GSA

Federal PKI
Management Authority
Enabling Trust

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

Thursday June 21, 2012

9:00 a.m. – 12:30 p.m.

9:00	Welcome & Opening Remarks	John DiDuro Jeff Voiner
9:15	Enhanced Monitoring and Testing	Wendy Brown Jeff Jarboe
10:15	Tagging Certificate URL's for Analytics	Giuseppe Cimmino
10:45	Flamer/SkyWiper	TWG Discussion
11:00-12:30	EKU and Technical Constraints	Joint Session with CPWG Wendy Brown Jeff Barry Dave Cooper

Attendance List

Name	Organization	T-Teleconference P-Present
Barry, Jeff	CertiPath	P
Bravo, Kathleen	IRS	T
Brown, Wendy	FPKIMA, Contractor	P
Cimmino, Giuseppe	GSA, Contractor	P
Cooper, David	NIST	P
DeAntonio, Damien	DHS, Contractor	P
DiDuro, John	GSA, Contractor	P
Donald, India	GSA, Contractor	P
Edmunds, Debbie	State	T
Gore, Darlene	GSA FPKIMA	T
Hansen, Maryam	BAH (DoD Contractor)	P
Head, Derrick	State	T
Hildebrand, Jeff	GPO	P
Jarboe, Jeff	GSA, Contractor	P
King, Matt	GSA, Contractor	P
Louden, Chris	GSA, Contractor	P
Rea, Scott	DigiCert	T
Robinson, Buddy	Treasury	T
Salgado, John	DoD	T
Samayoa, Manny	Entrust	T
Shomo, Larry	DHS, Contractor	P
Sikder, Faysal	CertiPath	P
Silver, Dave	GSA, Contractor	T
Slusher, Toby	HHS	T
Spence, Willie	IRS	T
Thomas, Michelle	Energy	T
Vargo, Peter	GSA, Contractor	P
Wallace, Carl	DoD, Contractor	T
Wilson, Gary	SAFE-BioPharma	T
Wyatt, Terry	NASA	T

Agenda Item 1
Welcome and Opening remarks
John DiDuro

The FPKI TWG met at Protiviti Government Services, 1640 King Street, Suite 400, Alexandria, VA.

Mr. John DiDuro called the TWG meeting to order at approximately 9:00 am EST, and introduced those attending in person and via teleconference.

Mr. DiDuro welcomed the TWG and mentioned that due to competing events, this TWG meeting was moved from its originally-scheduled date of Tuesday, June 19, 2012. Even with the date change, there was very good participation from TWG members.

Agenda Item 2
Enhanced Monitoring and Testing
Wendy Brown and Jeff Jarboe

Ms. Wendy Brown and Mr. Jeff Jarboe presented the Enhanced Path Quality Monitoring and Testing overview. This initiative is a way to improve the user experience with the FPKI, and is complementary to the FIPS 201 testing done within GSA OGP. The TWG approved the overall approach and recommends that the FPKIPA Chair make it official. Ms. Brown stated that the testing program is a free offering at this point in time, but that may change if a large number of vendors desire participation.

The TWG discussed the potential Personally Identifiable Information (PII) impact on the use of sample production certificates for the operational testing. Mr. Jeff Barry from CertiPath suggested that the FPKIMA investigate a different approach to CITE, one where the FPKIMA establishes a simulated CA for each FPKI Affiliate CA rather than asking Affiliates to maintain a test environment connected to CITE. The alternative approach would create a more complete simulation of production in CITE, which would should operational testing. However, the alternative approach would not provide the same level of assurance of production path quality as with performing operational testing of vendor products in the production environment.

Several TWG members volunteered to assist with developing the Operational Test Suite that will be used for product testing.

ACTIONS:

1. Ms. Brown to obtain approval from the FPKIMA System Owner to pursue enhancement to AIA web crawler to automate path quality report generation.
2. Mr. Jarboe to finish PDVal process document and obtain TWG review.
3. Ms. Brown to draft initial operational test plan and invite TWG members to participate in the test plan development.
4. Ms. Brown to provide status reports to TWG (frequency to be determined).

Agenda Item 3
Tagging Certificate URL's for Analytics
Giuseppe Cimmino

Mr. Giuseppe Cimmino described the option of providing a unique URL for the corresponding p7c in each cross-certificate issued by the FBCA, which would allow the FPKIMA to obtain information about FPKI Repository usage. The consensus was that this may be perceived as an attempt to track individual usage, and would not yield very useful information. In addition, there may be a negative impact on a relying party's ability to rely on cached files. No PKI's represented at this TWG meeting are pursuing this level of analysis.

ACTIONS: None.

Agenda Item 4
Flamer/SkyWiper
TWG Discussion

Mr. Peter Vargo outlined the Flamer/SkyWiper malware vulnerability and described the importance of this exploit to the FPKI Community. A known prefix MD5 hash attack collision was used. There was consensus that SSL validation via MD5 hashing should no longer be tolerated, and that SHA-1 should be deprecated. It was noted that SHA-1 cannot be used within the FPKI after December, 2013.

There was then discussion about ways to counter future, similar attacks. The discussion included browser patches and configurations regarding acceptance of MD5 SSL certificates, and "protected" EKU. The TWG consensus is that generally-available commercial fixes, such as MD5-Shield, are sufficient to protect the FPKI Community.

ACTIONS: None.

Agenda Item 5
EKU and Technical Constraints
Joint Session with CPWG
Wendy Brown, Jeff Barry and Dave Cooper

A joint TWG/CPWG session was held to discuss EKUs and Technical Constraints. CertiPath introduced an approved change to their policy that lists optional and restricted EKUs for each of their certificate profiles. Mr. Barry presented alternatives for mitigating a vulnerability in the way Microsoft validates signatures on code, which is the driver for the change proposal. Mr. Barry then presented a list of pros and cons for each alternative.

Mr. Dave Cooper suggested that the FPKI Community might be morphing our PKI to address the issue rather than addressing the issue with Microsoft directly. Mr. Jeff

Hildebrand asked about the risks and benefits of addressing the issue using the EKUs. Mr. Barry suggested that specifying parameters around EKUs was the right compensating control for CertiPath but it may not be the right choice for the FPKI. Mr. Cooper suggested there might be a great risk of harm rather than improved security posture by requiring the EKUs. Mr. Hildebrand added that simplicity is the goal, use of the EKU adds complexity, and most applications check policy OIDs rather than EKUs.

In addition, due to the lifespan of certificates already issued, a change to the FPKI Trust Infrastructure certificate profiles that mandates inclusion of EKUs on all certificates containing a key usage of digital signature will not address the vulnerability issue for at least 3 years. Further, since Microsoft will continue to trust code-signing certificates past their expiration dates, the vulnerability issue will continue unless Microsoft changes the way it validates code signatures.

Mr. Cooper also noted that the PIV-I profile mandates inclusion of “anyEKU,” so there may be a risk that some PIV-I cards would become non-interoperable. Mr. Chris Louden suggested that if these options are not acceptable, other options need to be explored. Reducing the attack surface is beneficial, but the FPKI Community needs to be concerned about uncovering unknown impacts. Therefore, our goal should be to stimulate long-term solutions. Mr. Gary Wilson suggested that evaluation of real risk is important so as not to create unviable solutions.

Ms. Maryam Hansen noted that the DoD believes further discussion and significant testing is required prior to the FPKI making any decision on adopting Certipath’s approach in specifying EKUs.

***ACTIONS**:*

5. Mr. DiDuro will resend the white paper to the CPWG and TWG mail lists that provides detail about the Code Verification vulnerability issue.
6. Mr. DiDuro will resend the CertiPath Certificate Policy that includes the EKU change proposal to the FPKI TWG and CPWG for determination of impacts and issues.

Agenda Item 6
Adjourn Meeting
John DiDuro

Mr. DiDuro adjourned the TWG meeting at 12:15 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 (Wendy Brown)	1/24/2012	March 2012	Closed
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 (John 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 (Wendy Brown)	1/24/2012	February 2012	Closed
39	Create and maintain a TWG list of documents written to-date.	TWG (John 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 (John DiDuro)	5/15/2012	Resend to TWG and CPWG prior to next TWG	Open
43	Obtain approval from system owner to pursue enhancement to AIA web crawler to automate path quality report generation.	FPKIMA (Wendy Brown)	6/21/2012	TBD	Open
44	Finish PDVal process document and obtain TWG review.	FPKIMA (Jeff Jarboe)	6/21/2012	TBD	Open

No.	Action Item	Point of Contact	Start Date	Target Date	Status
45	Draft initial operational test plan and invite TWG members to participate in the test plan development.	FPKIMA (Wendy Brown)	6/21/2012	TBD	Open
46	Provide status reports to TWG on Enhanced Monitoring and Testing initiative (frequency to be determined).	FPKIMA (Wendy Brown)	6/21/2012	TBD	Open
47	Distribute the white paper to the CPWG and TWG mail lists that provides detail about the Code Verification vulnerability issue.	TWG (John DiDuro)	6/21/2012	7/17/2012	Open