FPKIMA Newsletter

Spring 2019 | Volume 6, Issue 2

Federal PKI Management Authority
Enabling Trust

Inside This Issue

FPKIMA Content Delivery Network

The FPKIMA migrated the hosting of HyperText Transfer Protocol (HTTP) repository services to a cloud-based content delivery network solution. Existing Federal PKI CA certificate Uniform Resource Locators (URLs) will not change as a result of this migration and should be a seamless user experience with improved performance. For more details, go to https://go.usa.gov/xm9F5 or email fpki-help@gsa.gov

Big Bridge Issue

The Value of PKI Bridge Partners in the Federal PKI

The Federal PKI is unique in that it applies both a technical and policy constraint on its PKI members. In the PKI world, the technical constraint is known as a cross-certificate which contains specific constraint extensions. A cross-certificate is when Certification Authorities (CA) issue a certificate to each other and map certificate policies defined at a policy level to establish a trust relationship. This allows two or more organizations to better control how they trust PKI-based identities and signatures that originate from outside their organizations.

A Bridge PKI acts as the trust hub issuing cross-certificates to connect organizations or communities of interest. In the Federal PKI, the Federal Bridge CA serves this purpose by cross-certifying Federal Agency PKI, Bridge CAs, and commercial affiliates. These cross-certified CAs have established a trust relationship for interoperable use of PKI-based identities and signatures within and outside of the Federal Government, saving both time and money to the government issuing the same credential.

There are four commercial Bridge PKIs in the Federal PKI;

1) CertiPath Bridge serving the defense and aerospace community.
2) SAFE-BioPharma Bridge serving the healthcare community.
3) Southwest Texas Regional Advisory Council (STRAC) Bridge serving the State, Local, Tribal, and Territorial (SLTT) community.
4) Transglobal Secure Collaboration Participation (TSCP) Bridge serving the defense community.

For more information on the Federal Bridge CA and our bridge partners, go to https://fpki.idmanagement.gov or send a question to fpki@gsa.gov.

CertiPath Bridge CA

A Trust Hub for the Aerospace and Defense Industry

The CertiPath Bridge Certification Authority (CBCA) was established in 2006 as a trust-hub for commercial entities that were fielding PKI within their enterprises. The Impetus for the CBCA came from the Joint Strike Fighter program, a collaboration among the Aerospace-Defense industry, the Department of Defense (DoD) and U.S. Allies. CertiPath worked closely with the Federal PKI Policy Authority and the DoD PKI Office in establishing the CBCA, modeled on the Federal Bridge Certification Authority (FBCA), which resulted in high assurance environment suitable for trust across the three communities of interest.

The Department of Defense, a member of the FBCA, issued guidance recognizing the relationship between the Bridges as satisfying its own criteria for accepting digital credentials from external parties. Between them, CertiPath Bridge members use their own Enterprise credentials to access hundreds of websites associated with the programs they support, within DoD and with other Federal organizations. Some examples include;

- Joint Personnel Adjudication System (JPAS) - Organizations recognized by the DoD through their relationship with the FBCA via the CBCA can use their Enterprise-issued credentials to gain access to the JPAS personnel clearance repository, initiate an E-QIP session for the review and release of clearance paperwork to the government, and track clearance processing.
- Secure Web Fingerprint Transmission (SWFT) - This program permits members of the CBCA to upload fingerprints for submission to the clearance process.
- National industrial security program's Central Access Information Security System (NCAISS) - This portal managed by the Defense Security Service (DSS) affords members of the CertiPath community the ability to verify facility clearances, interact with DSS, and report on changes to facility parameters. This automated system has saved untold manhours in clearance document preparation.

Other members of the CBCA support use cases within the non-DoD Federal community. For example, the Department of Education (DoEd) refers defaulted student loans to third party debt collection companies and has mandated multi-factor credentials for accessing Department defaulted loan records. The preferred solution is the PIV-I card, and approximately one-half of the participating loan servicing companies acquire these from Carillon Federal Services, a CBCA member. In addition to the case studies above, member's credentials are used to authenticate individuals for access to online resources, to sign and encrypt email exchanges, and for digital document signing. The Netherlands Ministry of Defense leverages its relationship with the CBCA to exchange signed/encrypted email in support of several military jet fighter programs with other CBCA members and the DoD.

The CBCA is first and foremost a trust-hub for its own membership, among which are organizations that support the Aerospace-Defense Industry and its supply chain along with other commercial sectors. For more information on the CertiPath Bridge CA or how it supports the Aerospace and Defense Industry, go to https://www.certipath.com

NIST FIPS 201-3 Workshop

On March 19th, NIST hosted a federal-only FIPS 201-3 business requirements workshop. Topics included PKI and non-PKI derived credentials, federation, remote supervised identity proofing, and facility access. Go to https://go.usa.gov/xm59m for more information.

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/

An Offline Federal Bridge CA

A change request to operate the Federal Bridge CA as an offline CA was approved by the Federal PKI Policy Authority. This will give the FPKIMA the option of commissioning the Federal Bridge CA as an offline CA when it reaches its half-life at the end of 2019. The change request will also allow for a longer validity period if operated offline. For more information or to read the change request, go to https://go.usa.gov/xm9FB

Have you seen the revised NIST special publication on Trustworthy Email?!

NIST Special Publication 800-177 revision 1 was published in February 2019. Updates include newly specified email protocol security additions, such as Mail Transfer Agent Strict Transport Security (MTA-STS) and Transport Layer Security (TLS) Reporting, as well as an email system FISMA overlay developed to aid systems administrators in deploying email services that address relevant FISMA controls. For more information, go to https://go.usa.gov/xm9Mu

STRAC Bridge CA

Enabling State and Local Government Interaction

The Southwest Texas Regional Advisory Council for Trauma (STRAC) created the STRAC Bridge Certification Authority to help state and local governments and the healthcare community realize the benefits of federally trusted PKI credentials. The STRAC Bridge is helping its target communities interact with federal programs.

State, Local, Tribal, and Territorial (SLTT) emergency management agencies work closely with the federal government to plan for and respond to disaster incidents. Since 2017, they have used PIV-I credentials issued by STRAC Bridge CA affiliate Foundation for Trusted Identity (FTI) for access to federal emergency grant management systems.

Via the STRAC Bridge CA, SLTT emergency responders arriving at Joint Operations Centers prove their identities quickly and reliably by scanning their PIV-I credentials on mobile validation devices to support events as varied as hurricane response and the State of the Union Address. Through this application, the federal and SLTT responder agencies have awareness and accountability of their resources before, during, and in the aftermath of a disaster response. Similarly, SLTT emergency personnel use the Homeland Security Information Network (HSIN), for which smart card logon is enabled.

The STRAC Bridge CA also helps SLTTs interact with their federal government partners via physical access. When SLTT PIV-I cardholders visit a federal facility, they use their FTI PIV-I certificates to gain access to the building. For example, staff from the Texas General Land Office use their cards to gain access to the Texas Joint Field Office (a federal facility) to support the ongoing Hurricane Harvey recovery effort. The Federal PKI gains tremendous positive exposure this way as more than a few of those cardholders are leaders of state agencies visiting federal agency headquarters in D.C. (such as Interior and DHS) who greatly appreciate bypassing the usual time-consuming screening process.

In addition to benefiting from the traditional trust relationship provided by the FPKI ecosystem, SLTTs in STRAC's target communities can also use FTI PIV-I cards to meet less specific federal security requirements. The Missouri State Highway Patrol (MSHP), for example, has integrated FTI PIV-I certificates for use in its mobile VPN solution and accesses Criminal Justice Information Services (CJIS) subject to the CJIS Security Policy, which contemplates two-factor authentication. MSHP subscribers can use their cards to achieve two-factor authentication and improve the security of their interaction with the federal government via CJIS.

Finally, a tangential benefit for the federal government: when an entity in STRAC's community of focus enables its systems to consume PIV-I certificates, those systems can also consume PIV credentials presented by federal personnel. For both physical and logical access, customers of FTI are enabling federal personnel to use their PIV cards to access non-federal facilities and systems. For more information on STRAC or FTI, go to https://www.fti.org.

SAFE-BioPharma Bridge CA

Improving Patient Experience and Health Exchange

The SAFE-BioPharma community is focused on the use of high assurance digital signature and authentication credentials to support sensitive business transactions in the healthcare sector. Digital identity in healthcare is particularly important because it is a highly regulated industry with transactions that involve sensitive Protected Health Information (PHI). Companies who violate regulatory compliance rules or suffer data breaches of PHI can face severe penalties and significant damage to reputation.

Healthcare organizations that implement a strong digital identity strategy can reduce friction for patients, ensure patient privacy and safety, significantly reduce risk, and even create revenue opportunities. Use of credentials issued and managed according to SAFE-BioPharma standards, which align with Federal PKI standards, for business transactions in healthcare achieve these benefits. Business transactions where these credentials can be used include regulatory submissions to government agencies, electronic prescription of controlled substances (EPCS), and third-party business transactions.

As healthcare companies develop drugs and medical equipment, they must follow strict approval processes established by the US Food and Drug Administration (FDA) and/or the European Medicines Agency (EMA). Using a SAFE-BioPharma-compliant digital signature credential, a chain of custody requirement is easily achieved because the identity of the signer is very clear and easily proven by showing that the certificate was issued according to stringent policies and security controls. The EMA has more stringent requirements than the FDA and requires signatures mayde by a Qualified Certificate, which is considered valid, non-repudiable, and has the same effect as a handwritten, wet signature in the European Union by law.

The US Drug Enforcement Administration (DEA) governs how controlled substances are prescribed and requires either a digital signature from a Federal PKI certificate or a non-PKI credential that aligns with NIST Special Publication (SP) 800-63. While many of the EPCS transactions performed are executed with non-PKI credentials, some pharmacies and healthcare providers do use FPKI certificates and must follow DEA regulations or risk losing their licenses to do business.

The digital identity credentials issued under SAFE-BioPharma and FPKI rules, provide government and commercial organizations the ability to reuse credentials for information sharing, servicing medical devices, or systems used throughout the supply chain, while maintaining compliance with strict rules for audit and security to reduce their exposure to risk. While there are many uses cases for digital identity credentials in highly regulated industries, a high assurance credential that is recognizable across sovereign borders provides our partners with an increased return on investments across multiple risk categories. Credentials that are issued and managed according to the stringent standards set forth by SAFE-BioPharma can be used to improve the patient experience, protect patient privacy, enhance patient safety, and significantly reduce risk of data breaches or other cyber threats. For more information on SAFE Bio-Pharma, go to https://www.safe-biopharma.org/

CAB Forum S/MIME Working Group Charter almost finalized

The CAB Forum is a volunteer group of certificate issuers and certificate consumers creating PKI public-trust guidelines. They are finalizing a new charter to create an S/MIME Working Group who will draft S/MIME public trust requirements. If you are interested in following its development or participating yourself, go to https://cabforum.org/ for more information

FINAL VOTE!

The new U.S. Federal Public Trust TLS Certificate Policy is ready for a final vote by the Federal PKI Policy Authority. This new Certificate Policy and infrastructure is focused on Internet PKI requirements. The CAs operating under this Certificate Policy in the new infrastructure will not have cross-certificates with any existing Federal Public Key Infrastructure CAs. This is one step towards new purpose driven services intended to support mission needs. To read the new certificate policy, go to https://devicepki.idmanagement.gov/

Federal PKI Management Authority
Enabling Trust

Need Help?

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

ASK THE FPKI!

FPKI-Help@GSA.gov

Do you send digitally signed email and documents? Let us know!

The Federal PKI is currently updating our PKI use cases. One use case involves sending digitally signed emails or documents outside of the government to mission partners including U.S. or international business partners, foreign governments, or citizens. Please let us know if your agency uses a PIV card or other FPKI certificate to perform any of these actions. Send your feedback to FPKI@gsa.gov to ensure this capability is sustained in any future enhancements.

Federal PKI Working Group Updates

The Certificate Policy Working Group (CPWG) and work teams have met throughout the quarter to make progress on potential changes to device certificate and PIV-I procedures and multiple minor updates;

1) A number of low impact Federal Bridge and Federal Common Policy changes are scheduled for a discussion in Q4 FY19.
2) The group reviewed and recommended approval to the FPKIPA the "Allow FBCA Offline" change request introduced by the FPKIMA.
3) DoD briefed its CAC modernization memo which was released in December 2019.

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

1) **PKI Configuration Assessment Tool for Relying Party Applications** - The group was briefed by a non-profit organization that wrote a relying party configuration assessment tool. The tool combines both a server configuration and PKI assessment.
2) **Key Transparency** - Key Transparency is a Merkle-tree based ledger for storing and retrieving encryption keys. While not designed for PKI, it could accommodate PKI certificates and has potential over a wide range of encryption retrieval use cases.
3) **Post-Quantum Cryptography Status** - NIST gave a status update on its Post-Quantum Cryptography project. General guidance included wait for final results and implementation guidance at the end of the selection process. Similar to other cryptography selection projects, it is a multi-year effort between selection and vendor support.

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

Can I be notified of new certificate issuances or other system notifications?

Yes! System notifications including; changes to Certificate Revocation List Distribution Points (CDP) and Online Certificate Status Protocol (OCSP) endpoints, new or retiring URIs, and signing or revoking a Certificate Authority (CA) certificate are posted to the FPKI Guides System Notification page at https://fpki.idmanagement.gov/notifications/#notifications. You can subscribe to system notification and other issues by signing up for a GitHub account and watching the FPKI guide repository at https://github.com/GSA/fpki-guides.

Where Can I Find More Information about the FPKIMA?

For more Information about the the FPKIMA, go to https://www.idmanagement.gov/fpkima/ or the FPKI Guide website at https://fpki.idmanagement.gov/.