FPKIMA Newsletter

Winter 2018
Volume 5 Issue 2

Federal PKI Management Authority
Enabling Trust

Inside This Issue

Almost There!

The General Services Administration (GSA) in collaboration with the Department of Defense (DoD) has almost completed the new Federal Public Trust Device PKI Certificate Policy. This will be a new and separate PKI infrastructure from the current Federal Common Policy. The Public Trust infrastructure will address the internet PKI requirements and help agencies comply with OMB Memo 15-13. More information on the new Public Trust Device PKI can be found at https://devicepki.idmanagement.gov/

Microsoft and Google Updates

In April 2018, Microsoft and Google will implement two significant changes described below. Both changes will impact the Federal PKI and all federal agencies that rely on the U.S. Government Root CA (i.e., Federal Common Policy CA [COMMON]). The General Services Administration developed two announcements on the Federal Public Key Infrastructure Guides website to share information on the impetus for these changes, recommended procedures to lessen the impact, and frequently asked questions. They are available at https://go.usa.gov/xnFkK.

Microsoft Impact

Due to new Microsoft requirements, the FPKI Policy Authority requested Microsoft remove the SSL/TLS trust bit for COMMON from Microsoft's globally distributed Certificate Trust List. Once this occurs, government and partner Window users may receive errors when browsing to internet or intranet websites. These errors will appear if all the following are true:

1) Using a Windows Operating System and/or Windows Mobile device
2) Browsing with Microsoft Internet Explorer or Edge or Google Chrome
3) The website uses TLS certificates that were issued by Federal PKI CAs
4) The server is configured to use COMMON for website certificate validation.

This will also impact cross-agency users of intranet websites. For example, a State Department user browsing to a DHS-hosted intranet website.

Google Chrome Impact

Google will start enforcing Certificate Transparency (CT) in Chrome. This change requires all SSL/TLS certificates to appear in a CT log and serve proof of this inclusion. The impact is limited to SSL/TLS certificates that validate to a Root CA certificate distributed globally by a trust store.

Certificate Transparency is an open framework that allows website owners and browser operators to monitor and log TLS/SSL certificates, detect issuance/ mis-issuance, and identify rogue CAs.

A CT error page will appear if all the following are true:

1) Browsing with Google Chrome on a desktop or mobile device
2) HTTPS handshake does not serve a signed certificate timestamp either embedded in the certificate or by the server.

At the time of publishing, the majority of Federal PKI CAs used by **federal agencies** do not support CT while the majority of commercial CAs do support CT. if you're concerned about CT related error pages, see the announcement link posted at the beginning of this article. Have a question on these updates or something else FPKI-related? Open an issue at https://github.com/GSA/fpki-guides/issues and we'll answer it!

NIST Digital Identity Update

The New 800-63-3 is Final and FPKI Impact

The new NIST Special Publication 800-63-3 Digital Identity Guidelines breaks away from traditional level of assurance (LOA) guidance toward a modular future. The biggest changes between 8000-63-2 and 800-63-3 include several fundamental differences:

1) Changed the title name from "Electronic" to "Digital" identity, recognizing the new direction of government and consumer credentials.
2) Breaks away from the traditional OMB Memo 04-04 LOAs by removing the LOA 2 level. New guidance outlines three LOAs across three identity components.
3) Introduces a modular approach to assurance, authentication, and federation components. This modular approach allows an agency to pick and choose between different identity levels at different authentication or federation levels.
    a. **Identity Assurance** – Focus on how an identity is created.
    b. **Authenticator Assurance** – Focus on credential management.
    c. **Federation Assurance** – Focus on credential interoperability.
4) Deprecates use of SMS one-time passcodes.
5) Allows remote identity proofing with caveats based on the identity assurance level.
6) Defined password requirements.
7) Introduces privacy considerations including limiting the collection, use, and storage of Personally Identifying Information (PII).

NIST used a community-driven approach and collected comments on both GitHub and through traditional commenting methods.

How does this impact the Federal PKI?

The Federal PKI Policy Authority have developed a change proposal to incorporate changes in both the Federal Common Policy and Federal Bridge certificate policies. It will be transparent for subscribers and PIV holders, but the Federal PKI issuer community will need to update policies and procedures. The most impactful changes include the following:

1) Allow supervised remote identity proofing.
2) Passphrases will be a minimum of six characters.
3) Align language to reference 800-63A defined superior evidence level. In a nutshell, superior evidence includes:
    a. Person's full name, both printed and part of digital information
    b. Biometric and photograph
    c. Credential is unexpired and includes secure delivery
    d. Physically and digitally tamper-resistant
4) Limit PII collection, use, and storage

Please send any questions on the FPKI change proposals to FPKI@GSA.gov. The new NIST 800-63-3 is available online at https://pages.nist.gov/800-63-3/.

Explore the IT Security Hallway yet?

The GSA Acquisition Hallway 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 with full site access for federal acquisition employees and approved contractors. Sign up at https://hallways.cap.gsa.gov/

Have You Seen the FPKI and PIV Usage Guides Lately?

GSA is leading the effort to develop open source guides on both the FPKI and PIV. The FPKI Guides contain information on FPKI links, tools, tips, and how to leverage the FPKI for agency security needs. PIV Usage Guides do the same except for PIV. Can't find an answer? Submit an issue and collaborate on the answer! For more information on the FPKI Guides, go to https://fpki.idmanagement.gov/

For more information on PIV Usage Guides, go to https://piv.idmanagement.gov/

Google Chrome Update for HTTP Websites

Google announced on their security blog all HTTP websites not using a SSL/TLS certificate will be marked "not secure." Google led a multi-year campaign to educate users to identify secure versus not secure websites and is implementing the next piece of the strategy. Fortunately, the Federal Government is ahead of the game with OMB Memo 15-13 compliance!

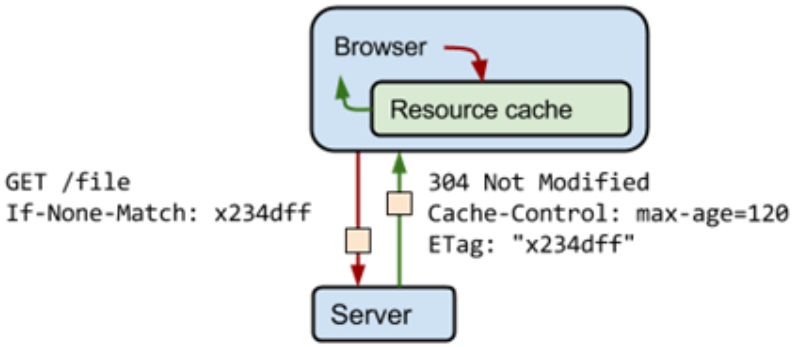
Tag It

How to Use E-Tags to Save Network Bandwidth

Is your agency hosting static HTTP artifacts including CRLs and p7c files? Are your cache control headers ignored by clients and relying parties? Use Entity Tags or E-Tags. A large amount of enterprise bandwidth is consumed by Relying Party Applications downloading these files when verifying certificates. A standard PKI use case is to verify a Certificate Revocation List (CRL):

1) An application requests an HTTP-based CRL to validate an email signature.
2) PKI HTTP repository sends full HTTP 200 response with CRL.
3) Application caches the CRL.
4) Five minutes later, the application requests the same CRL to verify another email and needs to confirm the CRL has not changed.

PKI artifacts are often only a few kilobytes, but a small file requested millions of times a day can consume astonishing amounts of bandwidth. For example, the average size of the Federal Bridge CRL file is 24 KB. Although no certificates were revoked in December 2017, it was downloaded 295,927,591 times which resulted in 6.27 terabytes of bandwidth… 6.27 TB for an artifact that did not change!



Example of an E-Tag (courtesy of Google Developer Page)

E-Tags can change this use case by assigning a fixed identifier to the artifact. Effective use of E-Tags is dependent on applying a consistent policy across all servers. The consuming client can determine if the content has changed and only download a new artifact if the E-Tag is different. It mimics the same effect as a caching mechanism due to the client implementation behavior. Using the example above:

1) An application requests an HTTP-based CRL to validate an email signature.
2) PKI HTTP repository sends full HTTP 200 response with CRL and E-Tag: "33a64df551425fcc55e4d42a148795d9f25f89d4"
3) Application caches the CRL.
4) The application requests the CRL again and includes the E-Tag in the request. The PKI HTTP Repository sends an HTTP 304 response with an empty body if the CRL has not been updated.

PKI Operators should verify their e-tag policy to ensure it is consistent across all web servers. Consider using and respecting cache control headers and E-Tags to save network bandwidth.

FPKI Working Group Updates

The Certificate Policy Working Group (https://go.usa.gov/xnraS) met in December 2017 to discuss the following topics:

1) **Bridge Test Plan** – The Requirements and Guidelines Document was published by the FPKIPA on December 19th, 2017. PKI Bridges must submit final test plans no later than May 31, 2018.
2) **PKI Operating on Virtualized Equipment Requirements** – The group is developing requirements for PKI operating on virtual equipment.
3) **NIST 800-63-3 Alignment** – 800-63-3 review against Federal PKI policy.

The FPKI Technical Working Group (https://go.usa.gov/xnrah) (Minutes - https://go.usa.gov/xnMK2) met in January 2018 to discuss the following topics:

1) **Microsoft Change Impact** – Microsoft updated its Trusted Root Program requirements. The group reviewed the advantages and disadvantages to either remove the TLS trust or accept government TLS domain constraints.
2) **Community Interoperability Test Environment (CITE) Feedback** – CITE is the FPKI test environment providing many different needs. Feedback was gathered on how to enhance and make it more useful/valuable.
3) **Monthly Statistical Report Feedback** – The FPKIMA publishes a monthly report on FPKI Trust Infrastructure activity and availability. Feedback was gathered on how to improve and make it more useful/valuable.

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 notification or status information on FPKI CAs?

There are a few tools available.

1) **System Changes and Notifications** – This information is available on the FPKI Guide site (https://fpki.idmanagement.gov/notifications/). Changes, planned outages, and CA certificate signing or revocation is posted here.
2) **FPKI CA Discovery** – The FPKI Graph (https://fpki-graph.fpki-lab.gov) and Crawler (https://fpki-graph.fpki-lab.gov/crawler) provide both a graphical interface and formatted reports on all CAs in the Federal PKI.
3) **FPKIMA Monthly Statistical Report** – This report contains CA compliance and status, FPKI Trust Infrastructure issuance, and FPKI directory and repository availability. To receive a copy of the report, send an email to FPKI@GSA.gov with subject line "Add to FPKI Customers List."

Don't see what you need? Send an email to FPKI@GSA.gov so we can add it.

Where Can I Find More Information on the FPKIMA?

Information is found on the idmanagement.gov website: https://go.usa.gov/xnraJ

Federal PKI Management Authority
Enabling Trust

Need Help? Can't figure out why your certificate is not validating?

Contact the FPKI!
FPKI@GSA.gov

Is Malware Hiding in a PKI Certificate Extension?

A potential PKI exploit was identified where malware, code, or other data can hide within a PKI certificate extension. The Subject Key Identifier extension does not have a size limit and may contain malware or be used to exfiltrate data. It may elude network appliances because the certificate is exchanged in plain-text and contents are not scanned. The impact is very limited. An attacker must be able to install a rogue CA into a target enterprise to execute the exploit and then issue certificates within the enterprise to exfiltrate the data.