NEWSLETTER

Federal PKI Management Authority
Enabling Trust

Winter 2023

NIST Revised Guidelines for Digital Identification in Federal Systems

On December 16, 2022 NIST released draft updated guidelines for digital identification in federal system. The guidelines support risk-informed management of people's personas online. The last major revision was in June of 2017.

Digital Identity Guidelines (NIST SP 800-63 Revision 4) covers technical requirements for establishing and authenticating digital representations of real-life people. The guidelines are geared mainly for external users—members of the public, or employees of a government contractor. The draft guidelines aim to help organizations manage risks associated with digital interactions while making it easier for individuals to use digital identities successfully, including when applying for government services. They include privacy requirements and offer considerations for fostering equity and the usability of digital identity solutions, as well as their supporting technologies and processes, placing the risks faced by individuals accessing services alongside risks to the organizations that operate those services.

Comments on this draft publication are due by March 24, 2023. To submit comments, download the comments template and email the completed form to dig-comments@nist.gov

On January 10, 2023, NIST also released two draft Guidelines on Personal Identity Verification (PIV) Credentials. Comments on these are also due by March 24, 2023. These complement SP 800-63-4 by providing guidance on identity management of government employees and their direct contract support.

SP 1800-157r1 has been revised to feature an expanded set of derived PIV credentials to include public key infrastructure (PKI) and non-PKI-based phishing-resistant multi-factor authenticators. SP 800-217 essentially profiles 800-63c for use with PIV.

In this Issue

NEWSLETTER

Federal PKI Management Authority
Enabling Trust

Winter 2023

PACS and Mobile Credentials

On January 24, 2023, the GSA ICAM team hosted a Physical Access Control System (PACS) Industry Information Exchange Day in conjunction with the Schedules Program. Of particular interest was the Mobile Credential Roundtable hosted by USAccess. Leading experts for the industry discussed the current state of PACS in the mobile space and what may be the next steps in advancing and better utilizing these technologies in the government space.

Areas of policy that should be examined:

- Should be equal usage and support of PIV for PACS and LACS
- Properly configured PACS is an issue, like LACS was before the 2015 CyberSprint following the OPM data breach
- NIST SP 800-63 rev4 does not address PACS. PACS community relies on SP 800-116 and FIPS 201 itself.
- PACS can't adapt to new credentials like LACS. Need to work with interfaces already supported by reader.
- Range on Bluetooth for PACS should be examined by APL lab
- Customer demand for mobile credentials is present

What can government do to facilitate PACS and PIV?

- Most of the work with PACS vendors has been ad hoc and scattered. Regular cadence between stakeholders, setting a schedule to do testing with multiple iterations would lead to success.
- Improved enforcement of existing policy
- Additional promotion of successful implementation
- Finalize standards
- FIDO's flexibility creates an opportunity. SP 800-157 suggests many derived credentials could be available for different purposes

TWG/ICAMSC TEM Meetings

The Combined TWG/ICAMSC TEM meeting will occur on the following:

- February 21, 2023
- June 20, 2023

Digital Autopen Update

The Identity, Credential, and Access Management Subcommittee collected final comments on new guidance for a digital autopen. The Digital Autopen for Federal Register Documents playbook outlines an agency process to use a role-based certificate to digitally sign and submit documents to the Office of the Federal Register for publication.

NEWSLETTER

Federal PKI Management Authority
Enabling Trust

Winter 2023

Developments in Digital Wallets

Mobile devices are quickly becoming a popular option for users looking to interface with digital or in-person services – a trend accelerated by the Covid-19 pandemic.

Digital Identity in the Electronic Wallet Era
In November, the Secure Identity Alliance released a whitepaper highlighting the use cases driving wallet adoption. The report highlights the need for governments and other service providers to pay close attention to how they adapt current digital ID systems when integrating e-wallets for both government and commercial use. Interoperability and standards in digital identity are rising in importance in both public and private ID schemes.

The Alliance emphasizes that governments are now looking beyond national digital identity programs expanding most notably into areas of interoperability with other countries. As e-wallets expand, user's security and usability expectations will increase, expecting technologies that make it possible to have trusted, fluid and personalized services without compromising their digital identities or privacy.

The growth of e-wallets and digital IDs is also inspiring the development of new international standards, protocols and data models including ISO 18013, ICAO DTC, Verifiable Credentials and DIDS which stakeholders will need to bear in mind when planning their digital ID programs

Various models are now being established: centralized data models continue to develop in many parts of the world, and hybrid models are also emerging as centralized public sector wallets and ID begin to interface with private federated models of management. Decentralized models where users manage their own identity are also being considered.

The growing technical complexity of the digital identity environment means governments should look to build technical governance and conformity frameworks that assure coordination between technical and policy decision makers.

Download "The Digital ID in the E-Wallet Era" report published by the Secure Identity Alliance here.

FIDO2 Community of Action

FIDO2 Community of Action recently completed its first round of pilot testing.

CoA will publish FICAM Phishing-Resistant Authenticator Playbooks based on working group and community of action findings.

Additionally, a new M-22-09 community of action is being established for network and encrypted DNS.

The group is currently recruiting potential next round of pilot cohorts for 2023. If your agency is interested in participating, contact ICAM@gsa.gov.

For More Info

- FPKI Info and Updates: https://www.idmanagement.gov
- FPKI Help and future topic requests: fpki-help@gsa.gov