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
March 22, 2012

1:00 p.m. – 3:30 p.m.

1:00	Welcome & Opening Remarks	Chris Louden Jeff Voiner
1:15	FPKI Technical Working Group Update	John DiDuro
1:45	Authority Information Access (AIA) Crawler	Sandy Metzger Schoen
2:45	RSA Conference Re-Cap	Chris Louden Giuseppe Cimmino Open to all participants
3:15	Actions and Next Steps	Wendy Brown John DiDuro
3:30	Adjourn Meeting	John DiDuro

Attendance List

Organization	Name	T-Teleconference P-Present A-Absent
Verizon Business	Blanchard, Deb	T
GSA (Contractor)	Brown, Wendy	P
DoD (Contractor)	Chokhani, Santosh	T
GSA (Contractor)	Cimmino, Giuseppe	P
GSA (Contractor)	DiDuro, John	P
State Department	Edmonds, Deb	T
DHS (Contractor)	Fisher, Dave	T
State Department	Head, Derick	T
GSA (Contractor)	Louden, Chris	P
GSA (Contractor)	Metzger Schoen, Sandy	P
GSA (Contractor)	Packham, Jordan	P
???	Robinson, Lee	T
DoD (Contractor)	Salgado, John (works with Dan Jeffers)	T
DHS (Contractor)	Shomo, Larry	P
???	Spencer, Willie	T
DoE	Thomas, Michelle	T
NASA	Wyatt, Terry	T

Agenda Item 1
Welcome and Opening Remarks
Chris Louden

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

Mr. John DiDuro called the TWG meeting to order at approximately 1:00 pm EST, and introduced those in person and via teleconference. Mr. Chris Louden welcomed the TWG and mentioned that because of the TSCP Event, the TWG experienced lower than normal attendance.

Agenda Item 2
FPKI Technical Working Group Update
John DiDuro

Mr. DiDuro presented an overview of the past topic areas covered by the FPKI TWG and outlined future topics for TWG consideration. In addition, Mr. DiDuro presented a listing of documents produced by the TWG over the past year. The ensuing discussion sparked several areas for the TWG to address, including:

<u>Name Constraints</u>
Issue with name constraints – and subjectAltName and UUID – any nameConstraints appears to break Microsoft interpretation of the UUID as a valid SAN.

Mr. Santosh Chokhani said that Cygnacom may have uncovered some additional Microsoft issues very recently, and will be reporting their findings once formalized. The TWG requests details from Mr. Jeff Barry once they're known.

<u>Microsoft Issues, in general</u>
Mr. Louden stated that the FPKIPA will be speaking with Microsoft again on this topic in an attempt to get a reaction to the U.S. Government's continued concern regarding their products.

Mr. Chokhani encouraged the FPKIPA to not ask Microsoft to make a judgment call, but to just correct their known issues.

The TWG community needsto identify additional tests for PDVAL testing to encourage Microsoft to enforce the standards to which others subscribe. In essence, Microsoft is violating several security issues by building paths beyond the root and causing excessive network traffic (at both the Certification Authority (CA) infrastructure's wide area network and at the end-user's local area network).

ACTIONS:

1. Mr. DiDuro to maintain the briefing that describes TWG events and deliverables.

Agenda Item 3
Authority Information Access (AIA) Crawler
Sandy Metzger Schoen

Ms. Sandy Metzger Schoen presented a briefing on the AIA crawler, which is a tool to discover and path-validate all CA certificates cross-certified with the Federal Common Policy (SHA-256) CA. The AIA crawler runs automatically on a weekly basis.

There were numerous discussions regarding the tool’s use, future enhancements, and technical details of the tool’s coding. Highlights of those discussions include:

- The tool does policy validation to all FPKI Object Identifiers (OIDs) and all FPKI Test OIDs including new EGTS OIDs.
- The tool summarizes various output files that are available and provides example Subordinates by agency or full paths.
- The tool does Online Certificate Status Protocol (OCSP) & Certificate Revocation List Distribution Point (CRLDP) validation checking – errors may include if the OCSP and CRLDP do not provide the same results and why.
- The tool uses custom code for the AIA chain and PKIX java library for general path, OID and path validation.

ACTIONS

2. Ms. Metzger Schoen to investigate future testing with the PKI Interoperability Test Tool (PITT) for path-validation.

Agenda Item 4
RSA Conference Recap
Giuseppe Cimmino

Mr. Giuseppe Cimmino, FPKIMA Platform Team lead, discussed his interaction with the BlueCoat federal team and a potential linkage with the FPKI TWG for future meetings.

ACTIONS

None

Agenda Item 5
Acton and Next Steps
Wendy Brown

Ms. Wendy Brown mentioned that the CAB Forum is developing network security guidelines that may be of interest to the FPKI TWG. In addition, Ms. Brown mentioned that the Four Bridges Forum is looking to develop audit requirements.

Agenda Item 6
Adjourn Meeting
John DiDuro

Mr. DiDuro adjourned the TWG meeting at approximately 3:00 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