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

February 2012 TWG Highlights (in lieu of a meeting)

The February 2012 TWG meeting was cancelled due to scheduling conflicts with a number of key security-related activities, most notably ICAM Sharing Day and the RSA 2012 Conference.   The following are several important updates.

Encryption Certificate Lookup Testing with CITE

Status: The TWG organized a test team meeting in mid-February 2012 to further explore encryption certificate lookup. The goals of the team are to test potential encryption certificate lookup models in support of encrypted email across the FPKI community, and make recommendations to the full TWG on viable models/requirements.

Next steps: The team is setting a realistic pace to establish requirements and test environments. Tasks were assigned to members from the Federal Public Key Infrastructure Management Authority (FPKIMA) as well as affiliates. Wendy Brown will report status to the TWG on a recurring basis until the team is ready to brief interim findings.

Introducing a new TWG Co-Chair

Jeff Voiner has joined Darlene Gore as a full-time member of the General Services Administration (GSA) Federal Acquisition Service (FAS) FPKIMA team, and will be co-chairing the TWG going forward. Jeff, while new to GSA, has been in federal service for seven years, and has been in an array of information technology positions for GSA and within private industry for PricewaterhouseCoopers and Mellon Financial. Jeff is anxious to use his considerable skills to help improve the PKI technical community.

Next TWG Meeting

The next TWG will be held on Tuesday, 20 March 2012.

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	Closed
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 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	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 publish a TWG list of documents written to-date.	TWG (J.DiDuro)	1/24/2012	February 2012	Open