NEWSLETTER

Federal PKI
Management Authority
Enabling Trust

Spring 2023

FPKI Public TLS Planning

The FPKI MA team has been tasked by the Federal CIO Council with developing a Federal Public Trust TLS PKI. The scope of the U.S. Federal Public Trust TLS PKI includes the Certification Authorities used for issuing and managing Transport Layer Security (TLS) certificates for public facing U.S. Federal Government services.

The scope is limited to:

- Services that resolve at a registered internet sub-domain under the .gov and .mil Top Level Domains
- Services that are accessible on the internet

The current iteration of the TLS development began in June 2022 with CIO Council approving the FPKI Management Authority to operate the issuing authority. After executive level discussion with OMB, the MA has begun planning and design that includes monitoring and integration of the evolving requirements from the CA/Browser Forum on trust store applications and inclusion.

In the first quarter of 2023 the TLS Certificate Policy (CP) draft was circulated for government review and comment. Next the FPKIPA will vote on final approval, after which the CP will be published on idmanagement.gov.

Building on the CP, the FPKIMA Community team is looking to begin gaging interest in a TLS user group beginning in early 2024. The group will help the FPKIMA to communicate with the community and later develop a testing pool of the automated issuance system.

For User Group updates, please contact: fpki-help@gsa.gov

In This Issue

NEWSLETTER

Federal PKI
Management Authority
Enabling Trust

Spring 2023

ICAM Subcommittee Charter Update

The ICAMSC aspires to be the catalyst that enables federal agencies to meet their missions in delivering federal services that are convenient and secure, by reducing friction in using digital identities across the federal government, while continuously enhancing digital identity practices and processes across the federal government.

In order to facilitate this, ICAMSC co-chairs have reorganized and streamlined the committees charter and structure to better serve its members and achieve the objectives of the charter. Beginning in May 2023, the overall ICAM subcommittee will consist of the Federal PKI Policy Authority, Digital Identity Community of Practice (CoP), and new Working Groups that will all report up to a streamlined ICAMSC.

The newly streamlined ICAMSC will hold 1-hour monthly meetings to identify, discuss, and recommend priorities to the Executive Committee. They will be responsible for maintaining and updating the ICAMSC strategy and establishing working groups, tiger teams, task forces, or other temporary bodies. This group will consist of only CFO Act agency representatives designated by the agency CIO/CISA and designated ex officio members.

The Digital Identity Community of Practice (CoP) will be the evolution of the current ICAMSC that the community is familiar with that has been sharing insights and success stories, recommending priorities to the ICAMSC, developing policy and guidance recommendations for the ICAMSC or higher-level bodies. It will be open to anyone with a .gov email.

This reorganization hopes to better align the subcommittee with the charter's goals and Standardize workforce identity system approach for the interoperability and cybersecurity of cross-agency information sharing and user authorization.

For more information contact: icam@gsa.gov

TWG/ICAMSC TEM Meetings

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

- May 16th, 2023 - Special session FPKI architectural discussion | 1:00 – 2:30 pm
- June 20th, 2023 | 1:00 – 2:30 pm

Architecture TWG

The FPKIMA team will be leading a special technical working group on May 16th to discuss various alternatives so the community as a whole can understand possible alternatives to the FPKI landscape, their relative impacts and benefits in order to reach a consensus on any changes that might be beneficial to the community as a whole.

For more information contact: fpki-help@gsa.gov.

CISA Zero Trust Maturity Model Updates

On April 11th, CISA released an update to the Zero Trust Maturity Model (ZTMM), superseding the initial version released in September 2021. The new version of the implementation guidance provides further detail for agencies on how to secure identity, networks, and applications. The latest version of the guidance updates key definitions and metrics for the governmentwide adoption of zero-trust security architecture.

The Maturity Model provides a roadmap for agencies to reference as they transition towards a zero-trust architecture. ZTMM provides a gradient of implementation across five distinct pillars to facilitate federal implementation, allowing agencies to make minor advancements toward optimization over time. The model also represents a variety of implementation levels across the pillars — identity, devices, networks, data, and applications and workloads. Each pillar includes details regarding cross-cutting capabilities: visibility and analytics, automation and orchestration, and governance.

CISA describes its maturity model as “one of many roadmaps” for federal agencies shifting to zero trust architectures, which are intended to prevent unauthorized or dangerous access to government data and services by consistently verifying user credentials when making authorization decisions

CISA encourages governments and the private sector to use ZTMM as a baseline for implementing zero trust architecture. The growing technical complexity of the digital identity environment means governments should look to build technical governance frameworks that assure coordination between technical and policy decision makers.

Digital Autopen Playbook

GSA has finalized the Digital Autopen Playbook. It outlines the process for an agency to implement a Digital Autopen for Federal Register documents. This digital autopen process is utilized when the agency official who signs Federal Register documents is unavailable or unable to sign and authorizes another agency employee to use a digital autopen to affix their digital signature to the Federal Register document.

This playbook will be available on https://playbooks.idmanagement.gov.

Please reach out to ICAM@gsa.gov with any questions on this playbook or the process.

For More Info

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