FPKIMA Newsletter

Summer 2018 | Volume 5, Issue 4

Federal PKI Management Authority
Enabling Trust

Inside This Issue

It's Official!

Apple has officially removed the Federal Common Policy from the latest Apple iOS 12 and macOS Mojave. For more information on Apple or other Root Program removals of COMMON, email the FPKI at FPKI@gsa.gov or go to https://fpki.idmanagement.gov/truststores/

What is Federal PKI Compliance?

The What, Why, and How of Federal PKI Compliance

Independent compliance audits are the primary way that the Federal PKI Policy Authority FPKIPA ensures that Certification Authorities participating in the Federal PKI comply with the requirements identified in the appropriate Certificate Policy. All organizations operating a PKI that is cross-certified with or subordinate to the Federal PKI, whether via the Federal Bridge Certification Authority FBCA or directly with the Federal Common Policy (COMMON) Root, must submit an Annual Review Package to the FPKIPA.

Federal PKI Annual Audit Criteria

The Certificate Policy establishes the requirements for operating and managing a PKI, to include the operations and management of the Certification Authority , Registration Authority , Repositories, Credential Status Services , and related security-relevant ancillary components (e.g., Card Management System). The Certification Practice Statement describes how the Certificate Policy requirements are met by the operational PKI system. A PKI Compliance Audit is conducted by an independent assessor that meets FPKI auditor qualifications and ensures:

1) The PKI's Certification Practice Statement adequately describes operational practices that meet the requirements stated in the relevant Certificate Policy, and
2) The PKI's operational practices follow the CPS.

The PKI Compliance Audit ensures that the PKI systems meet all security requirements specified in the policy and practice statement as well as the operational, technical, and procedural controls to meet the specified assurance that the certificates were issued correctly.

Federal PKI and Federal Information Security Management Act (FISMA) Compliance

Federal Agencies are also subject to additional assessments:

- A Federal Agency PKI certified with the Federal PKI and Shared Service Providers are subject to a FISMA Review / Authority to Operate (ATO).
- Shared Service Providers must also execute a Registration Authority Agreement with any organization, including federal agency customers, that provide any portion of identity proofing, enrollment, certificate request, and PIV card issuance activities.
- All federal agencies must undergo a NIST 800-79 *Authorization of PIV Card Issuers and Derived PIV Credential Issuers* assessment before issuing or contracting issuance of PIV services.

If you have any questions or want more information on the FPKI Compliance, go to https://www.idmanagement.gov/fpki-cas-audit-info/ or send an email to FPKI@gsa.gov.

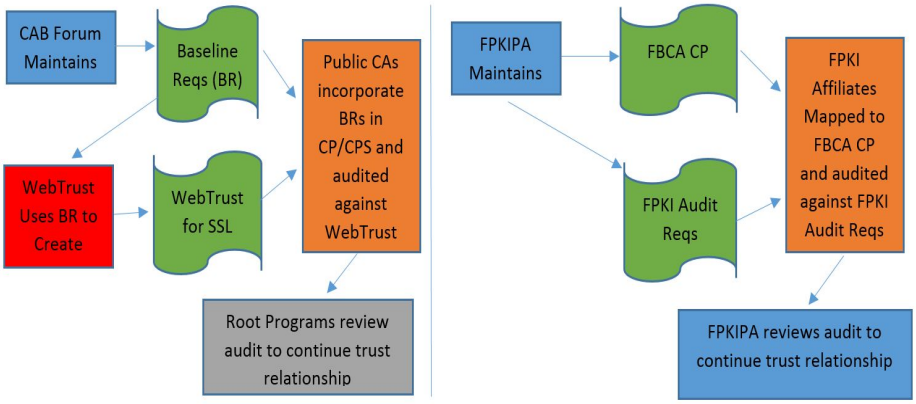
Industry PKI Compliance

What and How is it Different from Federal Compliance?

The Federal PKI isn't the only organization with a PKI assessment criteria. Three other organizations publish internationally recognized PKI assessment schemes for different, but similar purposes.

International Organization for Standardization (ISO)

Updated in 2018, ISO 21188:2018 *Public Key Policy and Practices Framework* is a set of framework requirements on PKI management specific to the financial services industry. In fact, the first digital signature and electronic authentication law in the US was related to the financial industry to update the Bank Protection Act of 1968. ISO 21188 was designed to help implementers define PKI practices for multiple certificate types, but stops short of addressing authentication methods, non-repudiation requirements or key management protocols. For more information on this or other ISO standards, go to https://www.iso.org/standard/63134.html.



Comparison of WebTrust and Federal PKI Audit Development

WebTrust

WebTrust was developed by a joint US/Canada PKI Task Force of public accounting professionals with the intent to increase public PKI confidence through third party assurance. The WebTrust Principles and Criteria for Certification Authorities is a general PKI audit based on ISO 21188 which also doubles as a self-assessment guide for enterprise and private PKIs. WebTrust also has additional schemes for SSL, SSL Extended Validation, and Code Signing Extended Validation to meet CA/Browser Forum requirements. WebTrust audits are performed by CPA Firms licensed as WebTrust practitioners. For more information on WebTrust and WebTrust audit standards, go to https://www.webtrust.org.

European Telecommunications Standards Institute (ETSI)

ETSI is an independent, not-for-profit, organization responsible for standardization of information and communication technologies within Europe (kind of like a European version of NIST). Specific to PKI, ETSI has developed a set of electronic identification and trust services for electronic services which is trusted across the European Union and the world. The ETSI standards include requirements for digital signature (EU Qualified Certificate), website, and time stamping as well as an audit scheme. ETSI audits are actually more like a certification are performed by EU regionally accredited assessors. For more information on ETSI, go to https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx

Have you seen the new Federal PKI Activity Report?

The Federal PKI Activity Report is a near real-time resource of the latest technical and policy compliance status. See the report at https://fpki.idmanagement.gov/tools/fpkiactivityreport/ and leave a comment on how we can improve it.

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/

Have you seen the new Apple Certificate Transparency Policy?

Apple confirmed it will enforce certificate transparency (CT) on all Apple platforms for publicly-trusted TLS server authentication certificates issued after October 15, 2018. For more information on the Apple Certificate Transparency Policy go to https://support.apple.com/en-us/HT205280 or email the FPKI at FPKI@GSA.gov.

Have you seen the new Federal PKI X.509 Certificate Linter?

The certificate profile conformance tool is a new Federal PKI tool to analyze a certificate conformance to a predefined certificate profile. The tool works by the user selecting a Federal PKI certificate profile and uploading a certificate to the tool. The new tool will output a table which includes additional analysis indicating a "PASS" or "FAIL" to certificate profile conformance. Go to https://github.com/GSA/fpkilint for more information or https://cpct.app.cloud.gov/ to see the new tool in action.

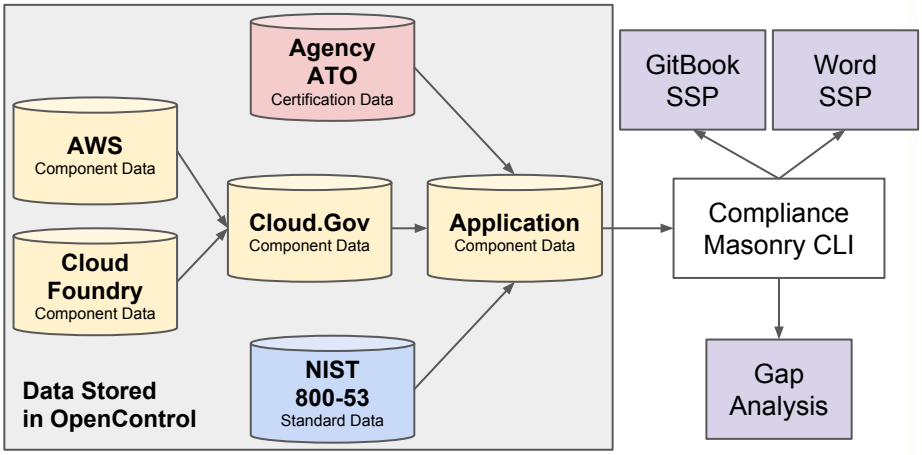
Machine Readable Compliance

Potential Tools to Help Meet Compliance Objectives

Maintaining compliance is critical for federal security systems and can be a very manual process. Artificial intelligence, blockchain, or robotic process automation are some of the newest tools, but so are open schemas. OpenControl is one of those compliance schemas to help continuously update security documentation as you continuously update your system. If you're using infrastructure as code, why not compliance as code?

Modern applications are built on a number of existing applications and platforms such as AWS, Cloud Foundry, or Red Hat. OpenControl is a schema written in YAML, a human-readable data language for configuration files. System operators can translate their system controls and certifications into OpenControl to automate compliance documentation such as a System Security Plan and maybe even a Certification Practice Statement. Configuration files can be shared with other government system owners to streamline the authorization process. It has three fundamental pieces:

1) **Standard** - A standard is a list of individual security control requirements. An example of a standard is NIST 800-53 or Payment Card Industry Data Security Standards (PCI DSS).
2) **Certification** - A certification is a curated list of controls that require some of kind confirmation. An example of a certification is an Authority to Operate or an Auditor attestation.
3) **Component** - A component defines a system's configuration. For example, the access control component would address a system's access controls.



Example of Compliance Masonry Data Flow (courtesy of https://github.com/opencontrol/compliance-masonry/tree/master/docs)

Compliance Masonry is a command-line tool and a GSA 18F project to construct certification documentation and create compliance dashboards using OpenControl schema. Engineers can update component files which will automatically update documentation to focus more on security and less on maintaining static documents. For more information on OpenControl and Compliance Masonry, check out http://opencontrol.cfapps.io/.

Federal PKI Working Group Updates

The Certificate Policy Working Group met in July and September 2018 to discuss the following topics:

1) **Private Key Retention Change Proposal** - This change proposal will allow Certification Authority private keys to be retained after it is decommissioned due to technical constraints and archive requirements. The private key must be protected in a manner comparable with its protection while active.
2) **Remove Public Trust TLS Requirements Change Proposal** - In May 2015, requirements were added to the COMMON Certificate Policy to align with the CA/Browser Forum. With the new Public Trust TLS effort, these requirements are no longer needed in the COMMON policy and will be removed in this change proposal.
3) **Policy Roadmap** - The working group discussed planning and prioritizing of policy updates and practices to meet federal agency mission needs.
4) **NIST 800-63-3 Alignment Change Proposal** - This change proposal will add supervised remote proofing as an additional proofing option per minimum requirements set in NIST 800-63-3.

The FPKI Technical Working Group will meet in November to discuss the following topics:

1) CITE Participation Guide Review
2) Offline Requirements for Intermediate CAs
3) Two Person Control for Remote Access Terminals

The Technical Working Group is always looking for new topics, best practices, or other discussion items to share knowledge with the FPKI Community. Participation in Federal PKI working groups is limited to Federal Agencies and Federal PKI affiliates. Please send any questions to FPKI@GSA.gov.

Ask the FPKIMA

Where can I find the FPKI Graph and Crawler?

The FPKI Graph has migrated to a new home at https://fpki.idmanagement.gov/tools/fpkigraph/. The Graph is a graphical depiction of how Certification Authorities in the Federal PKI link to another through cross-certificates, subordinate certificates, or PKI bridges. The Crawler capability which allowed a user to download certificates or certificate bundles is no longer available. To download certificates, you need to retrieve the information through the Authority or Subject Information Access URIs in the certificates. The FPKI Graph website has instructions on how to find the information to download certificates. Send any questions to FPKI@GSA.gov or post on comment to the FPKI Guide github.

Where Can I Find More Information about the FPKI?

Information is found at https://www.idmanagement.gov/fpki/ or 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

Monitor Your Network for Expired Certificates!

A report from the Government Accountability Office on the Equifax breach found that one of the causes of the breach was due to an expired certificate. Equifax found while it had devices to monitor encrypted network traffic for malicious activity, it somehow allowed traffic to pass through the network without being inspected. Upon further investigation, Equifax found the traffic was not being inspected due to an expired certificate. For more information on certificate management, follow the NIST NCCOE TLS Server Certificate Management project at https://go.usa.gov/xP5cj