Technical Working Group (TWG) Meeting Notes - 7/9/2020

Agenda:

- Open Discussion to answer questions about the FCPCA Rekey Timing paper distributed on 6/18/20

India Donald welcomed the participants and provided an introduction to the meeting which included:

- Welcoming all participants
- We want to ensure we hear all your concerns in order to finalize the schedule for the rekey of the Federal Common Policy

Wendy Brown - The purpose of today's meeting is another open discussion to try to answer any questions or concerns about the proposed timing for the FCPCA Rekey explained in the paper distributed after the last TWG.

In particular we want to hear if the proposal to make the new root and cross-certificates between it and the FBCAG4 available via out of band means for 30 days prior to the issuing any other replacement certificates from the new FCPCAG2 meets agency requests for the time needed to push these out to relying parties, prior to encountering them in dynamic path discovery.

Discussion

Julia Ott - DoD is concerned that the FBCAG4 to Common cross-certificate won't be issued until Phase 2. This would result in people with paths to Common back to the DOD Interoperability Root CA, might be broken until Phase 2.

A: The FPKIMA will need to re-issue the cross-certificate from the FBCAG4 to the FCPCA prior to establishing the new FCPCAG2. This is because the current cross-certificate expires on 10/28/20. So a new certificate will be issued to ensure the path through the current FCPCA will work during that first migration phase for DoD and any other partner relying on that path.

Santosh Chokhani asked about the need to revoke the certificates from the current FCPCA. Decommissioning the CA and issuing a long term CRL is not as good as having all certificates issued to it revoked and having it removed from all trust stores.

A: The intent is to request all relying parties to remove the old FCPCA from their managed trust stores after they are sure the new FCPCAG2 is properly installed in the managed trust store. The 6 months or so of having parallel paths available is to give people time to make the transition. The FPKIMA will be coordinating with the DHS/CISA similar to what was done when everyone was asked to ensure they had the FCPCA in their trust stores when we thought Microsoft would remove it from their public trust store, in order to get the word out.

When we have confirmation that most agencies are ready we will start the decommissioning process. That will include:

- Swapping the cross-certificate from the FBCAG4 to the FCPCA for the one from the FBCAG4 to the new FCPCAG2 in the FPKIMA's repository
- Revoking the certificates issued from the FCPCA
- Revoking the certificate issued to the FCPCA
- Issuing a long term CRL
- Decommissioning the CA and notifying Microsoft and Adobe

The timing of swapping the cross-certificates from the FBCAG4 to the FCPCA to the one to the FCPCAG2 is critical, so there will not be a discoverable path that might cause a looping linkage between the two. The instructions that will be communicated when the root and cross-certificates are made available will include information about only having one of those trusted at a given time in trust stores. When an application is sure that the path can be built to the new root, they should distrust the old cross-cert and replace it with the new one.

Todd Johnson - Looping is not an issue, it is more an issue of unpredictable path selection. If given a choice of multiple paths the Axway often chooses the wrong path. This is why we need a 2-week notification . The plan and previous notifications are not detailed enough - we need the exact date an action will happen. Communication is key! Even if the initial communications are draft and get tightened up near execution. It sounds like the 6-month migration plan will work fine for all parties.

Tim Baldridge - What is the plan for incorporating the new Common with the Microsoft trust store?

A: The plan currently is not to ask Microsoft to include the new root and notify them when the current Common has been decommissioned.

Tim stated he was in favor of that approach and also in favor of the early-notification and cross-certification approach proposed.

Donovan Demshock indicated FAA was also in favor of the 30 days to trust the new root certificate and configure validation solutions in preparation for the use of new certificate chains in advance.

Todd stated he was concerned with web applications that might not get updated correctly, they might be serving the entire path to the current trust anchor and the client responds with a path to the new trust anchor. Getting the word to all of these implementors will be crucial.

A: We will be trying to spread the word as widely as possible using the DHS/CISA but we are requesting help from everyone on the call to make sure the instructions get to whoever needs them within your organization. In addition if Todd or anyone else develops instructions for web application or other trust store management we would appreciate getting

copies so we can share with other agencies or post as notifications on idmanagement.gov if appropriate.

Raghu Vallurupalli - Asked to be able to test the changes in a test environment first. He supports the Fiscal Services and their Secure Payment System which accepts users from all agencies using all 3 certificates on a PIV or CAC and he would really like to be able to test as many agency credentials as possible in the test environment so there are no surprises when users need the SPS to work in production.

A: CITE is available, but there are not enough of the issuers and affiliates participating in the CITE environment. Currently only Treasury, DoD and DigiCert have CA certificates from CITE. Todd added that the test CAC they had from DoD have expired. Tim said he could assist in getting Treasury connected to the correct people within DoD to get new test cards if they need the assistance. The FPKIMA requests that organizations that choose not to participate in CITE explicitly state they will not participate when they are asked for a p10 for their test environment.

Tim - Recommends that agencies should have an internal OCSP responder for all known CAs but it is difficult to locate the correct URLs for all the issuing CAs. The system notifications were supposed to help address that, but it is a manual process.

Todd has developed a utility to help with that, it is publicly available at https://apidoc.fpki.io/. Currently it is updated manually and is a personal effort. However, Todd hopes to someday move it to a government asset.

There was a discussion about the heuristics used by Microsoft in determining the certificate path. Some stating it chooses the path with the latest date, or the one with the most information or most constraints. The best way to manage the path selected is by distrusting cross-certificates that would build a longer path to an unexpected root.

Tim suggested we should have a stated rule that no PKI cross-certified with the FBCA can have its root in a public trust store so we do not run into the case where Microsoft chooses that root over the FCPCAG2 due to it being a newer or longer path.

Andre Veracka asked if we would require the SSPs to rekey their intermediate CAs when they get a new certificate from the new FCPCAG2.

A: No, the FPKIMA intends to issue the replacement certificates with the same expiration date as the current certificate and expects them all to be with the same key. Anyone requiring a new CA certificate from the FCPCA in the near future should let the FPKIMA know as soon as possible.

Todd asked, just to be sure there are no architectural changes planned with the rekey.

A: Correct, we heard that request at the last meeting.

Summary

The plan is

- Re-issue the cross-certificate from the FBCAG4 to the FCPCA prior to the rekey so it will not expire during the migration to the new root.
- Provide the new FCPCAG2 root certificate and cross-certificates between it and the FBCAG4 via out-of-band (ie not dynamically discoverable via AIA/SIA) for approximately 30 days prior to additional certificate issuance
- Only 1 FBCAG4 to Common cross-certificate will be available via AIA at a time and the replacement of the one to the FCPCA will not happen until the FPKIMA has confirmation most everyone is ready
- Affiliates and agencies can manage the transition within their own trust stores by manually adding the new certificates and distrusting the older ones.

If anyone has additional questions or concerns please contact the FPKIMA at fpki-help@gsa.gov.

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.

Adam Jones - DHS	Larry Shomo - State
Andre Varacka - Verizon	Mark Delgado - DHS
Brittany Davis - SSA	Matt Ambs - DHS
Cynethia Brown - State	Matt Cooper - CertiPath
Daniel Ridings - DoD	Matt Meyer - SSA
Dan McKinney - FPKIMA	Melissa Nimmo - Sandia Labs
David Fisher - DHS	Mike Bliss - GPO
Derrick Head - State	Paul Newton - State
Donovan Demshock - FAA	Santosh Chokhani - DoD
India Donald - FPKIMA	Subrahmanyam Peddibhotla
James Knapp - FPKIMA	Tim Baldridge - DoD
Jamie Wasserman - SSA	Tim Stroh - USDA
Jeff Jarboe - Treasury	Tim Wilson - DoD
Jimmy Jung - Slandala	Todd Johnson - Treasury
John DiDuro - FPKIMA	Tom Connelly - FPKIMA
Josh Coffman - USDA	Wendy Brown - FPKIMA
Judy Spencer - CertiPath	
Julia Ott - DoD	