Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

October 25, 2011

9:00 a.m. – 12:00 p.m.

9:00	Welcome & Opening Remarks Introductions	Matt Kotraba
9:05	Microsoft Timestamp Authority Position Paper Update	Wendy Brown
9:15	Plans for Encryption Certificate Lookup & Retrieval Testing	Wendy Brown
9:20	Microsoft Path Building Anomalies Design Change Request Update	Matt Kotraba
9:30	Trust Store Management Guidance • Logistics for developing guidance	Matt Kotraba

9:40	• Review and discuss research findings
	  ○ ICAM Roadmap Guidance
	  ○ USGCB / FDCC Settings
	  ○ DoD PKE Guidance	

10:30	• Recommendations Paper Outline & Writing Assignments
	  ○ Problem Statement
	  ○ Current Status of Federal Guidance
	  ○ Recommendations	

12:00	Adjourn Meeting	Matt Kotraba

Attendance List

Organization Supported	Name	Email	P-Present/ T-Teleconference
CertiPath	Jeff Barry	jeff.barry@certipath.com	P
Department of Defense (Contractor)	Curt Spann	spann_curt@bah.com	T
Department of Defense (Contractor)	Dan Jeffers	jeffers_daniel@bah.com	T
Department of Defense (Contractor)	Santosh Chokhani	schokhani@cygnacom.com	P
Department of State	Deb Edmonds	edmondsdd@state.gov	T
DHS	Larry Shomo	Lawrence.Shomo@associates.dhs.gov	P
DHS	Neal Fuerst	Neal.Fuerst@ASSOCIATES.HQ.DHS.GOV	T
DHS	David Fisher	David.Fisher@ASSOCIATES.HQ.DHS.GOV	T
DigiCert	Scott Rea	Scott.Rea@DIGICERT.COM	T
DOE	Michele Thomas	Michele.Thomas@hq.doe.gov	T
DOJ	Scott Morrison	Scott.k.morrison@USDOJ.GOV	T
Entrust	Gary Moore	gary.moore@entrust.com	T
eValid8	Jim Schminky	james.schminky@evalid8.com	P
GSA	Darlene Gore	darlene.gore@gsa.gov	T
GSA	Jeff Voiner	jeffrey.voiner@gsa.gov	T
GSA	Albert Ingram	albert.ingram@gsa.gov	T
GSA (Contractor)	Brant Petrick	Brant.Petrick@gsa.gov	P
GSA (Contractor)	Chris Louden	chris.louden@pgs.protiviti.com	P
GSA (Contractor)	Dave Shepherd	DSHEPHERD@lmi.org	T
GSA (Contractor)	John DiDuro	john.diduro@pgs.protiviti.com	P
GSA (Contractor)	Matt Kotraba	matthew.kotraba@pgs.protiviti.com	P
GSA (Contractor)	Wendy Brown	wendy.brown@pgs.protiviti.com	P
GSA (Contractor)	Dave Silver	dave.silver@pgs.protiviti.com	T
GSA (Contractor)	Jeff Jarboe	Jeff.jarboe@pgs.protiviti.com	P
HHS	Toby Slusher	tus8@CDC.GOV	P
NRC	David Sulser	david.sulser@nrc.gov	P
PTO	Amit Jan	Amit.Jain@USPTO.GOV	T
Safe-Biopharma	Gary Wilson	gwilson@SAFE-BIOPHARMA.ORG	T
Treasury	Dan Wood	Daniel.Wood@treasury.gov	P

Agenda Item 1
Welcome & Opening Remarks
Introductions--All Attendees
Matt Kotraba and Chris Louden

The Federal Public Key Infrastructure (FPKI) Technical Working Group (TWG) met at Protiviti Government Services, 1640 King Street, Suite 400, Alexandria, VA. Matt Kotraba called the meeting to order at 9:00 a.m. EST and introduced those in person and via teleconference.

Agenda Item 2
Microsoft Timestamp Authority Position Paper Update
Wendy Brown

Wendy Brown informed the TWG that Microsoft responded to the FPKI TWG Timestamp Server Authority (TSA) Position Paper and Microsoft is still moving forward with the TSA requirement to maintain the codeSigning Extended Key Usage (EKU) property in the Windows Root Certificate Program. The FPKI Policy Authority (FPKIPA) Chair submitted a 180-day extension request to Microsoft to obtain additional time for the FPKIPA to address the TSA requirement.

Matt Kotraba shared the results of the survey sent to the FPKIPA on the usage of code signing certificates. The survey revealed several findings:

- The Department of Defense (DoD) does issue code-signing certificates for use on code shared externally (however DoD is not directly under Common Policy CA) and that DoD uses a Verisign TSA.
- The United States Postal Service uses commercial code-signing certificates
- The Department of Treasury shares externally with financial institutions along with distributing the Treasury Root.

The TWG agreed that more information on agency use of code-signing certificates is necessary to gauge the full impact of dropping the codeSigning EKU from Common Policy.

Use of the FPKI Community Interoperability Test Environment (CITE) to test the effects of dropping the codeSigning EKU from the Windows Trust Store was discussed. However, there is not enough known to effectively model and simulate the FPKI usage of code signing, and therefore the results of the test may not give an accurate depiction of what will occur in production environments.

ACTIONS

1. Matt Kotraba will inform Deb Gallagher that there are FPKI members who currently have a TSA as one solution to this issue..

Agenda Item 3
Plans for Encryption Certificate Lookup & Retrieval Testing
Wendy Brown

Wendy Brown informed the TWG that testing of the Transglobal Secure Collaboration Program (TSCP) Secure Email (SE) solution for public encryption certificate lookup and retrieval (*discussed at the September 2011 TWG*) will take place after the TWG completes the *Trust Store Management Guidance* document. Certipath, NRC, and NASA have already volunteered to participate in the test. TWG is actively seeking additional volunteers who are willing to assist with this effort.

ACTIONS

- None.

Agenda Item 4
Microsoft Path Building Anomalies Design Change Request Update
Matt Kotraba

Matt Kotraba provided an updated status of the NASA and NRC open tickets with Microsoft regarding “Microsoft Cryptographic Application Programmer Interface (CAPI) Path Building Anomalies” (*discussed at the September 2011 FPKI TWG*). NASA needs assistance in building their business case with Microsoft. The DoD has also experienced similar path building issues where Microsoft selects an inappropriate chain. NASA is looking for impact statements which specify the impact to the affected organizations, the number of users this issue affects, and specific examples to include screen shots or logs that capture examples of incorrect paths being selected.

Santosh Chokhani informed the TWG of a DoD VIP session with Microsoft involving a 4-star General. This issue is on the list of top DoD issues with Microsoft products. Dan Jeffers indicated the DISA DoD PKE group does not have its own Premier support agreement with Microsoft and instead must rely on the Services and Agencies within the DoD to submit tickets to Microsoft. .

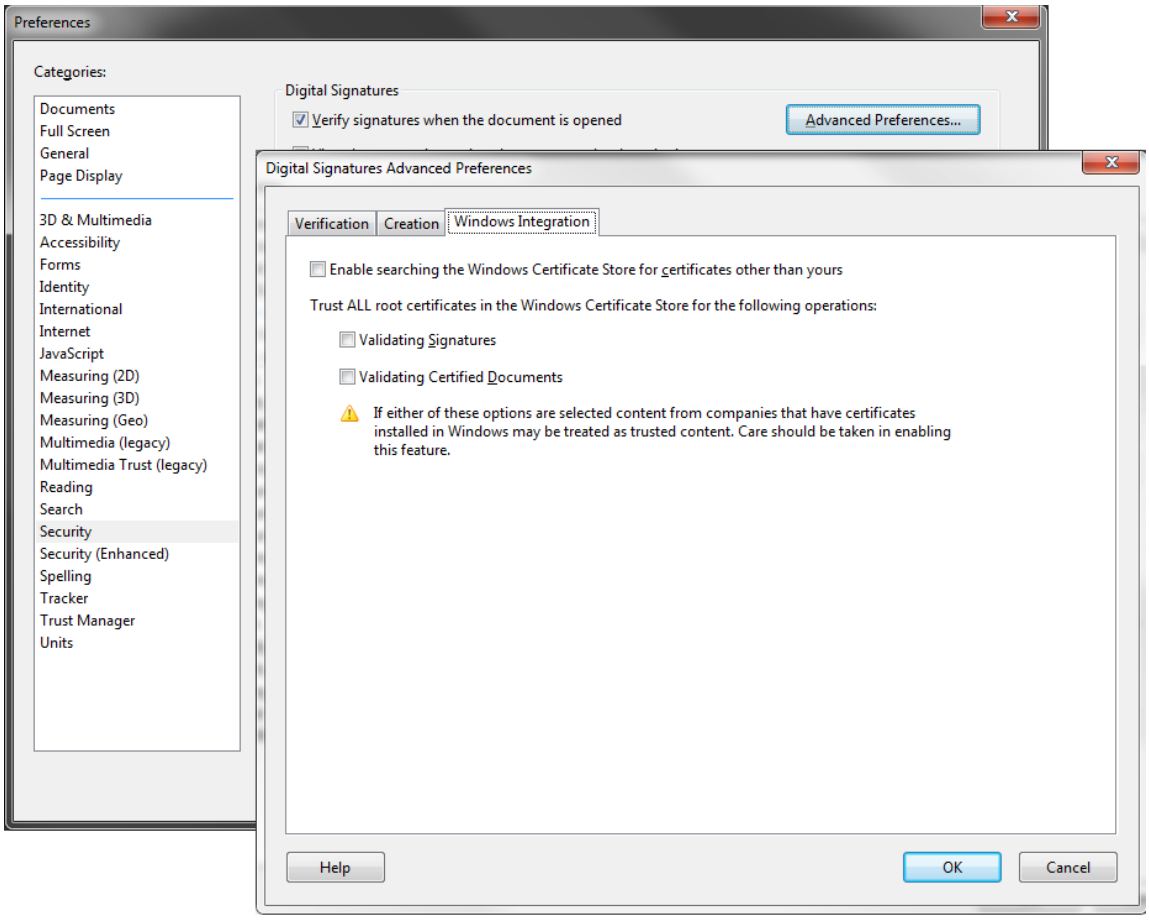
ACTIONS

1. Dan Wood will submit a request to Treasury to see if Treasury has experienced similar path building issues with Microsoft.
2. Santosh Chokhani will check if the DoD VIP session with Microsoft included this path building issue and determine what if any action is being taken by Microsoft. Santosh will include the information about the NASA and NRC tickets that have been opened to assist DoD in associating their issue with a wider impact across the entire federal community.

Agenda Item 5
Trust Store Management Guidance Working Session
Matt Kotraba

Matt Kotraba led a review of the Trust Store Management research findings, which included ICAM Roadmap guidance, NIST U.S. Government Configuration Baseline (USGCB) and Federal Desktop Core Configuration (FDCC) settings, and DOD PKE guidance presented at the April 2011 Identity Protection and Management (IdPM) Conference.

- The draft ICAM Roadmap Guidance version 2 (*not yet published*) includes definitions of Trust Anchors and the Trust Anchor Management Protocol (TAMP), but does not provide system owner / administrator level guidance for configuring current vendor products.
- USGCB and FDCC provide Trust Store settings for Windows systems, but do not provide settings for non-Windows systems or supplemental guidance on how a system owner should manage their Trust Stores manually if they choose to do so.
- An Adobe setting to leverage Microsoft CAPI was discussed. To access the setting in Adobe Reader 9, click Edit, Preferences (or Ctrl-K), click the security category on the left menu, then click on Advanced Preferences, then the Windows Integration tab. See screen shot below for available settings in Adobe Reader 9.



Details on these Adobe settings are discussed on http://learn.adobe.com/wiki/pages/viewpage.action?pageId=67076127.

Two Adobe posts are particularly relevant.

- "There are several checkboxes in the Security->Advanced preferences relating to Windows Integration. How do these affect Acrobat and Reader's interaction with the Microsoft Certificate Store and CAPI?

  During chain-building of the signature process, Acrobat and Reader search all over for the needed certificates; the Acrobat Address Book (AAB), the Windows Cert Store, the CertCache folder, P12/PFX files, smart cards and tokens, and maybe even the internet if bFollowURIsFromAIA (a registry option) is turned on. Other than the last item, Acrobat doesn't care one iota what reg key or preference setting is selected. It builds the chain, top to bottom, as best it can.

  Now comes time to establish trust. Here's is where the "use Windows trust anchor" option comes into play. Either it's off (the default setting) and the only place Acrobat can use to establish trust is the AAB, or it's on and Acrobat will use both the AAB and Windows. They are not mutually exclusive."

- "Is there a way to force Acrobat/Reader to use CAPI for OCSP checking? If so - what's the regkey? Also, what are the implications?

  The order in which revocation checkers are invoked is fixed. It is always OCSP->CRL->CAPI discriminated against the content of cRevocationChecker array in the registry. If cRevocationChecker is not defined all three are used in the listed order. If cRevocationChecker is defined then only those that are defined in cRevocationChecker are used but in the same order sans those that are not in cRevocationChecker array. For instance if cRevocationChecker array contains MSCAPI_RevocationChecker and Adobe_OCSPRevChecker (in this order) then only these two will be used but Adobe_OCSPRevChecker first and MSCAPI_RevocationChecker second, not in the order they are listed in cRevocationChecker array.

  LTV has embedded OCSP/CRL. Those are always checked with Acrobat's code, not CAPI. However, if only MSCAPI revocation checking is enabled then embedded LTV info will NOT be used, eliminating the benefit of this long-term validation information."

- An important lesson learned was gained from the DoD effort to use automated tools to remove unnecessary Trust Anchors from application Trust Stores. The automated tools often removed Trust Anchors that were necessary for system operations. System owners and administrators must be involved in the Trust Anchor assessment in order to properly identify the necessary Trust Anchors and avoid system performance issues.
- DHS found challenges identifying the Trust Anchors necessary for drivers and access to external websites. Dan Wood recommended contacting the DHS Trusted Internet Connections (TIC) Access Provider group to find out more on what external sites are accessed.

The second half of this session focused on developing a white paper for the FPKIPA and ICAMSC audience detailing the challenges associated with managing the current vendor Trust Stores, the current state of Federal guidance, and recommendations to enhance Federal guidance on Trust Store Management.

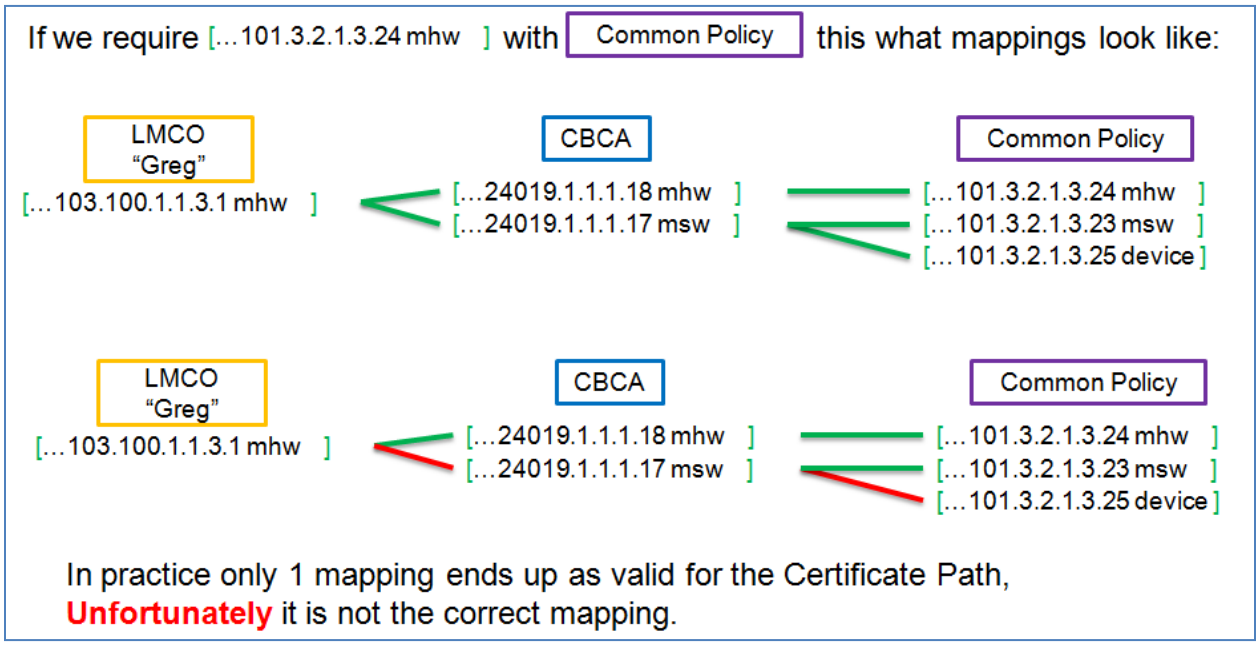
- Matt Kotraba led the review of a proposed outline for this white paper and comments were captured during the meeting.
- To facilitate additional community participation in the development of the white paper the full TWG review of the draft paper was pushed back until the December 2011 TWG.

ACTIONS

1. Once finalized, Matt Kotraba will send the TWG a copy of the ICAM Roadmap version 2.
2. Matt Kotraba will coordinate with the DoD PKE group to find out more on the process used by DoD to identify which Trust Anchors were required in their environment.
3. Dan Wood to provide TWG a copy of the Treasury's Participation in the Federal PKI ECO-System white paper. (completed)

Open Discussion
Microsoft CAPI Policy Mapping Anomalies
Santosh Chokhani and Jeff Barry

Santosh Chokhani and Jeff Barry introduced an issue with Microsoft CAPI policy mapping during the path building process. When Microsoft CAPI runs into multiple policy mappings from the issuer domain mapped to the same policy in the subject domain, CAPI only selects the first mapping in the list. The illustration below helps to visualize the error.



Within the Certipath community, this issue is causing significant user authentication issues with applications that leverage policy mappings during the authentication process. There was significant interest from the TWG to put this issue on the November 15, 2011 TWG meeting agenda.

ACTIONS

1. Follow-up action for Jeff Barry and Santosh Chokhani to prepare a full session on this topic at the November 15, 2011 TWG meeting.

Agenda Item 6
Adjourn Meeting
Matt Kotraba

The next FPKI TWG meeting is scheduled for Tuesday, November 15, 2011 from 12:30 p.m. to 3:30 p.m. EST. The meeting location is 1640 King Street, Suite 400, Alexandria, VA. Teleconference and Live Meeting will be provided for remote attendees.

Matt Kotraba adjourned the FPKI TWG meeting at 12:00 p.m. EST.

Action Item List

No.	Action Item	Point of Contact	Start Date	Target Date	Status
11	Provide FPKI TWG members a brief on the Entrust server-based encryption certificate mining tool.	Entrust (Gary Moore)	9/15/2011	10/31/2011	Open
12	Send a message to the FPKI TWG members asking for Agency support of the CITE testing of TSCP SE Public Encryption Certificate Lookup and Retrieval	FPKIMA (Matt Kotraba)	9/15/2011	10/7/2011	Closed
13	Contact NIST (Cooper / McGregor) to set up a brief to discuss key history and overflow design choices in 800-73-3	FPKIMA (Jeff Jarboe)	9/15/2011	11/15/2011	Open
14	Coordinate a review of the FBCA and Common certificate policies to identify the policy requirements for key history and recovery	FPKIMA (Jeff Jarboe)	9/15/2011	11/15/2011	Open
15	Follow-up with Microsoft regarding the TSA position paper and distribute Microsoft's response to the FPKI TWG.	FPKIMA (Matt Kotraba)	9/15/2011	10/7/2011	Closed
16	Contact NIST to identify the trust store management guidance that has been published through USGCB and legacy FDCC.	FPKIMA (Matt Kotraba)	9/15/2011	10/15/2011	Closed
17	Research the language in the FICAM Segment Architecture and Roadmap to identify its guidance on trust store management.	FPKIMA (Matt Kotraba)	9/15/2011	10/15/2011	Closed
18	Contact USCERT to determine if there is any additional guidance related to the DigiNotar compromise and if the USCERT picked up on the CertiPath member compromise.	FPKIMA (Matt Kotraba)	9/15/2011	10/15/2011	Open

No.	Action Item	Point of Contact	Start Date	Target Date	Status
19	Contact the FPKI TWG to identify members for the Trust Management Guidance tiger team.	FPKIMA (Matt Kotraba)	9/15/2011	10/15/2011	Closed
22	Send a message to the FPKI-TTIPS list to identify who has a Microsoft Premier or Partner level support to submit the design change request	FPKIMA (Matt Kotraba)	9/15/2011	9/30/2011	Closed
23	Inform Deb Gallagher that there are FPKI members who currently have a TSA as one solution to this issue. The DoD is leveraging a VeriSign TSA.	FPKIMA (Matt Kotraba)	10/25/2011	11/15/2011	Open
24	Internal inquiry within Treasury to determine if Treasury is experiencing the Microsoft Path Building Anomalies Issue	Treasury (Dan Wood)	10/25/2011	11/15/2011	Open
25	Check if the DoD VIP session with Microsoft included the Microsoft Path Building Anomalies issue and determine what if any action is being taken by Microsoft.	DoD (Santosh Chokhani)	10/25/2011	11/15/2011	Open
26	Once finalized, send the TWG a copy of the ICAM Roadmap version 2,	FPKIMA (Matt Kotraba)	10/25/2011	Based on release of ICAM Roadmap	Open
27	Provide TWG a copy of the Treasury's Participation in the Federal PKI ECO-System white paper.	Treasury (Dan Wood)	10/25/2011	10/25/2011	Closed
28	Coordinate with the DoD PKE group to find out more on the process used by the DoD to identify which Trust Anchors were required in their environment.	FPKIMA (Matt Kotraba)	10/25/2011	11/15/2011	Open
29	Prepare a TWG session for the Microsoft CAPI Policy Mapping Anomalies issue	Certipath (Jeff Barry)	10/25/2011	11/15/2011	Open