FPKIMA Newsletter

Fall 2017
Volume 5 Issue 1

Federal PKI
Management Authority
Enabling Trust

Inside This Issue

[Have you provided your comments to the Federal PKI NPE Certificate Policy?](https://devicepki.idmanagement.gov/)

OMB M-15-13 mandates federal agencies secure web services and websites using PKI server certificates. In response, the Federal PKI has developed a new Certificate Policy (CP) to support the establishment of a new Public Trust Device PKI for .mil and .gov websites. This new device PKI will not be cross-certified with the same people PKI that issues the PIV cards and contains the Federal Bridge. The draft CP is publicly available for review and comment at

https://devicepki.idmanagement.gov/

What Does the Future Hold for PKI?

PKI has experienced widespread adoption within the federal government, for example, server certificates on devices, smart cards issued to employees, and software-based signature and encryption certificates. Where are government and industry taking PKI in the future? The Blockchain is seen as the next "digital disruption" and many agencies are waiting to see how it can transform digital government services. The main advantage of Blockchain is it allows untrusted entities to agree on transaction history and arrive at an agreement on the current state. The entities may continue to distrust each other, but the transaction is trusted based on a consensus of the starting point and history. This simple principle may be applied over multiple solutions such as passport verification, identity proofing, financial operations, evidence chain of custody, and various other scenarios.

Blockchain allows multiple untrusted or distrusted entities to agree on a transactions history to trust a future transaction.

Blockchain is dependent on a decentralized trust model where no one trusts a single source of data. The aggregation and consistency of data across multiple nodes decrease the risk on various fronts:

- **Single point of failure** – One node can go offline without disrupting the whole system.
- **Censorship** – A single entity does not control the transaction and cannot alter conditions or history.
- **Single point of trust** – The aggregate and consistency of the distributed information allows confidence in the system rather than in one entity or source.
- **Compliance** - The multiple nodes can also enforce consensus against future fraudulent transactions based on a review of its history.

How could Blockchain apply to PKI? Blockchain could decentralize how PKI is trusted:

1. **Revocation checking** – Rather than rely on individual revocation lists or online status checks, a PKI vendor would publish revocation data to a Blockchain.
2. **Validation checking** – Similar to revocation checking, Blockchain would contain the path to the trusted root based on the transaction history.

Those are just two examples of many. DNS, authentication, and signature are only a few of the potential Blockchain applications. Have an exciting Blockchain project? Send an email to FPKI@gsa.gov to be featured in a future newsletter.

FPKIMA State of the Union Summit 2017

Know Your Past, Know Your Future

The FPKIMA held a private, one-day summit in June to discuss the past, present, and future of the FPKI. PKI experts supporting federal, defense, aerospace, healthcare, pharmaceutical, and technology industries convened at GSA to understand the original intent of the FPKI and explore its future trajectory. The open discussion format provided the following key points, observations and recommendations.

Key Points

- PKI is not managed in a single location on a system or in an organization. PKI operators must educate their communities on how to properly use it.
- The Federal Bridge is the right trust model for the government community because of its embedded governance and technical controls. OMB originally requested the Federal Bridge include external organizations to facilitate e-commerce and electronic transactions between federal government and business, non-federal government, and citizen partners.
- The Federal PKI is a success. Agencies trust externally-issued credentials from other agencies and business partners because of the Federal Bridge.
- Communication and participation between PKI communities are the keys to success.

Observations made by Government/Industry attendees:

- The Federal CIO Council support was critical in building the Federal PKI. Regular briefs to the CIO Council should be conducted to maintain adequate support.
- Many may say Federal Bridge validation is technically unfeasible, but most cryptographic libraries actually support it. Guidance on how to enable it is needed.
- As more federal IT services move to the cloud, it is important that Federal PKI is trusted and functioning properly in leading internet browsers.
- Develop and integrate Agile processes into PKI compliance and change management and ensure technology acquisitions include Federal PKI requirements.
- Participation in various PKI groups is the best method to ensure unique government requirements are integrated and understood.

Overall, the summit was a success in understanding the future direction of identity and authentication and how the government can support its growth. The Federal PKI will take these observations and evaluate if they should be implemented. While Industry PKI has traditionally focused on solving server authentication, all attendees recognized identity verification and authentication as the next building block to secure digital transactions. Recent authentication developments such as industry adoption of the Fast ID Online (FIDO) protocol is gaining wider recognition and use for its open source, privacy-enhancing, secure, and convenient form factor. Interested in attending the next summit? Send an email to FPKI@gsa.gov to be added to our customer's mailing list.

Did you know DHS has an Identity Management R&D Program that other agencies can leverage?

The Homeland Security Advanced Research Projects Agency (HSARPA) has a Cyber Security Division and funds identity management projects. The intent is to help government program managers with the research and development expertise and resources to increase security and trustworthiness of government programs. For more information, go to https://go.usa.gov/xnraG

Did you know Universities are one of the largest users of smart cards?

Colleges around the nation have consolidated access control and financial transactions to a single smart card. At some universities, students can buy food, access buildings, and log in to university websites via a smart card. They may even be able to use the same card to purchase items at local stores similar to the George Washington (GW) University network next to the GSA building. For more info on the GW program, go to https://gworld.gwu.edu/card-access

Increase Data Security with the Federal PKI

The Federal PKI is one of the most effective tools available to ensure confidentiality, integrity, and availability of government data. The Federal PKI takes the effort out of identifying implementation standards and ensures vendors and other federal agencies are operating securely. For example, both DoD and GSA require external users to acquire Federal PKI PIV-I, software PKI or other approved credentials before either gaining access or submitting official documents. To learn more, go to https://go.usa.gov/x3tRm

DHS Binding Operational Order (BOD) 18-01 – Enhance Email and Web Security

DHS first BOD of FY18 is to improve federal email and website security. For more details on deadlines and compliance reporting, go to https://cyber.dhs.gov/.

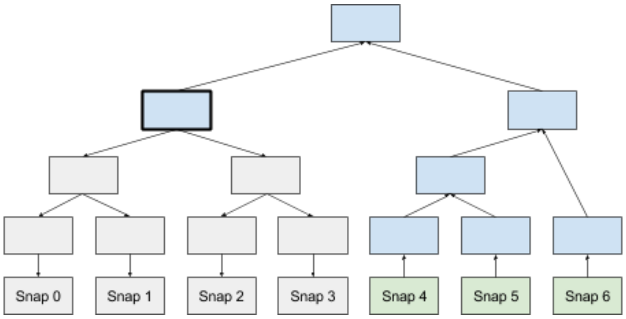
The Transparent Future

Blockchain-Like PKI Examples in Practice

Blockchain is touted as the future of everything digital, a disruptive technology similar to the World Wide Web. While traditionally associated with digital currencies such as Bitcoin, many federal agencies are testing its capabilities for everything from secure payments to identity management. In this newsletter, we will briefly look at the leading PKI-related projects using Blockchain-like technology.

Certificate Transparency (CT) is an experimental Internet Engineering Task Force (IETF) protocol (https://tools.ietf.org/html/rfc6962) for logging and identification of public server certificates. CT is dependent on three functions:

1. **Logs** are "cryptographically assured, publicly auditable, append-only records of certificates." Anyone can query or submit a certificate to a log which may be operated by various organizations. To further adoption, Google has adopted CT as a browser requirement with some participating CA's operating independent logs (https://www.certificate-transparency.org). There are currently 15 active logs.
2. **Monitors** periodically review public logs for suspicious activity. They can identify unusual extensions, mis-issuance, or other illegitimate certificates. One monitor is the website https://crt.sh which is an open source project from Comodo.
3. **Auditors** serve two functions in verifying logs remain cryptographically secure and verifying certificates appear in a log.



Example of a Merkle Tree appending only additions in bold (Source: Google Key Transparency)

CONIKS is a Princeton University project (https://coniks.cs.princeton.edu) for logging and managing user encryption keys and certificates. Encryption keys are stored in tamper-evident and publicly auditable key directories available to messaging clients. This provides the benefit of automated retrieval and verification of user identity to prevent malicious hijacking of communication sessions. Google also sponsors an open source project based on CONIKS called **Key Transparency (KT)** (https://github.com/google/keytransparency). KT has added privacy-enhancing features to only reveal keys individually rather than in bulk. CT, CONIKS, and KT rely on a Merkle Tree structure similar to Bitcoin in creating tamper-evident records.

The DHS HSARPA is currently funding government blockchain projects using actual mission use cases. For more information, go to **https://go.usa.gov/xnraG**

FPKI Working Group Updates

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

1. **New Change Proposals** - Potential Certificate Policy change proposal to extend Certificate Authority security requirement to virtual environments and ancillary components.
2. **Cache Control Header Requirements** – Cache Control headers decrease network traffic by maximizing CRL and P7C caching.
3. **Key Recovery Policy** - Final review of the Key Recovery Policy.

The FPKI Technical Working Group (https://go.usa.gov/xnrah) met in July to discuss the following topics:

1. **FPKI TLS/SSL Browser Testing** – GSA presented a case study on public internet perception of FPKI SSL certificates.
2. **USDA PIV Validation Challenges** – USDA operates a PIV-enabled authentication portal for 450 web applications. They presented common challenges to integrating the various cross-certified root certificates to accept PIV cards.
3. **Automated Certificate Management Environment (ACME) Protocol Overview** – NASA presented a case study on adopting the ACME protocol. ACME is an IETF standard for automated device certificate issuance.

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

How do I setup network PIV authentication on Windows machines?

Unfortunately, this question cannot be answered in this space, but the Federal PKI PIV guide is the perfect resource (https://piv.idmanagement.gov/networkconfig/). Network PIV authentication is broken down into six steps. More details and implementation guidance is found in the PIV guide.

1. Ensure the proper network ports and protocols are open.
2. Domain controllers certificate have been issued.
3. Configure Trust store and NTAuth Enterprise store.
4. Implement an active directory to PIV card linking solution.
5. Update group policy and enforcement to align with US Government Configuration Baseline (USGCB).
6. Tune network to increase performance.

Where Can I Find More Information on the FPKIMA?

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

Federal PKI Management Authority
Enabling Trust

Need Help?

Contact the FPKI
FPKI@GSA.gov

Explore the IT Security Hallway yet?

The GSA Acquisition Hallway aims to help federal acquisition official's 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/