Technical Working Group (TWG) Meeting Notes - 4/23/2020

Agenda:

- FCPCA G2 Characteristics
- Proposed Architecture
- Impacts on Common Policy CP
- Plans for cross-certification
- Proposed Migration Plan
- Request for Agency Input

FCPCA G2 Characteristics

- New CA Distinguished Name:
  - CN = Federal Common Policy CA – G2, OU = FPKI, O = U.S. Government, C = US
- RSA 4096 bit key
- Signing CA Certificates using RSA SHA-384
- 20 year validity period

Q: Santosh Chokhani expressed concern that the FPKIMA is making it appear that 4096 will be more secure when signed with SHA-384. 4096 bit keys only gives you 136-bits of security. SHA-256 is fine, but describe the reason for the change more precisely.
A: We hear you and will try to appropriately provide the reason for the recommendation. The NSA recommendation for RSA4096/SHA384 was based in part on CNSS Policy Directive 15 (CNSS-15).

Proposed Architecture

This will be a long-term evolutionary strategy, but the FPKIMA is looking to leverage the need to rekey the FCPCA to take a first step in evolving the FPKI. We propose creating a path toward an FPKI architecture that more closely aligns with current trends in industry standards and practice, while providing flexibility to better support both current and future uses within the government. This involves creating the ability to separate issuing CAs by application use. We understand this impacts all the issuing CAs as well as relying party application configurations. This would not be a done deal at the time of the FCPCA Rekey, but just the first step of a migration path that may take from 3 to 6 years.

In order to do this, we want to establish a second layer of “sub-roots” under the rekeyed Common Policy CA (FCPCAG2). To allow a slow migration to this new strategy we would initially create a Migration Sub-Root and move all the current CAs with a certificate from the current Common Policy (FCPCA) to this Migration Sub-Root. When issuing CAs and their customer agencies are ready for separate issuing CAs, additional Roots under the FCPCAG2 can be established. The sub-roots allow applications to be configured with a simpler certificate path that is only for one type of certificate. The FCPCAG2 can still be used by applications that can handle the more complex paths and determine which certificates are appropriate for their application. In other words, the same as the current FCPCA trust anchor with only the addition of a 1 more hop in the path.

At the same time, we would entertain the possibility of establishing a new Root to be used as the trust anchor for the Federal Bridge. There has been discussion at the FPKIPA for breaking the cross-certification between the FBCA and FCPCA due to the complexity in path validation and a desire to differentiate between federal issuers and our commercial partners.

One reason for the separation by certificate type is to distinguish between PKI uses entirely for "enterprise" or internal to the government use versus something where it might be useful for public trust. For example, digitally signed documents or email.

Q. Are we expecting most government employees will have 2 identities? One for Publicly trusted signatures and one for PIV?
A: No, there are 4 different subscriber certificates on a single PIV card and in a few current agencies these may already be issued by more than one CA on each user's PIV card. In most cases all 4 are issued by the same issuing CA. We envision the PIV Authentication and card Authentication certs might be issued from a CA under the Federal Authentication sub-root and the Signature and Encryption certs would be under the Public Signature sub-root, at least for those agencies that see a need for some of their signatures to be publicly trusted. However, in the short term things would continue to operate as they are now with all issuing CAs having a path up through the Migration sub-root.

Q. What does the FPKIMA define as a root?
A: A self-signed certificate for the CA that can be distributed for use as a trust anchor for relying party applications

Q. Are we going to be doing policy mapping?
A: Just like today, everything under the FCPCA G2 is expected to be operating in compliance with the Common Policy CP and asserting Common Policy certificate policies, with exceptions if we have a PIV-I Bridge Root or a cross-certificate to the FBCA or other Agency PKIs still operating under their own CPs,

Q. Why do we want to have a sub-root?
A: To allow for future flexibility

Todd Johnson: Stated he does not have a use case for publicly trusted signatures. Looking for other agencies that have the need for the Public Trust. Concerned that sharding CA 4 different ways will increase cost by 4.

Q. Are we looking at the tradeoffs?
A: Yes, but looking for Agencies to provide additional input as well. There are tradeoffs between separating CAs ability to issue only certain types of certificates by putting EKU on the CA certificate which is a Microsoft invention which may or may not be enforced by other path discovery and validation (PDVAL) libraries or just having separate PKI hierarchies by doing the separation based on different sub-roots.

Santosh Chokhani - Limiting a CA's issuance by way of EKU may help with security in some cases.

Tim Baldridge - Think about separation of CA's at agency level. Cost and time period. Does not feel we can get to it. Do not put EKUs in the CA certificates. Having an acceptable root has a lot of value.

Santosh Chokhani would like to have a discussion of the security trade offs. These should be documented to enable better discussion.

Todd Johnson - Feels it creates more issues across the board and does not see any value.

Tim Baldridge - Huge impact to DoD. DoD has multiple Root CAs. All other CA types are under a DoD Root. Do not require EKUs in the issuing CA certificates, it would take DoD a long time to be able to do that.

Wendy – at least from the names, DoD already has separate issuing CAs for identity vs Email protection, under those DoD Root CAs, they stand up issuing CAs in pairs. This may not be as big an impact to DoD as it might be to some other agencies. But, we are looking at what we expect to be a multi-year evolution. So take the idea of this proposed architecture back to your agencies and get additional input on whether this is something that should be considered.

Q. What are the questions we need to take back to figure out how we understand the decision?

A: These are some of the questions the FPKIMA would like agencies to consider. Please let us know if you have additional questions you think all participants should consider.

- Is there a need for public trust of signature certificates used for signing PDF documents?
- Is there a need for public trust of signed or signed/encrypted email?
- Is there value in simplifying path validation by having separate validation paths for different use cases, for example client authentication separate from digital signature, NPE separate from people?
- Is there a value in simplifying path validation by having separate validation paths by assurance level?
- Is there a value in having separate paths for Federally issued certificates vs those issued by our commercial partners under the FBCA?
- How should PIV-I be treated since it is defined strictly to be equivalent to PIV in everything but NACI?

Santosh - a document describing the changes, tradeoffs that we could edit and add comments would be easier than just a briefing and presentation deck.

Separate out the rekey versus ideas to improve the operation over time.

Q. Why remove the cross-certification of the Federal Bridge from the Federal Common Policy CA?

A: This is partially in response to the presentation DoD made to the FPKIPA. They indicated a need to be able to distinguish federally issued certificates from those issued by our commercial partners. They also indicated a need to be able to ensure there were no lower assurance certificates in the path to the FCPCA before DoD could rely on it as a trust anchor. This is just a question to the community, should we stand up a separate root for the FBCA?

- And if so, do we need different roots for each of the assurance levels under it to simplify the path building for applications that do not want to trust Basic or Rudimentary certificates?
- What do we do with PIV-I, keep it with the FCPCAG2, as it meets all the requirements of PIV other than the NACI or keep it with the FBCA, or split it so we end up with 2 types of PIV-I?

Tim Baldridge - DoD has a strict set of rules. Operation under the Risk Management Framework, federally issued certificates require an ATO which means the security requirements are strictly defined, assessed, and audited which means DoD can accept it.

Rebecca Nielsen – DoD has an additional set of rules for which CAs are acceptable for DoD applications. They are more concerned with the assurance level and do not want to accept anything external lower than medium Hardware. So PIV is acceptable as are all the PIV-I issuers. But they only accept medium assurance certificates from DoD or the ECA issuers because DoD owns the ECA CP. The DoD's baseline assurance level for external interoperability is Medium Hardware. However, DoD has expressed that they might be willing to trust the Federal Common Policy CA if the minimum assurance level for Federal agency PKIs is medium. The DoD CIO office is looking at changing DoD policies to better leverage credentials partners already have.

Q: Kyle Neuman - there is a requirement for a publicly trusted root CA for the Electronic Prescription for Controlled Substances (EPCS) program.

A: If the FBCA no longer has a path to the FCPCAG2 there would be a new Root established to be used as a trust anchor for the FBCA. However, whether this root or the FCPCAG2 are in public trust stores is part of the discussion. There has been a multi-year effort to remove the current FCPCA from public trust stores and at the current time it only remains in Microsoft. The EPCS requirement is for cross-certification with the FBCA, not necessarily a path to the FCPCA.

Q: Chris Benard - we have to validate prescriber signing certificates for controlled substance prescriptions. DEA requires they be signed eventually by FBCA. I'm unclear after the transition if FBCA will still be signed by FCPCA. We validate the chain up to the installed root on each windows box right now to FCPCA and verify FBCA is in the chain. Will there be some chain in the Windows store that something under a path signed by the FBCA will chain to for validation?

A: The certificate we are proposing be in the Windows store is the Federal Public Signature Root (in blue). We believe there is a need for signature verification in the public space. No one has brought to our attention needs for other public trust. We can still change this if there are such requirements though. More specifically, the "Bridge Root" would not be publicly trusted, and distributed through the MS Trust store. Again, this could be changed based on feedback if this is necessary.

Chris Benard - this is absolutely necessary for us (relying party) and every relying party in the HUGE EPCS (electronic prescription of controlled substance) space. We are required by DEA to validate certificates from prescribers that are signed by a CA signed by FBCA (along with

policies on the cert). it needs to chain to something in the trust store. Why would FPKI want windows machines NOT to trust something by default signed by the bridge?

Donovan Demshock - the reason the Common Policy CA certificate was removed from public browsers and OS was because some of the policies and statements could not be made publicly available, do we consider not including those in cross certification with FCPCAG2 so we can maintain industry compliance and public trust. As it is I believe agencies force particular trust paths as opposed to allowing any chain to be built and trusted for the federal bridge PKI.

A: While that was part of the issue, later resolved to some point, there was also the issue of Server Authentication certificates issued under FCPCA that did not meet CABForum requirements. Additionally, there are members of the PA that believe there is no need for public trust for non-Server Authentication certificates, and there is no one voicing that need (for digital signature, S/MIME, etc.). The public trust of Server Authentication certificates will be solved via a separate PKI hierarchy. If you feel your agency requires the FCPCAG2 or FBCA be publicly trusted please voice this at a FPKI Policy Authority meeting.

Q. Feedback on how long it will take to establish the CA after the rekey?
A: The Migration Root would be established at the same time as the FCPCAG2, the other sub-roots could be established when an agency was ready to take advantage of them.

Q. What does this mean to the current CITE Root CA.
A. Tom answered it will have no impact. Changes to CITE will mimic what we are proposing to do in production. The current test FCPCA environment stays untouched. A separate test FCPCAG2 and Migration Root are made publicly available in CITE when the first agency says they are ready to start testing and request a CA certificate from it.

Todd - We would need the date and time frame when changing to minimize impact for the ability to test. Treasury applications rely on the Entrust JAVA tool kit which assumes all certificates on each user's PIV to be issued by the same CA. They had to get a new release to deal with DoD CAC that has the authentication certificate issued from a different CA than the signature and encryption certificates. This type of change may require additional updates.
A: Let us know when you are ready to start testing with the test FCPCAG2 and test Migration Root CAs in CITE. But understand that the separate issuing CAs would be a long term migration strategy and the availability of those would be dependent on those managing the issuing CAs.

Discussion about the transition to the new FCPCAG2 and Migration Root and the time it will take to update all the relying party configurations.

- This is a requirement whether or not a subRoot is introduced. Since we are creating a new FCPCA with this key change and not doing the traditional key rollover with cross-certificates between the 2 roots, applications will need to be reconfigured and the FPKIMA will work with the community in determining how long the 2 parallel paths need to be maintained.
- The current FCPCA does not expire until the end of 2030, it just cannot issue any new 10 year CA certificates by the end of this calendar year. However, once all the current

CAs have a path to the new FCPCAG2 and the community tells us they have had sufficient time to push out the new path, the intention is to revoke the cert to the current FCPCA. Once all current CA certificates have been revoked or expired, the FPKIMA will publish a final long term CRL and decommission the current FCPCA.

- The preference is to work with the community to determine a few dates for issuing certificates from the new root CA and then revoking the old paths.

Scalability needs to be considered. If validation services are already operating near capacity and they suddenly get hit with validation requests from millions of citizen users who received signed emails there are costs for being able to scale to respond. However, this is not new functionality, SSPs should already be scaled to support validation of signatures.

What agency has the need for public trust of their digital signature? Treasury never sends emails to citizens. You will not see an email about your taxes or the COVID-19 payments. Todd sees no value in trying to have a root in the public trust stores for S/MIME because currently a lot of the email clients do not natively display the signature especially on mobile phones.

Whether S/MIME is natively supported now or not, there is a movement within industry to support and standardize on certificates issued for email protection. The CAB Forum is trying to start up an S/MIME Working Group and Apple, Google, and Microsoft are all very active in it.

Tim Baldridge brought up a potential issue with PIV and O365. When authenticating to O365 cloud service, using PKI, it expects the certificate to contain the email address associated with the user's outlook. Since PIV has separate certificates for Authentication and Digital signature and many agencies are not putting the email SAN in the Authentication certificate. Do we need to rethink this in the certificate profiles?

Tim Baldridge - We may not actually know who is using the trust anchor store for validation across the board.

Wendy – this is partially why Microsoft has been reluctant to remove the FCPCA from their trust store. They have not been able to determine the potential impact to all Microsoft customers.

Todd is concerned with the privacy impacts of having public trust for email signatures. When the email system validates the signature and requests certificate status from OCSP servers, the CA may be obtaining too much information about the user.

When Google natively supports S/MIME Todd would like to see documentation from Google providing the details on privacy.

Wendy speculated that Google might decide to simply not check the status or the certificate, similar to the way Chrome does not check the status of serverAuth certificates.

Tim Baldridge – systems are going to have to be reconfigured for the new FCPCAG2 anyway, so this is the right time to consider what changes should be made to the FPKI.

Impacts on Common Policy CP

The Common Policy CP update that is currently out for review already contains an update to allow for the use of SHA-384 with RSA, which was the recommendation from NSA.

A slight rewrite of the wording in section 6.3.2 would be required to allow the sub-roots to have a 20 year validity period that would allow them to issue 10 year CA certificates would be required.

Plans for cross-certification

No plan to issue cross-certificates between the current FCPCA and FCPCAG2.

Looking for input on whether we establish a separate Root for the FBCA or cross-certify with the FBCAG4.

Proposed Migration Plan

Testing
CITE can be available when Agencies are ready to test

- Do agencies have the ability to issue & test during current telework restrictions?

Production

1. Establish the FCPCA G2 and subordinate Migration Root
2. Issue CA certificates from the Migration Root to replace all required CA certificates currently issued by the FCPCA
3. Coordinate revocation of current CA certificates issued by the FCPCA allowing time for agencies to transition applications and environments to the new hierarchy
4. Once all current FCPCA issued certificates have been revoked, the FPKIMA will use a final long term CRL and decommission the current FCPCA

Wrap up

India Donald - This is for long term consideration. We are looking for feedback and additional questions. Please provide feedback by May 5, 2020 to the TWG listserv: fpki-ttips@listserv.gsa.gov and thank you for your participation.

Attendees

Note: If you have any additions/corrections to the attendance list please let us know. Some people may have only been on the phone, in which case we didn't see the name, or we may not have been able to identify the associated organization.

Name		Name	
Adam Mead		LaChelle Levan	GSA
Allan Turner		Larry Shomo	State
Amanda Williams		Lee Noble	
Andre Varacka	Verizon	Lisa Best	

Brando Meyer		Mark Delgado	DHS
Bryan Blakemore	DoD	Matt Ambs	DHS
Chris Benard	Pioneer	Matt Cooper	CertiPath
Cynetheia Brown	State	Matt Pooler	Treasury
Dan McKinney	FPKIMA	Mike Bliss	GPO
David Dixon	USDA	Mike Damoah	FAA
David Fisher	DHS	Ming Chan	Exostar
Derrick Head	State	Paul Newton	State
Donald Lopez	USDA	Patrick Garritty	Entrust
Donovan Demshock	FAA	Portia Cross	Treasury
Elston Holman		Ray Shanley	State
Fanny 'Elizabeth' Venegas		Rebecca Nielsen	DoD
Sandra I. Giraldo-Stables	State	Ridley DiSiena	NASA
Giuseppe Cimmino	DHS	Ryan Dickson	GSA
India Donald	FPKIMA	Santosh Chokhani	Libra
James Knapp	FPKIMA	Sherri Horner	State
James Napper	USPTO	Taconis Lewis	FPKIMA
Jeff Jarboe	Treasury	Terry Wyatt	NASA
Jeff Voiner	FPKIMA	Tim Baldridge	DoD
Jimmy Jung	Slandala	Toby Slusher	HHS
John DiDuro	FPKIMA	Todd Johnson	Treasury
Johnny Sais		Tom Connelly	FPKIMA
John Salgado	DoD	Tom Dwyer	
John Shuey	USDA	Tom Gindin	Treasury
Judy Spencer	CertiPath	Toma Smith	FPKIMA
Juston Ledoux		Tony Barrett	NASA

Kris Jones	Verizon	Wendy Brown	FPKIMA
Kyle Neuman	SAFE	Yared Taye	State