latest Microsoft Update?

The Federal PKI may limit or remove Federal Common Policy from the Microsoft Root Store Program. Follow the latest developments https://fpki.idmanagement.gov/announcements/mspkichanges/.

Explore the IT Security Hallway yet?

The GSA Acquisition Hallway aims to help federal acquisition officials 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. Sign up at https://hallways.cap.gsa.gov/

GSA Access Certificates for Electronic Services (ACES) Sunset!

The GSA ACES Program was the first federally operated PKI program designed specifically for secure government transactions. The Federal Bridge Non-Federal Issuer (NFI) program has matured to the point where a federally-operated program for business partners is no longer needed. For more information on the ACES Sunset, contact the ACES Program at GSA-ACES@GSA.gov or review ACES Transition FAQs in the ACES Sunset Guide.

The FPKI Graph has a New Home on the FPKI Guides Web Page!

The FPKI Graph, a useful tool to navigate the FPKI, is moving to the Useful Tools section of the FPKI Guides web page. The Graph displays the relationships between Certification Authorities in the Federal PKI ecosystem. It is a great tool to see the trust relationships and understand the structure of the FPKI ecosystem. Check out the new home of the FPKI Graph!

Federal PKI and FAR Compliance

How to Use FPKI for NIST 800-171 Compliance

NIST 800-171 "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organization*" is one of the latest policies for protecting the federal government supply chain. It is a tailored version of 800-53 that specifically addresses confidentiality controls for non-federal systems.

Why is there a NIST Policy on Non-Federal Systems?

Over the last couple of years, many federal incident post mortems found the leak of government information was not due to federal systems, but business or mission partner systems. The solution was to integrate non-federal system security into acquisition law and the NIST 800-171 standard was created as a result. It requires any organization (profit or non-profit) that receives, or stores government controlled unclassified information to show compliance with NIST 800-171. The data must be marked properly which is defined in Executive Order 13556 . NIST 800-171 compliance is already codified in the Defense Federal Acquisition Regulation Supplement (DFARS) and will soon be included in the Federal Acquisition Regulations (FAR). Until the FAR reference is released, civilian agencies may directly require 800-171 compliance. At a high level, non-federal systems must undergo an initial and ongoing assessments, documenting control implementations in a System Security Plan (SSP), and then create a Plan of Action & Milestones (POA&M) to address remediation. Templates are available for both the SSP and POA&M on the NIST 800-171 Revision 1 website as well as a mapping between NIST 800-171 and the NIST Cybersecurity Framework.

How Does the Federal PKI Fit In?

Non-federal entities may use Non-Federal Issuer (NFI) credentials to meet NIST 800-171 compliance. The NFI program under the Federal Bridge was designed for business and mission partner collaboration with the federal government. It allows private companies and communities of interest to use commercially available credentials that meet strict federal security guidelines when interacting with the government. Use of NFI credentials, which include PIV-I, can be used to support the reporting requirements to the government. While NIST 800-171 focuses on confidentiality of information, it also aims to ensure information is properly stored and transmitted.

Which NIST 800-171 Controls Can I Meet using the Federal PKI?

One of the new requirements in NIST 800-171 is multi-factor authentication to privileged accounts and network access to non-privileged accounts. NFI credentials meet the multi-factor authentication requirements in both hardware (PIV-I) and software credential formats. In addition, NFI credentials may also meet the following control family requirements:

- System & Communication Protection (SC)
- Identification & Authentication (IA)
- Physical & Environmental Protection (PE)

For more information on NFI credentials, go to the NFI Business Identity and Credentials section on idmanagement.gov.

FPKI Working Group Updates

The Certificate Policy Working Group met in March 2018 to discuss the following topics:

1) **Nine Year Identity Refresh Policy -** The group discussed removing the nine-year identity refresh requirement because in-person proofing for PIV is already conducted every six years when PIV cards expire.
2) **Federal PKI Public Trust Impact and Path Forward** - Several Microsoft, Google, and Apple updates will impact how the Federal PKI is distributed in applications. Google is enforcing certificate transparency, multiple applications are distrusting Symantec authorities, and Microsoft is implementing a technical constraint on government-operated PKIs. For more information on the latest developments of Public Trust impact, see the FPKI's Announcements page.

The FPKI Technical Working Group met in April 2018 to discuss the following topics:

1) Federal PKI Trust Strategy
2) Public Trust Challenges
3) Synopsis of GSA ICAM Day 2018 and CAB Forum F2F
4) PKI Subject Alternative Name (SAN) Attack Vector and Mitigation

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

Ask the FPKIMA

How Do I Check a Digital Signature in Adobe?

Adobe is one of the few programs that perform certificate policy validation as part of a digital signature check. Only certain types of FPKI certificates validate as trusted in Adobe. Those certificates include PIV, PIV-I, CAC, and other hardware-based credentials. To view which policies are trusted locally follow these steps:

1) Open Adobe Acrobat.
2) Select **Edit > Preferences > Signatures > Identities & Trusted Certificates**.
3) Choose **Trusted Certificates** from the left-hand sidebar.
4) Choose **Federal Common Policy CA**, then the **Certificate Details** tab.
5) Choose **Certificate Viewer** window and click on the **Policies** tab.
6) In Certificate Policies, you will see a comma-separated list of policy Object Identifiers (OIDs).

For more information on Adobe settings, see the FPKI Guide's Trust Store page.

Where Can I Find More Information on the FPKIMA?

Information is found at https://www.idmanagement.gov/fpkima/

Federal PKI Management Authority
Enabling Trust

Need Help?

Can't figure out why your certificate is not validating?

Contact the FPKI!
FPKI@GSA.gov

DHS Binding Operational Directives are Online!

DHS has publicly posted Binding Operational Directives (BOD) including BOD 18-01. The repository can be found at http://cyber.dhs.gov/bod

Are You Following the Latest Apple Updates?

The Federal PKI has requested removal of Federal Common Policy from the Apple Root Store Program. Stay tuned for an announcement or email FPKI@gsa.gov for more details. Follow the latest developments at https://fpki.idmanagement.gov