FPKIMA Newsletter

Winter 2018 | Volume 6, Issue 1

Federal PKI Management Authority
Enabling Trust

Inside This Issue

The Home Stretch!

The Federal PKI TLS Working Group is putting the final touches on the new TLS Certificate Policy. This policy was written to address Internet PKI requirements and to support the establishment of a new U.S. Federal Public Trust TLS PKI for .mil and .gov public web services. This new Public Trust TLS PKI will be under a new federal root and not connected to the Federal Bridge. For more details on the new Public Trust TLS or the Public Trust TLS policy, go to https://go.usa.gov/xE4cQ

GSA ACES Program Sunset Update

Important Dates in 2019 and Beyond

The GSA Access Certificates for Electronic Services (ACES) Program was established in 1999 to support the growth of PKI credential use for high assurance needs. Since that time, the Federal PKI has matured to the point where a government-operated, citizen-based PKI is no longer needed. In January 2018 it was announced the GSA ACES Program would be sunset over a two-year period to allow all ACES relying parties, vendors, and subscribers to migrate to an alternative credential. As the current ACES credential expires, it will be renewed with a FPKI alternative credential. The recommended FPKI alternative credentials are either Non-Federal Issuer (NFI) credentials from the Federal Bridge or Department of Defense External CA credentials, but check with the relying party before buying a replacement credential. A transition plan was implemented in three phases:

1. **Inform (FY18Q1 – FY18Q2)** COMPLETE
   a. Notify ACES vendors and federal relying parties of the program sunset and transition plan. After understanding vendor and federal relying party impact and needs, develop transition guidance and a public sunset announcement.
2. **Transition (FY18Q2 – FY18Q4)** COMPLETE
   a. The ACES PMO will collaborate with the ACES vendors and federal relying parties to transition to Federal PKI alternatives that are comparable to ACES certificates.
3. **Sunset (FY18Q4 – FY20Q4)** In Progress
   a. Based on the expiration date of the last active ACES certificate, the ACES PMO will monitor sunset status through ACES vendor monthly reporting on remaining active certificates. Around September 2020 when the last ACES certificate is either revoked or expires, the ACES PMO will direct the ACES vendors and the Federal PKI to revoke all ACES CA certificates and decommission the ACES issuing CAs. The ACES PMO will also be decommissioned and program material archived.

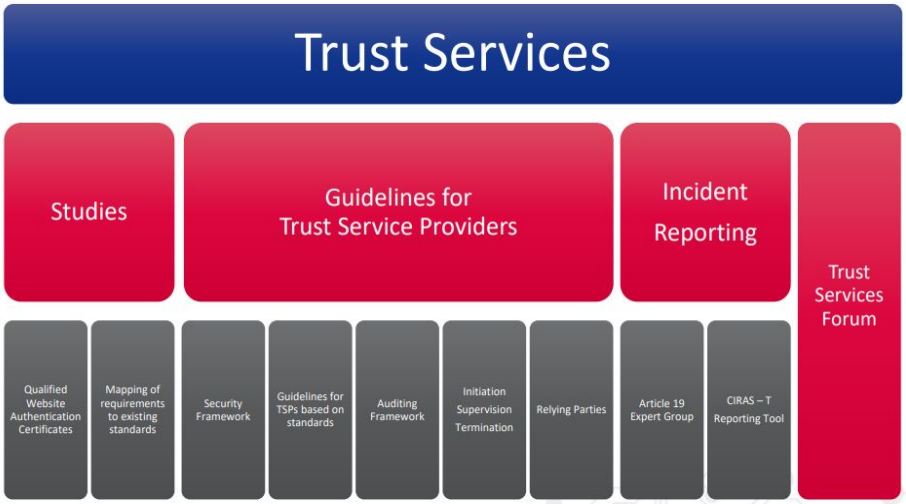
The first two phases of the transition plan were completed by September 2018. The official deprecation began in September 2018 with a decrease in ACES credential validity period from two years to one year. The next milestone is September 2019 when all ACES vendors will stop certificate issuance. The final sunset date is set for around September 2020. The ACES Program served a fundamental role in the development and growth of the Federal PKI and will be remembered as one of its foundational elements. For more information on the ACES Transition, go to https://go.usa.gov/xQTsq or email GSA-ACES@gsa.gov.

10th EU Certification Authority Day

Latest Progress in EU PKI Implementation

In conjunction with the 4th Annual European Union (EU) Trust Services Forum, EU PKI and Auditors hosted their 10th Annual Certification Authority Day in Alexanderplatz, Germany. The purpose of the event focused on current issues related to Trust Service adoption across Europe including implementation, operations, and recognition within and outside of the EU.

The EU, through its technical and independent agencies, have implemented a legal framework for electronic identification within the EU referred to as "Trust Services". The framework not only includes electronic and digital signatures, but also person authentication and devices. For digital signatures, the framework includes a PKI certificate policy, certificate profiles, an audit and security framework, incident reporting, and Trust Service Provider (TSP) guidelines. The intent of this framework is for national and international recognition of EU Member State issued credentials (Qualified Certificates or QC). Instead of a bridge PKI similar to the U.S. Federal Government, the EU has implemented trust lists. These lists are published by EU Member States with the goal that a QC issued in Greece is recognized in Germany or even the U.S. to digitally sign various documents or authentic through a passport or other type of nationally issued identification. A lofty goal that relies on reciprocity, governance, and trust.



***EU** Electronic **ID**entification, **A**uthentication, and Trust **S**ervices (eIDAS) in a Nutshell*

Some of the CA Day topics included:

- New opportunities for Remote Signing Trust Services
- Global recognition of eIDAS compliance audits
- eIDAS role in EU Cybersecurity Policy
- Trust Lists Situation, Initiatives, Next Steps, and Challenges
- Hybrid PKI for IoT Solutions

Full recognition of eIDAS Trust Services went into effect on September 29th, 2018. The ultimate goal is global interoperability of EU Trust Services with national and international partners including the U.S. Federal Government along with alignment with a broader EU cybersecurity policy. For more information on the eIDAS, EU Trust Services Forum, or the EU CA Day including presentations from the event, go to https://www.enisa.europa.eu/events/tsforum-caday-2018/

NIST 800-37 R2 Finalized

The next revision of the NIST Risk Management Framework was finalized in December 2018. This new revision evolves the risk framework into an enterprise risk management framework incorporating automation and privacy considerations. For more info, go to https://go.usa.gov/xE4aX

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/

Does your agency have tight network egress controls?

The FPKIMA is currently testing a new content delivery network for production HTTP repository services. The testing is occurring in the Community Interoperability Test Environment (CITE) with a few agencies. If your agency has tight network egress controls, you may be impacted by this change. Please contact the FPKIMA at FPKI@GSA.gov to be part of the testing.

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 you feedback to FPKI@gsa.gov to ensure this capability is sustained in any future enhancements.

Federal PKI Activity Report Update

Enhancements to Keep you Knowledgeable

The Federal PKI Activity Report is an almost real-time dashboard of the latest FPKI compliance status, FPKIMA certificate activity, and FPKI repository availability. It is a great resource if you need FPKIMA certificate information on issued, removed, or expiring certificates as well as compliance status of all FPKI partners.

This quarter featured a number of user experience and interface changes including color coded status and availability tables as well as format improvements based on feedback from the FPKI Technical Working Group and various FPKI users.

Federal Agency and Affiliate PKI Status Summary

Federal Agency or Affiliate PKI	FPKIMA CA	Status
CertiPath Bridge	FBCA & SHA1FRCA	No Issues
Department of Defense	FBCA & SHA1FRCA	No Issues
DigiCert/Symantec NFI	FBCA	No Issues
Entrust Managed Services NFI	FBCA	No Issues
Exostar NFI	FBCA	No Issues
Government Printing Office	FBCA	No Issues
GSA Access Certificate for Electronic Services (GSA ACES)	FBCA	No Issues

Repository Availability

Federal Agency or Affiliate CA	FPKIMA CA	Nov 2018	Average
CertiPath Bridge CA - G2	FBCA	100	100
CT-CSSP-CA-A1	FBCA	100	100
DigiCert Federated ID CA-1	FBCA	100	100
DoD Interoperability Root CA 2	FBCA	99.05	99.92
Entrust Managed Services NFI Root CA	FBCA	100	100
Entrust Managed Services NFI Root CA 2	FBCA	100	100
Exostar Federated Identity Service Root CA 2	FBCA	100	99.99
Federal Bridge CA 2013	FBCA	100	100
Federal Bridge CA 2016	FBCA	100	100

Color coded status tables make it easier to identify an issue

FPKIMA Certificate Activity

Affiliate	Subject CA	Issuing CA	SHA-1 Hash	Issued Date
Verizon	Verizon SSP CA A2	Federal Common Policy CA	477BF4017D25CDE276CDDDF756D40CA591D76F6D	12/05/2018

Uses hash rather than serial number to identify a certificate

A few of the proposed, future enhancements include:

1. Expanding certificate activity to include all CA certificates issued under COMMON including the Federal Bridge.
2. An RSS or other notification service for Report updates.
3. Automating the certificate activity reporting to GitHub.

The Federal PKI Activity Report is available on the FPKI Guide site at https://fpki.idmanagement.gov/tools/fpkiactivityreport/. Have an idea for a new enhancement or other change? Submit it as an issue through our GitHub repository at https://github.com/GSA/fpki-guides/issues with the title "FPKIAR Enhancement".

Federal PKI Working Group Updates

The Certificate Policy Working Group (CPWG) met in October and November 2018 and created two new Work Teams to develop policy updates for device certificate automation and Federal PIV-I issuance.

1) **Device Certificate Automation** - This Work Team plans to address NPE certificate issuance policy challenges that restrict the use of automation in Federal Enterprise use cases including network infrastructure, TLS intranet, external and international partners.
2) **Federal PIV-I Issuance** - This Work Team plans to address federal issuance of PIV-I cards. This includes examining potential policy gaps, Federal Enterprise needs for alternative hardware tokens, and PIV-I recognition of federal employees and federal support that do not qualify for a PIV card. Questions to be answered include whether federal relying parties need to be able to distinguish federally issued PIV-I from current PIV-I credentials or from PIV.

The FPKI Technical Working Group (TWG) met in November 2018 to discuss the following topics:

1) **CITE Participation Guide Review** - The CITE Participation Guide will be updated to reflect changing environment requirements.
2) **Offline Requirements for Intermediate CAs** - The Federal Bridge CA should be allowed to operate in an off-line status.
3) **Two Person Control for Remote Access Terminals** - The terminal used to remotely access a CA zone must be controlled at the same level as the zone it is accessing.

The TWG also distributed a survey to develop potential topics for 2019.

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

Why are my PIV certificates validating to an Alexion Pharmaceuticals CA?

The Federal PKI uses a bridged PKI hierarchy where after establishing a business relationship based on mutual assurance, a set of cross-certificates are exchanged. The cross-certificates allow users in each organization to trust credentials issued from either party. FPKI certificates have the potential to validate to multiple CAs because of this relationship. As long as you see either the Federal Bridge or COMMON in a validation path, there is reasonable assurance the credential can be trusted. For more information on certificate trust, go to https://go.usa.gov/xE4Gy or send an email to FPKI@GSA.gov.

Where Can I Find More Information about the FPKI?

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

NIST Draft Publication on Internet Routing Integrity

Most of the routing infrastructure underpinning the internet lacks basic security services. Due to this, there is a higher potential for the introduction of internet routing misinformation to redirect valid traffic to malicious websites. The solution is wide adoption of Border Gateway Protocol route origin validation (BGP ROV). The NIST NCCOE has published new guidance demonstrating how to implement BGP ROV using a resource PKI to protect against internet traffic routing hijacks. To read the new pub or more information on the NCCOE project, go to https://go.usa.gov/xE4G5