



Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By SRA International

**Wednesday
July 8, 2015**

1:00 p.m. – 3:00 p.m.

Teleconference

<u>Time</u>	<u>Topic</u>	<u>Presenter</u>
1:00	Welcome & Opening Remarks	Ola Bello
1:05	Microsoft Certificate Reputation Program	Anoosh Saboori
2:00	DHS SSL Wildcard Certificates in Support of Microsoft SharePoint 2013	Mike Ambs Larry Shomo
2:45	TWG Updates	Kenneth Myers
3:00	Adjourn	Ola Bello

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 may not have identified their organization.

Name	Organization
Ambs, Matt	DHS
Anand, Neha	Symantec
Baldridge, Tim	DoD
Bello, Ola	GSA FPKIMA
Blanchard, Debb	ORC
Brown, Wendy	GSA FPKIMA
Cimmino, Giuseppe	GSA FPKIMA
Chokani, Santosh	CygnaCom
Cotton, Michael	Microsoft
Johnson, Todd	Treasury
Jung, Jimmy	State
McBride, Terry	Treasury
McLain, Drew	Treasury
Mill, Eric	GSA
Myers, Kenneth	GSA FPKIMA
Robinson, Buddy	Treasury
Saboori, Anoosh	Microsoft
Salgado, John	DoD
Shomo, Larry	DHS
Spence, Willie	IRS
Weaver, Kurt	Treasury
Wyatt, Terry	NASA

Welcome and Opening remarks (Ola Bello)

The FPKI TWG met to receive two information presentations which could impact the Federal PKI (FPKI). Mr. Kenneth Myers opened the meeting and thanked everyone for attending and added Mr. Ola Bello, TWG Chair, was delayed by another meeting, but would join shortly. He then turned it over to Mr. Anoosh Saboori, Microsoft, to discuss the first agenda item.

Agenda Item 1 – Microsoft Certificate Reputation Program (Anoosh Saboori)

Mr. Saboori introduced the agenda topic with a general overview of the PKI threat landscape and then a description of the Microsoft Certificate Reputation or Cert Rep program. The current PKI threat landscape includes fraudulent certificate use on fake and real web sites, unreliable certificate revocation list (CRL) checking, and applications ignoring CRL issues. The intent of the Cert Rep program is to monitor public PKI certificates for anomalies and other possible issues to protect end users and certificate authorities (CAs). The program currently encompasses three components:

- 1) Microsoft Trust Store Program for trusted root CA certificates.
- 2) A blacklist for identifying untrusted intermediate certificates. This blacklist is automatically pushed to Windows computers which are configured to request it every 16 hours. This feature is turned on by default. One of the TWG members asked about Window client and servers which have automatic updates turned off for security reasons. Mr. Saboori replied the only way to receive the blacklist updates is to have the auto update feature enabled. The automatic update is controlled via a registry setting, Mr. Saboori will provide additional information about this configuration to the TWG at a later date.
- 3) The smart screen feature included in Windows Internet Explorer to capture SSL certificates for analysis and notification.

Mr. Saboori then explained the smart screen feature from multiple member questions. The smart screen feature is a data collection point in Internet Explorer which captures SSL certificates that validate to a third party root. Back end Microsoft servers analyze the certificate for anomalies and verifies it has not been issued from a compromised CA. Microsoft analyzes the certificates looking for patterns that may indicate issues and learn to distinguish between false positives or actual issues. Microsoft is concerned with the tradeoffs between the need to perform this analysis and the requirement to preserve the privacy of users. Website owners are notified through the BING Webmaster Tool and Microsoft is working on other forms of notification for CA operators to include possible information sharing agreements as well. Browser clients do not receive any feedback at this time. Mr. Todd Johnson asked if the smart screen feature also captures internal certificates and who is told if an anomaly is found. Mr. Johnson was concerned smart screen was exfiltrating private certificates that were not meant to be publicly analyzed. Treasury issues internal certificates under the Treasury root which has a path to Common Policy which is in the Microsoft Trust Store. Mr. Johnson also

asked if Microsoft has analyzed the certificates for weak keys and if that analysis could be shared? Mr. Saboori did not have this information and would follow-up with the TWG when he finds it and if he can share the information. Mr. Myers thanked Mr. Saboori for presenting the topic.

Agenda Item 2 – DHS SSL Wildcard Certificates in Support of Microsoft SharePoint 2013 (Matthew Ambs)

Mr. Larry Shomo, DHS, opened the topic with a background of the situation. DHS has invested in Microsoft SharePoint and with the latest upgrade to SharePoint 2013 one of the system requirements is to issue SSL wildcard certificates. This alleviates the need to issue hundreds of individual certificates to each SharePoint website. DHS also has an internal policy that all certificates are issued from a DHS CA under Common Policy. Mr. Matthew Ambs, DHS, continued the topic to add the current Common Certificate Policy (CP) is very vague around SSL and device certificates, but does not specifically state a wildcard certificate is not allowed. Microsoft recommends the wildcard "*" is more than one level down from the department root for sufficient risk mitigation (i.e. *.sharepoint.dhs.gov). DHS was looking to the TWG on a consensus to the best technical mitigation to use SSL wildcards which are policy compliant.

DHS is proposing the FPKIPA update section 3.11 and 3.1.5 of the Common Policy CP to specifically address SSL wildcards and recommends the wildcard be placed at least three levels down from the top level domain (i.e. *.sharepoint.dhs.gov) for proper risk mitigation. DHS shared their current proposal which includes the use of 6 levels and registering a DNS A Record for the FQDN following the wildcard. A discussion around the use of the subjectAltName (SAN) versus the subject DN followed, as well as the tradeoffs between issuing a certificate to each server vs a single certificate issued to an entire server farm with a single DNS A record.

Mr. Tim Baldrige, DoD, added since the current policy does not state wildcards are not allowed, DHS can issue SSL wildcard certificates that they think meet the uniqueness criteria as set forth in the Common Policy CP. Mr. Baldrige asked the group if anyone objected to the TWG sending a formal request to the FPKIPA to have the Common Policy CP updated to address wildcard certificates. No one objected to the motion. Mr. Bello took the group consensus as an action and thanked DHS for presenting.

ACTION: The TWG will send a formal request to the FPKIPA to update the Federal Common Policy CP to address SSL wildcards.

Agenda Item 3 – TWG Updates

- 1) **GSA CyberSprint** – In support of the OMB directed CyberSprint, the FPKIMA is assisting GSA in identifying gaps in FPKI services. A survey was distributed to the FPKIPA and ICAMSC listservs for any suggestions of what services are needed or not offered in the FPKI. If you have any suggestions, please send your responses to fpki-help@gsa.gov or the TWG listserv. Mr. Baldrige added he is co-chair of the OMB Multi-Factor Authentication (MFA) Tiger Team and the White House is taking this initiative very seriously. Any input on how to enable PIV for (MFA) to share is greatly appreciated.
- 2) **OMB HTTPS Memo** – OMB released a new memo requiring all public facing websites to use SSL certificates by end of calendar year 2016. Mr. Johnson added the FPKIPA should coordinate with OMB to address those public websites which cannot have SSL certificates due to availability concerns such as HTTP repository pages. No action was taken at this time.

Adjourn

Mr. Bello thanked the presenters and everyone who participated for the lively discussion and closed the meeting.