NEWSLETTER

Federal PKI
Management Authority
Enabling Trust

Fall 2022

In This Issue:

Post Quantum Planning

On September 21st, the FPKIMA team hosted a Technical Working Group to discuss NIST's upcoming post quantum cryptography guidance and how the FPKI community can begin planning for this cryptographic transition.

NIST presented their latest research on quantum algorithms and the current candidate for inclusion in the upcoming guidance based on the requirements set forth in NISTIR 8412-udp-1. Based on the presented timelines, three lattice based candidate algorithms (Public-Key Encryption/KEMs CRYSTALS–KYBER, Digital Signatures CRYSTALS–Dilithium FALCON SPHINCS+) draft specification will be available for public comment in early 2023. Pending feedback, the first PQC standards will be published in 2024. BIKE, Classic McEliece, HGC & SIKE are still being reviewed as future candidates for Encryption/KEMs in another round of evaluations - if they pass won't be available for another year or more.

As transition to these new algorithms begins NIST will provide further guidance to the FPKI community. The time frame for full transition will vary based on the risk assessment of quantum attacks. NIST predicts these timelines will be several years into the future. NIST's current direction to those looking to begin planning is to start with research into their current environments. Take inventory of your current cryptography, set up data calls, and begin discussing the PQC standards with vendors and stakeholders.

Participants in the Working Group were especially interested in the availability of parameters, object identifiers etc. NIST will not assign these until the specifications are published. They were able to confirm that all new algorithms will require a hash function with the mechanisms for that described in the final standard for each algorithm.

Additional support for transition will be made available through the National Cybersecurity Center of Excellence (NCCoE) Migration to PQC project. To learn more or participate in the Community of Interest contact: applied-crypto-pqc@nist.gov.

Third-party credential self-assessment

Earlier this year, the FPKIMA team organized a working group with the purpose of developing a standardized self-assessment that could be used by both commercial providers and mission partners to assess the technical implementation of third-party credential service providers (CSPs).

This template is intended to assist as part of decision processes for contracting the use of third-party credentials for federation and other use. It will provide a consistent format for input to government entities who may be conducting standardized risk assessments during procurement and purchasing decisions. Moreover, this assessment is designed to expand and clarify gaps in the current CSP evaluation process by expanding upon the Identity and Authenticator (I&A) requirements specified in NIST SP800-63 to include the underlying security of how the systems are operated, that may sign assertions used in federation, or in binding the identity to the authenticator.

After several rounds of discussion and comment from the FPKI community a finalized draft was presented for publication at the Identity, Credential and Access Management Subcommittee (ICAMSC) in October.

For more on this assessment, or to participate in the development of assessor playbooks, contact the FPKIMA team (fpki-help@gsa.gov).

Developments in Digital Identity

Decentralized Identity
At the September ICAMSC meeting Emerging Technology CTR at GSA presented a brief on Decentralized Identity. Decentralized Identity is of interest in the federal space due to:

- There being no reliance on a centralized trust framework. Instead, the trust is distributed.
- Establishes trust between all participating agencies
- Minimizes the need to create multiple federation connections
- Gives the ability to use mobile/digital identity

The Emerging Technology team will be researching best practices to issue a standardized policy to address conflicting regulations that are critical to blockchain technology. For more information on this effort contact ICAM@gsa.gov

International Mutually Recognized Digital Identity
Digital Identities can be used within a country to assist citizens interacting with government services which are moving toward digital platforms. Examples include electronic filing of tax returns; enrollment or eligibility checking for benefits such as Social Security or Medicare; providing identity documents like passports or driver license for travel, or enrollment for school.

Eight countries have formed a working group on digital identity. An initial report from this Digital Government Exchange (DGX) Digital Identity Working Group (DIWG) spells out eleven principles:

- Open
- Transparent
- Reusable
- User-centric
- Inclusive and accessible
- Multilingual
- Secure and private
- Technologically neutral and compatible with data portability
- Administratively simple
- Able to preserve information
- Effective and efficient

GSA to study equity of remote identity proofing tech

The General Services Administration (GSA) is planning to facilitate a research study on the impact different demographic features have on remote identity proofing technologies – like facial recognition.

The agency is requesting public comments before November 21st on whether the collection of this information is necessary, and ways to enhance the quality, utility, and clarity of the information collected.

You can find the full release here

The group was established in 2020, and they have determined that a universal taxonomy for digital identity would help achieve mutual recognition and interoperability of digital identities across borders, which would assist with free-trade agreements.

An example is the European Digital Identity Wallet. Although an EU initiative based on EU standards, it is also aligned with ISO standards. The EU Digital Wallet will be a voluntary program. Individual citizens will be able to opt-in with the ability to decide what data is stored with it, as well as who it is shared with. Member states have been asked to contribute to a common toolbox including technical architectures, standards, and guidelines for best practices. The group hopes to publish a common toolbox in the October 2022 timeframe.

For More Info

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