Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

Tuesday
May 15, 2012

12:30 pm – 3:30 pm

12:30	Device OID Mapping	Joint Session with CPWG Wendy Brown
1:00	Welcome & Opening Remarks	John DiDuro Jeff Voiner
1:15	OCSP Stapling	Tim Moses
2:00	Microsoft Relationship Development	Jeff Barry
2:45	Use of EKU in End User Certificates	Santosh Chokhani
3:30	Wrap-up and Adjourn Meeting	John DiDuro

Attendance List

Name	Organization	T-Teleconference P-Present
Baldridge, Tim	NASA	T
Barry, Jeff	CertiPath	P
Brown, Wendy	FPKIMA, Contractor	P
Chokhani, Santosh	DoD, Contractor	P
Cozzens, Scott	Treasury	T
DeAntonio, Damien	DHS	T
DiDuro, John	GSA, Contractor	P
Edmunds, Debbie	State	T
Hansen, Marianne	BAH (DoD Contractor)	P
Hildebrand, Jeff	GPO	P
Jarboe, Jeff	GSA, Contractor	P
Jeffers, Dan	DoD, Contractor (BAH)	T
Keating, Amy	SSA	T
King, Matt	GSA, Contractor	P
Moses, Tim	Entrust	T
Salgado, John	DoD	T
Shomo, Larry	DHS, Contractor	P
Silver, Dave	GSA, Contractor	T
Slusher, Toby	HHS	T
Spence, Willie	IRS	T
Spencer, Judy	CertiPath	T
Sulser, Dave	NRC	P
Thomas, Michelle	Energy	T
Wyatt, Terry	NASA	T

Agenda Item 1
Device OID Mapping
Joint Session with CPWG
Wendy Brown

The FPKI TWG met at Protiviti Government Services, 1640 King Street, Suite 400, Alexandria, VA beginning with a joint session with the CPWG.

Mr. John DiDuro called the TWG meeting to order at approximately 12:30 pm EST, and introduced those in person and via teleconference.

Ms. Wendy Brown explained that when the new device policy object identifiers (OIDs) were added to the Federal Bridge Certification Authority (FBCA) and Federal Common Policy Certification Authority (FCPCA) certificate policies (CPs), the cross-certificates between the FBCA and FCPCA were re-issued to include the new OIDs. The policy mapping extension mapped common-device to FBCA mediumDevice and common-deviceHW to FBCA mediumDeviceHW. This created a potential problem for certificate paths of Affiliates that previously had a device policy OID mapped to common-device. The initial rule the Federal Public Key Infrastructure Management Authority (FPKIMA) followed was that a policy cannot be mapped to something else and be passed on directly. Ms. Brown presented examples highlighting the issue, as well as options for mitigating the issue including the re-issuance of cross-certificates between the FBCA and FCPCA.

Mr. Tim Baldridge supported the suggestion that both the FBCA and FCPCA should contain all the OIDs from both CPs. Simplification via a single policy and single set of OIDs is preferred. Mr. Santosh Chokhani said he never understood why there were two separate CPs, and that it would make sense for the CPs to be combined.

It was suggested it would be cleaner to re-issue the cross-certificates between the FBCA and the affected Affiliate CAs. Mr. Jeff Barry agreed with this approach, and indicated that CertiPath, not seeing the need for an immediate correction, would be willing to re-issue their cross-certificate during their June 2012 key signing ceremony.

Mr. Baldridge suggested that the FPKI Community be notified when new cross-certificates have been issued.

ACTIONS for CPWG:

1. CertiPath will correct the OID mapping in their next certificate signing ceremony, which is scheduled for June 2012.
2. The FPKIMA will coordinate with affected Affiliates to have corrected cross-certificates issued.
3. When the new cross-certificates have been issued, the FPKIMA will inform the FPKI Community (via the FPKIPA email list) why the reissuance was necessary.

Agenda Item 2
Welcome and Opening remarks
John DiDuro

Mr. DiDuro welcomed the TWG and mentioned that due to competing events (primarily the DoD Identity Management Conference in Anaheim, CA), this TWG meeting has lower than normal attendance.

Agenda Item 3
OCSP Stapling
Tim Moses

Mr. Tim Moses, a Certification Authority/Browser (CAB) Forum participant, presented a provocative discussion about certificate revocation – that it doesn't work within a publicly-trusted Public Key Infrastructure (PKI). Mr. Moses discussed several revocation issues to support the claim.

Mr. Moses introduced the concept of "hard fail"[1] and asserted that it is desirable to PKI relying parties. To implement hard fail, relying parties, applications, operating systems, certification authorities (CAs), and subscribers need to work together.

Mr. Moses provided an overview of Online Certificate Status Protocol (OCSP) stapling, where a subscriber obtains an OCSP response and sends it with(i.e., stapled to) the certificate during a Transport Layer Security (TLS) handshake. He then provided a potential path toward community-wide adoption of hard fail via OCSP stapling, and presented evidence that most browsers are beginning to support stapling (browsers ask for the OCSP stabling, but do not necessarily fail when not supplied). However, very few web servers return OCSP stapling at this time. In addition, stapling provides revocation information about the end-entity certificate, but not the CA certificates in the path. There is a new Internet Engineering Task Force (IETF) work item to allow multi-stapling to address the entire certificate path.

Mr. Moses concluded by challenging the TWG to support a transition strategy toward hard fails and adoption of OCSP stapling by subscribers.

During the discussion, points were raised (from the TWG perspective) that availability rather than hard fail is more desirable. In addition, it was noted that there is no effective way to ascertain the opinion of relying parties regarding the hard fail notion.

ACTIONS: None.

[1] If revocation information is not returned in a timely manner, the application should act as it would if the certificate had been revoked .

Agenda Item 4
Microsoft Relationship Development
Jeff Barry

Mr. Barry described some continued issues with Microsoft's Cryptographic Application Programming Interface (CAPI) and how CertiPath is leveraging its findings on building a cooperative relationship with Trevor Freeman (Microsoft lead for federal government), which may lead to escalation of this issue to Microsoft senior management. Mr. Barry pointed out that while the fix process within Microsoft is slow, CertiPath interoperability testing's ability to discover CAPI issues is progressing quickly.

To get Microsoft to address issues, it is important to highlight to them the business impact (i.e., cannot accept PIV-I) on the FPKI Community. Accordingly, the CertiPath Policy Management Authority (PMA) will be sending waves of similarly-formatted bug reports to Microsoft.

Mr. Barry discussed a recently-discovered issue where nameConstraints in the path causes Windows 7 CAPI to return a nameConstraints error if the end-entity certificate contains a Uniform Resource Name (URN) for Universally Unique Identifier (UUID). This means that Personal Identity Verification - Interoperable (PIV-I) Authentication certificates (which require UUID) issued by PIV-I issuers approved through the CertiPath Bridge do not validate back to the FCPCA.

ACTIONS

4. CertiPath will test adding a "permit nameConstraint" as a potential work-around to the latest CAPI issue, and will report back their findings.

Agenda Item 5
Use of EKU in End User Certificates
Santosh Chokhani

Mr. Chokhani described how any digital signature certificate without an explicit Extended Key Usage (EKU) can be used for signing anything (e.g., code, time). Mr. Chokhani then described the merits of optional EKUs versus required EKUs, and preventing misapplication of an EKU when using a special-use certificate. One needs to ensure that applications looking at EKU (a) have the appropriate settings specified, and (b) avoid AnyEKU to not override the intent of limiting what can be used for codeSigning.

ACTIONS

5. Distribute the EKU table from the CertiPath CP for TWG review and comment.

Agenda Item 6
Adjourn Meeting
John DiDuro

Prior to adjournment, Mr. Baldridge asked for volunteers to help test some software code he is willing to share to get an independent, third-party review of an active project's development effort. In exchange for the code, Mr. Baldridge requires a quick turnaround on the test results.

Mr. DiDuro adjourned the TWG meeting at approximately 3:20 pm 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
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
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	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	Closed
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	Closed
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	Closed
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	Closed

No.	Action Item	Point of Contact	Start Date	Target Date	Status
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	Closed
29	Prepare a TWG session for the Microsoft CAPI Policy Mapping Anomalies issue	CertiPath (Jeff Barry)	10/25/2011	11/15/2011	Closed
30	CertiPath will present the results of the December 22, 2011 Microsoft/NIST/CertiPath meeting to the FPKI TWG.	CertiPath (Jeff Barry)	12/20/2011	1/24/2012	Closed
31	Matt Kotraba and Dave Silver to finalize recommendations white paper and distribute the final paper to the TWG, CPWG, and FPKIPA.	FPKIMA	12/20/2011	12/23/2011	Closed
32	Schedule a TWG-Microsoft meeting to review the Microsoft CodeSigning EKU Security Issue and clarify if the issue is valid or if there are any misunderstandings of Microsoft CAPI's code signing processes.	FPKIMA	12/20/2011	12/20/2011	Open
33	Add CertiPath' issue update to the January 2012 TWG meeting agenda.	FPKIMA	12/20/2011	12/20/2011	Closed
34	Look at the order of certificate mapping in cross-certificates issued by the FPKI Trust Infrastructure CAs.	FPKIMA (W.Brown)	1/24/2012	March 2012	Open
35	Facilitate a TWG/NIST follow-up meeting to discuss PKITS changes that address the Microsoft CAPI issues discussed above and planning (targeting Feb/March timeframe). We also need to encourage the TWG to provide inputs.	TWG (J.DiDuro)	1/24/2012	March 2012	Open

No.	Action Item	Point of Contact	Start Date	Target Date	Status
36	The TWG needs to develop a strategy to handle current and future issues identified with Microsoft products.	TWG (Unassigned)	1/24/2012	TBD	Open
37	Ensure the FIPS 201-2 allows for the recent Common Policy CP change proposal that allows the use of different protocols (LDAP vs. HTTP) for repository support as long as the URIs included in certificates are fully supported.	FPKIMA (Unassigned)	1/24/2012	TBD	Open
38	Schedule a planning meeting with test volunteers.	FPKIMA (W.Brown)	1/24/2012	February 2012	Closed
39	Create and maintain a TWG list of documents written to-date.	TWG (J.DiDuro)	1/24/2012	March 2012	Ongoing
40	Ms. Metzger Schoen to investigate future testing with the PKI Interoperability Test Tool (PITT) for path-validation.	S. Metzger Schoen	3/22/2012	TBD	Open
41	Add “permit nameConstraint” as potential work-around to CAPI issue and report findings	CertiPath (Jeff Barry)	5/15/2012	TBD	Open
42	Distribute EKU table from the CertiPath CP for TWG review and comment.	TWG (J. DiDuro)	5/15/2012	5/30/2012	Open