



Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

**Wednesday
June 11, 2014**

1:00 p.m. – 2:30 p.m.

General Services Administration 1800 F Street Northwest Washington, DC

1:00	Welcome & Opening Remarks	Chris Loudon
1:05	Ozone Server PDVAL Report	Kenneth Myers
1:15	FPKI CDN Project	Giuseppe Cimmino
2:25	Wrap-up and Adjourn the Meeting	Chris Loudon

FPKI TWG June 11, 2014 Meeting Minutes

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or not identified their organization.

Name	Organization
Ambs, Matthew	DHS
Baldrige, Tim	DoD
Ball, Mike	Electrosoft
Barry, Jeff	Certipath
Blanchard, Deborah	Verizon Business
Bolin, Neil	Certipath
Boss, Daniel	USDA
Brown, Wendy	FPKIMA
Burke, James	DoJ
Camat, Aldrich	DHS
Carson, Mike	Telos
Chokhani, Santosh	DoD
Cimmino, Giuseppe	FPKIMA
Cunningham, Robert	VA
Davies, Jim	DHS
Diduro, John	FPKIMA
Disiena, Ridley	NASA
Erickson, Shari	USDA
Evans, Paul	DoE
Gerhard, Andrew	Verizon Business
Gray, Michael	Education
Hai Ja, Curtis	Transportation
Hannan, John	GPO
Head, Derrek	State
Jackson, Angela	USPS
Jeffers, Daniel	DoD
Jarboe, Jeff	State
Johnson, Todd	Treasury
Kandela, Savith	FPKIMA
Kluegel, Lynn	DoE
LeVan, LeChell	DHS
Louden, Chris	FPKIMA

FPKI TWG June 11, 2014 Meeting Minutes

McBride, Terry	Treasury
McCloud, Dennis	HHS
Morrison, Scott	DoJ
Myers, Kenneth	FPKIMA
Page, Ryan	PM-ISE
Race, Steve	TSCP
Salgado, John	DoD
Sambit, Dash	Symantec
Shorter, Scott	Electrosoft
Skordinski, Steve	TSCP
Slusher, Toby	HHS
Smith, Thomas	John Hopkins APL
Spainhour, Ben	DoD
Spence, Willie	Treasury, IRS
Stone, Wayne	NASA
Talley, Janet	FAA
Thakkar, Jay	DoD
Thomas, Michele	USDA
Townsend, Paul	Mount Airey
Walker, Dave	DHS
Wallace, Carl	DHS
Ward, Keith	TSCP
Wasserman, Jamie	SSA
Weiser, Russ	Verizon Business
Woods, Dan	Treasury
Woodford, Christopher	Treasury
Wyatt, Terry	NASA
Zeimat, Adam	USDA

Agenda Item 1 - Welcome and Opening remarks (Chris Loudon)

The FPKI TWG met at GSA, 1800 F Street Northwest, Washington, DC. Mr. Chris Loudon (Supporting FPKIMA) opened the meeting by thanking everyone for attending and stated that Ms. Darlene Gore would not be able to attend due to a sudden conflict. He reviewed the agenda and then introduced Mr. Kenneth Myers (Supporting FPKIMA) to present the Ozone Server PDVAL report.

Agenda Item 2 - Mount Airey Ozone Server PDVAL Report (Kenneth Myers)

Mr. Myers opened the topic by introducing the report and then introduced Mr. Paul Townsend from Mount Airey. Mr. Townsend started with a functional description of the Ozone Server. It operates by acting as a verification plug-in to an application. It makes a verification decision based on the certificate asserted from the user against a set of proofs created from an authoritative source designated by the Server. The proof can be either static or dynamic and is delivered to the Ozone Server which makes a verification decision. The decision is asserted to the application to allow access based on the presented credential. One unidentified caller asked if the Ozone Server will be deployed as publicly accessible. Chris Loudon responded no, the FPKIMA tests commercial product capabilities against NIST PKITS guidelines to create a list of approved products to be used in the FPKI. It is up to the individual agencies to contact the company and obtain a service contract for use. Mr. Myers concluded the topic with the test results. The Ozone Server passed all required and optional tests except for one issue in the optional name constraints tests. In these tests, an error message created stated the error was with the subject alternative name even when the subject alternative name wasn't what violated the name constraints. The optional test criteria only test for the appropriate result and not the error message. In all tests, the Ozone Server successfully returned the appropriate response. No comments or concerns were raised by those in attendance. The next step is to forward the report and validation report to the FPKIPA Chair and then add the product to the PDVAL Product List.

Mr. Myers introduced Mr. Giuseppe Cimmino (Supporting FPKIMA) to present a brief and discussion on the FPKI Content Delivery Network Project

ACTIONS:

1. An FPKIPA approval letter will be drafted and sent to the FPKIPA Chair, Deborah Gallagher, for signature and acceptance into the FPKI PDVAL Product List.

Agenda Item 3 – FPKI CDN Project (Giuseppe Cimmino)

Mr. Cimmino opened the topic with a brief introduction of general CDN operations. He explained the concept of origin and edge servers and also the general performance and security enhancements possible with a CDN. He then moved onto the detailed technical brief of the FPKI CDN Project. Currently, the FPKI CRLs are hosted from an HTTP

repository with two static IP addresses. The project proposes to transition the HTTP capability of the FPKIMA repository to a CDN for performance and security enhancements. Mr. Cimmino outlined the three options that are currently being considered being (1) a full move to CDN, (2) a limited CDN option with a block of IPs for those Entities with tight egress controls and (3) a hybrid option combining both a CDN option and retaining the current HTTP repository for those Entities that cannot support the dynamic nature of a CDN.

An unidentified caller asked if there was a plan for stale content on CDN. Mr. Cimmino responded the CRLs are published twice a day and the FPKIMA is looking at future enhancements to the HTTP cache headers to guarantee a system that cached the content could determine if the data is up to date based on the content of the CRL. CDNs are used today for CRL and OCSP delivery by both government and commercial PKIs. If an emergency CRL is needed, the FPKIMA can push it to the CDN which can flush the outdated content on their network in a magnitude of minutes. Cache flushing is a well-known requirement and well supported by commercial CDN vendors.

There was a question if the CDN would service HTTPS. The FPKIMA does not serve over HTTPS today because the content is already digitally signed.

Todd Johnson (Treasury) asked how many edge servers would be located outside the US because there might be the potential for traffic analysis. If a CONUS based users hits an OCONUS server someone could analyze what traffic is hitting which server for authentication methods and use it for advanced targeting. Mr. Cimmino responded CDNs have different "maps" and we can choose which ones we want. The issue there is two-sided. Traffic analysis could be done on OCONUS origin servers as well. Whether CONUS traffic would ever be sent OCONUS in the case of all US servers being unavailable is an interesting edge condition and we can ask the vendor if this has come up and if we can require a geo-based map to the same region i.e. CONUS to CONUS.

In response to a question whether the CDN would support DNSSEC, we would support DNSSEC from the root though .gov to fpki.gov, but we didn't find CDN vendors who did dynamic signing. We would support DNSSEC up to the return of the CName to the CDN. The follow-up question was whether this would be a violation of the requirement to support DNSSEC for government systems. There are a number of government systems using CDNs today, the White House being one of them, but this is something the FPKIMA will investigate further.

Matt Ambs (DHS) asked if the hybrid approach is used would the dual existing HTTP servers exist indefinitely. Mr. Cimmino responded they would exist as long as they are needed. The FPKIMA would continue to support the current setup because regardless of the CDN option, the FPKI's HTTP server would always be needed to be the origin server for the CDN.

There was a contracting question about the decision to use Akamai. This isn't a contracting discussion; this is a technical discussion on Entities ability to configure their systems to use a CDN.

There was a question how to support an agency that is using DNS resolution provided through another provider, like openDNS or a commercial vendor. If that agency also has strict egress controls, the limited map option is the only option. The limited option, meaning a limited set of IPs is used in the CDN. This is a specific issue with the Federal Reserve Board (FRB), but may apply to other entities with strict egress and outbound traffic firewall policies. Todd Johnson (Treasury) asked the FRB representative to get with him offline as it might be a Treasury only issue. Giuseppe remarked that the FRB currently uses a limited map configuration of the Akamai CDN through their current vendor, Symantec.

Jim Davies (DHS OneNet) asked if there is any advice on configuring non-proxy aware devices. A non-proxy aware device is a service where the application doesn't know there is a proxy http service. The Proxy service usually provides a many to one relationship, the CDN would create many-to-many relationships. This might be solved with a rule that bypasses the proxy service for given content such as p7c files and CRLs. Could do rules based on content for CRLs. Would the proxy allow access to the edge server from the domain resolvers? Mr. Cimmino responded adding a CDN shouldn't impact whether you're using a proxy or not. Mr. Cimmino said he would set up a separate call with DHS to fully understand and resolve this question.

Dave Walker asked if there is a technical document we can take a look at it for our network engineers? Mr. Cimmino responded there is the presentation that was sent out in the meeting announcement and the intro presentation that was also presented to the FPKIPA. Mr. Cimmino will send both presentations to the participants if they send their emails. Once the CDN options are approved, details will be distributed to the community. Agreements will be sent to those with egress controls to properly set up access to ensure operational continuity. The FPKIMA will also send out implementation time lines after approval, but there isn't a firm date of when an option will be decided.

ACTIONS:

1. Follow-up with Akamai on geo-based traffic analysis for advanced targeting.
2. Research DNSSEC support on CDNs.
3. Set-up call with DHS to discuss non-proxy aware devices and CDNs.
4. Send any additional questions/concerns to giuseppe.cimmino@protiviti.com
5. Distribute presentations to participants who send their contact information.
6. Distribute technical documents and option descriptions to participants after FPKIPA approval is complete.

Agenda Item 4 - Wrap-up and Adjourn Meeting (Chris Loudon)

Mr. Loudon thanked everyone for attending and adjourned the TWG meeting at approximately 2:00 PM EST.