Technical Working Group (TWG) Meeting Notes - 6/2/2020

Agenda:

- Proposed Architecture -
  Open Discussion

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

- Do not be concerned about changes to the current cost recovery for FPKIMA operations. We have been operating and maintaining the trust infrastructure for the same budget for the last 10 years.
- We have also been operating within policy. We view the proposed changes as continuing to operate within that same policy.
- We are taking a phased approach to the proposed architecture which will begin to build flexibility into the architecture, but may not require changes to current issuing CAs for the next 3 to 5 years
- We have heard your concerns about wanting to see the proposal in writing in order to provide more concrete feedback and are currently developing a whitepaper to address them.

Wendy Brown: We have no formal presentation for today, the agenda is to be an open discussion to continue getting your feedback on the proposal. But first a recap of what we have heard so far. We received feedback from 5 agencies. DoD, DHS, USDA, NASA, SSA. We are not looking for formal decisions from agencies at this time, but just trying to get input for additional discussion about a long term strategy. Summarizing what we have heard so far:

- There is wide use of PIV signature cert for signing PDFs - mostly for use within the government, but some with external partners - a desire for signatures on PDFs to be trusted by the public
- Some use of signed email within gov or to mission partners - not so much yet with citizens
- Limited encrypted email but when used, internal to gov or mission partners
- Not much support for splitting issuing CAs related to certificates on PIV
- Possible interest in support of cross-agency NPE, possible interest in splitting NPE from PIV
- Treasury doesn't ever send email to citizens but we have heard or seen at least 10 examples of government to citizen emails: including things like reminders to check SS information, opt-in like informed delivery from USPS, Medicare, TSP & VA emails that may go both to employee and private emails

Given that input, we would still like to take advantage of the rekey to move to an architecture that will provide more flexibility moving forward. The initial proposal allows all CAs with a direct relationship with the FCPCA to move intact to the new key/architecture by receiving a

CA Certificate from the Migration SubRoot. This allows over time for additional subRoots as agencies are ready, for separating cross-government NPE certificates from People/PIV. Instead of trying to push all signature/encryption certs from PIV to separate issuing CAs, we propose the possibility of a separate Hierarchy for public trust signature/email potentially for organizational emails that might be sending the types of public facing emails we have seen. We recognize these emails are not signed today, and some people believe many of the popular email programs do not currently validate/display signatures, but there is a move within industry to more widely support S/MIME.

Open discussion

Todd Johnson: Concerned about operational impact. Can we separate changes to the architecture from the rekey.

Jamie Wasserman: Major concern for SSA due to the current telework situation. There is concern that any changes may impact employees' ability to use their PIV for access.

Todd Johnson: Treasury has put together a presentation with a list of concerns, physical servers, business lines, and customer concerns due to financial services Treasury provides to the full government. We are cognizant of our own credentialing. But our business lines are concerned with the financial operations Treasury provides that service all agencies. They accept PIV authentication from all the agencies. PKI is used to support all of that like sending out 50K SS checks, cards to make same day payments, there are 4 major payment applications., 100% collection, gogo payments use PKI to manage.

Is there any way to focus on rekey without injecting additional CAs in the path? If we do not have a plan in place, we will have an issue operationally. The sub root adds no value at this time. We can address it sometime next year.

Jeff Jarboe: The presentation with a counter proposal, Todd referred to is being reviewed to get Treasury full approval, prior to providing it to the TWG. They are concerned that the proposed changes will require Treasury to go from 5 issuing CA's to 21 issuing CAs. However, it sounds like that may have already changed, if the signature certs do not need to be issued from a separate CA

Todd: Insert a new root above the existing common root at a later time The budget is already approved for 2020-2021.

Jamie Wasserman: Why the sense of urgency?

Todd: How about we rekey this year while maintaining as is until next year.

Matt Myers: I support Todd's position.

Todd: When can we start testing in CITE?

Wendy: As we said last time, CITE is ready, we asked agencies to let us know when they were ready to accept a CA certificate from CITE. We would still like to introduce the sublayer which will give us the flexibility to add additional sub roots at a later time for example to enable a public trust option.

Santosh: I have to see the document before commenting. Rather have a document we can review. I don't know what it means to layout the architecture changes first then make a decision.

Todd: Super helpful to see examples of what intermediate and subroots are doing. Naming constraints. I have been working with software that had some bugs when there are Subject name and name constraint case sensitivity differences. Challenges with agency's credentials.

We are very highly academic when it comes to certificate extensions. Switching out new root CA, making a path back to the CA

Santosh: I can't make any commitment without looking at something. Again a request for a white paper.

Wendy: We are working on a white paper, but were hoping to get additional input for the paper in terms of needs and uses from agencies as part of the input for that paper.

Todd: Like to access testing in CITE. Intent to inject the subroot to observe it. Is there any kind of diagram or artifact for the new CA or root. Plan the change and put it through change control on their side. We only see Treasury and DoD in CITE now.

Wendy: Right, it would be more useful if additional issuing PKIs participated in CITE and could make test certificates available for all.

We would appreciate additional input from the questions we sent out.

India Donald - We hear you that the agencies are not prepared to fully support the move to a new architecture right now, even if any operational impacts to issuing PKIs would not be required for 3 to 5 years. Because of the Pandemic, we are prepared to just do the rekey in October, with all new CA certificates issued within 3 weeks after that, and a 6-month timeline after the rekey for full migration to the new FCPCAG2.

We will continue working on the white paper for future evolution/maturation of the FPKI architecture with the expectation these changes will not occur until later.

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
Alex Graves - State	Mark Delgado - DHS
Andre Varacka - Verizon	Maryam Hansen - DoD
Bobbie Brown - HHS	Matt Ambs - DHS
Brando Meyer -	Matt Cooper - CertiPath
Brian Schuler - NASA	Matt Meyer - SSA
Chris Benard - Pionner RX	Mike Bliss - GPO
Cynetheia Brown - State	Mike Meyer - ICFI
Dan McKinney - FPKIMA	Paul Newton - State
David Dixon - USDA	Patrick Garritty - Entrust
David Fisher- DHS	Phil Simon - FPKIMA
Derrick Head - State	Portia Cross - Treasury
Donovan Demshock - FAA	Ray Shanley - State
Giuseppe Cimmino - DHS	Ridley DiSiena - NASA
India Donald - FPKIMA	Ryan Dickson - GSA
James Knapp - FPKIMA	Sandra I. Giraldo-Stables - State
Jamie Wasserman - SSA	Santosh Chokhani - DoD
Jeff Jarboe - Treasury	Taconis Lewis - FPKIMA
Jimmy Jung - Slandala	Terry Wyatt - NASA
John DiDuro - FPKIMA	Tim Baldridge - DoD
John Salgado - DoD	Tim Stroh - USDA
(JT) John Taylor - DoD	Todd Johnson - Treasury
Josh Coffman - USDA	Tom Connelly - FPKIMA
Judy Spencer - CertiPath	Toma Smith - FPKIMA
Juston Ledoux -	Wendy Brown - FPKIMA
Kyle Neuman - SAFE	Yared Taye - Stata