FPKIMA Newsletter

Volume 6, Issue 3 | Fall 2019

Federal PKI
Management Authority
Enabling Trust

Inside This Issue

FICAM PACS Playbook!

This Physical Access Control System (PACS) Guide will help you understand concepts related to Federal Identity, Credential, and Access Management-compliant PACSs. At a high level, a PACS is a collection of technologies that control physical access at one or more federal agency sites by electronically authenticating employees, contractors, and visitors. This informative guide can assist agencies in planning a PACS install or upgrade. For more information, go to https://go.usa.gov/xVem

New Federal Identity Guidance

OMB Memo 19-17 Charts a Renewed Course

The Office of Management and Budget (OMB) finalized its long awaited identity policy update on May 21st. This final memo has some minor changes from the last draft and charts a renewed course for federal identity management in 2020 and beyond.

Contextualizing Identity in the Federal Government

Identities are defined as either a (1) Federal enterprise identity or a (2) public identity. The main difference between the two is a Federal agency manages one of them, the Federal enterprise identity.

Managing Identities, Credentials, and Access in Modern Government

Through this Federal ICAM policy, the Government is continuing a common vision for identity as an enabler of mission delivery, trust, and safety of the Nation. Agencies must be able to identify, credential, monitor, and manage subjects that access Federal resources, including information, information systems, facilities, and secured areas across their respective enterprises.

Adapting the Government's Approach to HSPD-12

HSPD-12 and FIPS 201 continue to form the basis for a Government-wide policy for standards-based, secure, and reliable forms of common, Government-issued identification. Different authenticators that meet the intent of HSPD-12 can be piloted. Agencies should support PIV identity assertions from other agencies as well as support use of PIV-based encryption and require use of PIV-based digital signatures.

Shifting the Operating Model Beyond the Perimeter

To ignite adoption of using identity as the underpinning for managing risk around ICAM capability deployment, each agency must harmonize its enterprise-wide approach to governance, architecture, and acquisition. Each agency shall designate an integrated ICAM office or team to support Enterprise Risk Management as well as write a single ICAM policy. Agencies shall also establish authoritative identity services and sources.

Improving Digital Interactions with the American People

The focus here is on leveraging existing and compliant Federal or commercially operated shared services that align with NIST and ICAM requirements such as Login.gov.

In addition to the specific guidance, a number of previous OMB memos were rescinded including M-04-04 - eAuth for Federal Agencies, M-05-05 - Electronic Signatures, and M-11-11 - Continued Implementation of HSPD-12. Go to ***https://go.usa.gov/xVePk*** to read OMB M-19-17.

Don’t Reinvent the Wheel

Best Practices in ICAM Governance

Identity Management is a cross-functional area. It requires experience in leveraging Human Resource records to implement network or physical controls on applications or buildings. An enterprise-wide approach to identity governance is necessary to ensure using identity as the underpinning for managing risk is successful. The OMB Identity Policy M-19-17 identifies identity governance as a critical area. Agencies do not need to reinvent the wheel when building or updating their ICAM governance structure. Whether it is a program office, an office, a team, or something else, all share similar characteristics for success;

1. **Align Priorities and Budget of Stakeholders** - This is a critical step in any project, Specific to identity management, common stakeholders include IT, human resources, physical security, privacy, acquisitions, and potentially many others. Each has their own priorities and budgets, but to be successful they must be aligned toward a common Identity goal.

2. **Integration with Enterprise Risk Management** - Enterprise Risk Management or ERM is defined as *a common understanding for recognizing and describing potential risks that can impact an agency’s mission and the delivery of services to the public* (OMB M-17-25). With agencies shifting mindsets away from a perimeter-based risk model and using identity as the underpinning for managing risk, integration with the agency’s ERM strategy is a key component.

3. **Executive Support -** There is no greater ally than executive support to ensure ICAM policies, processes, and technologies are being coordinated among agency leaders and mission owners. Identity goals should be identified to facilitate realizing business, cost, risk management, and operational efficiency benefits. This may include:
   a. Reducing maintenance and development cost through identity federation.
   b. Digitizing processes with electronic or digital signatures.
   c. Reducing risk through strong authentication mechanisms on desktop and mobile devices.
   d. Reduce risk of data compromise through data encryption tied to device identities.

4. **Teamwork** - A top down approach is an effective show of support, but it should also be reinforced at the implementation level. Identity is a cross-functional domain that requires equal parts information technology (IT), human resources (HR), physical security, and privacy to ensure the right identity is used to access the right information at the right time in a privacy-enhanced manner.

Building a strong foundation for an agency identity governance program can be accomplished by aligning priorities and budgets, integration with ERM, executive support and teamwork. For more guidance, go to the ICAM subcommittee page on Max.gov at ***https://go.usa.gov/xVey3***.

NIST NCCoE Mobile Single Sign-On Project

The NCCOE project features the use of non-PIV authenticators to efficiently and securely gain access to mission data via mobile devices and applications. Go to https://go.usa.gov/xVeEr for more info on multifactor authentication and mobile single sign-on.

Explore the IT Security Hallway yet?

The GSA Acquisition Gateway 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/

What Happened to M-04-04?

OMB Memo 04-04 E-Authentication Guidance for Federal Agencies was a foundation memo establishing four identity authentication assurance levels for e-government transactions. NIST drafted the original 800-63-1 based on those levels. The newest NIST 800-63-3 reduced the number of levels to three and also separated identity, assurance, and federation categories. To ensure alignment with the newest NIST standard, OMB rescinded M-04-04.

Have you noticed idmanagement.gov lately?

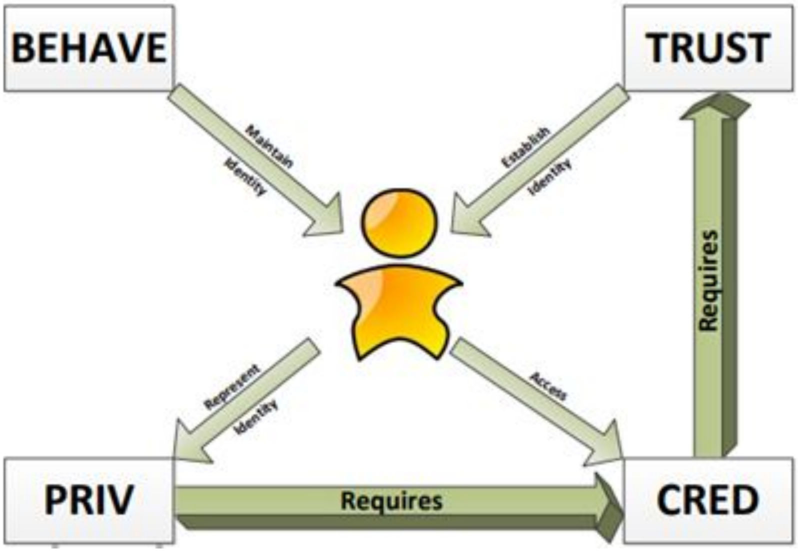
Your one stop shop for all things federal identity management is idmanagement.gov. It has guidance for teams to design and build functional and secure identity systems, GSA identity products and services, how to manage identity systems, and an identity topics and community section. The playbooks section feature specific guidance on the Federal PKI, PIV, Architecture, and now PACS. Something missing? Send questions to comments to FPKI@gsa.gov

Aligning Investment

Leveraging Federal PKI Credentials for DHS CDM

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 Federal PKI 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. **CRED** - An issued credential is properly bound and valid before granting physical or logical access to federal assets.
4. **PRIV** - Credential privileges are reviewed and corrected on a recurring 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 Playbook*** page or ***PIV Usage Playbook*** page on how to configure and use the FPKI.

Federal PKI Working Group Updates

The Certificate Policy Working Group (CPWG) met in September 2019 to discuss the following topics:

1) **Common Policy Update** - The FPKIPA support team completed a section-by-section review of the Common Policy and are preparing change proposals for CPWG review.
2) **Authorization Data Attributes in Certificates** - Authorizations are currently allowed in a certificate, but it is unclear if they are actually used. Provide feedback on if and how they are used.
3) **Federal Subscriber Certificate Naming** - Review of 2018 audit certificate samples found agencies applying a policy deviation. The policy will be updated to standardize use and remove edge use cases.
4) **Change Proposal Update** - There are two change proposals waiting to be finalized by the sponsors after CPWG review.

The FPKI Technical Working Group (TWG) met in September 2019 to discuss the following topics:

1) **Validation Data Analysis Results** - GSA is examining chaining and revocation data provided by FPKI partners to help inform an appropriate timeline to remove Federal Common Policy from the Microsoft Root Program.
2) **Federal Common Policy Rekey Alternatives** - The GSA FPKIMA presented an analysis of Federal Common Policy Rekey alternatives to maintain a public trust infrastructure.

Participation in Federal PKI working groups is limited to Federal employees, contractors, and invited guests. Please send any questions to ***FPKI@GSA.gov***.

Ask the FPKIMA

Is there a list of Federally Approved Identity Providers?

No. There are approved credential providers (https://www.idmanagement.gov/want-to/buy/), but the onus is on the agency to set up credential use within their agency. For cloud-based applications, this is usually done through federation with the agency's existing authentication mechanism which is also outlined in the FedRamp requirements. While there isn't a list of Federally approved Identity Providers, there are two federally-operated services which agencies can leverage for authentication. Login.gov and Max.gov are both authentication providers that can leverage CAC/PIV for cross-agency access to federally-operated websites and web services.

Where Can I Find More Information?

Information is found on the FPKIMA at ***https://www.idmanagement.gov/fpkima/*** or on the FPKI Guide website at ***https://fpki.idmanagement.gov/***.

Federal PKI
Management Authority
Enabling Trust

Need Help?

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

ASK THE FPKI!

FPKI@GSA.gov

Derived PIV Reference Architecture

The NIST NCCOE finalized special publication 1800-12, Derived PIV Credentials project. The NCCoE at NIST built two security architectures by using commercial technology to enable Derived PIV Credential issuance to mobile devices that use a PIV shared services provider. One option uses a software-only solution while the other leverages hardware built into many computing devices used today. This project resulted in a freely available NIST Cybersecurity Practice Guide on mobile device multifactor authentication leveraging PIV standard strengths credentials.

https://go.usa.gov/xVeyr