Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

June 16, 2011

9:30 a.m. – 3:30 p.m.

Agenda

9:30	Welcome & Opening Remarks Introductions	Cheryl Jenkins
9:40	E-Governance Trust Services (EGTS)	Chris Louden
10:00	FPKI Community Interoperability Test Environment (CITE) Comment Review	Wendy Brown / Jeff Jarboe
11:15	PKI Repository Requirements Evolution	Wendy Brown / Chris Louden
12:00	Lunch	All
1:00	Timestamp Authority Discussion with Microsoft	Matt Kotraba
3:00	Transition Framework: FPKIMA Release Strategy	Matt Kotraba
3:30	Adjourn Meeting	Chris Louden

Attendance List

Organization Supported	Name	Email	P-Present/ T-Teleconference
Department of Defense (Contractor)	Sam Schaen	sam.schaen.ctr@disa.mil	T
Department of Defense (Contractor)	Santosh Chokhani	schokhani@cygnacom.com	P
Department of State	Deb Edmonds	edmondsdd@state.gov	P
Department of State	Derrick Head	headdl@state.gov	T
DigiCert	Scott Rea	scott.rea@digicert.com	T
Entrust	Gary Moore	gary.moore@entrust.com	P
GPO	Jeff Hilderand	jhildebrand@gpo.gov	P
GSA - FPKIMA	Cheryl Jenkins	cheryl.jenkins@gsa.gov	P
GSA	Darlene Gore	darlene.gore@gsa.gov	T
GSA (Contractor)	Brant Petrick	brant.petrick@gsa.gov	P
GSA (Contractor)	Wendy Brown	wendy.brown@pgs.protiviti.com	P
GSA (Contractor)	Chris Louden	chris.louden@pgs.protiviti.com	P
GSA (Contractor)	Dave Silver	dave.silver@pgs.protiviti.com	T
GSA (Contractor)	Giuseppe Cimmino	giuseppe.cimmino@pgs.protiviti.com	P
GSA (Contractor)	Matt King	matthew.king@pgs.protiviti.com	P
GSA (Contractor)	Matt Kotraba	matthew.kotraba@pgs.protiviti.com	P
GSA (Contractor)	Jeff Jarboe	jeff.jarboe@pgs.protiviti.com	P
NASA	Terry Wyatt	terry.wyatt@nasa.gov	T
NASA	Tim Baldridge	tim.baldridge@nasa.gov	T
ORC	Jim Patten	Not available	P
Treasury	Dan Wood	daniel.wood@do.treas.gov	P
Treasury	Jim Schminky	james.schminky@do.treas.gov	P
Treasury	Kurt Weaver	kurt.weaver@bpd.treas.gov	T
Verizon	Debb Blanchard	deborah.blanchard@verizon.com	T

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

The Federal Public Key Infrastructure (FPKI) Technical Working Group (TWG) met at General Services Administration (GSA) One Constitution Square Office, Room 801, 1275 1st Street, NE, Washington, DC. Matt Kotraba called the meeting to order at 9:35 a.m. EST and introduced those in person and via teleconference.

Agenda Item 2
E-Governance Trust Services (EGTS)
Chris Louden

Chris Louden provided an overview of the EGTS initiative and the FPKIMA plan to deploy a new E-governance Certification Authorities (EGCA) in support of EGTS. Clarification was provided as to why the EGTS certificate services are not being issued under the FPKI Common Policy Framework (Common) CA. The necessary policy Object Identifiers (OIDs) are not included in the Common certificate policy and current vendor products cannot provide the proper path discovery and validation. Clarification was provided regarding the services EGTS will provide to Attribute Authorities. EGCA will provide PKI certificates to Attribute Authorities for the purpose of signing attribute claims, and to the E-Governance Metadata Authority (EGMA) for signing metadata.

ACTIONS
No actions.

Agenda Item 3
FPKI Community Interoperability Test Environment (CITE)
Jeff Jarboe

FPKI CITE v0.1.0 participation guidelines were sent to the FPKI TWG for review and comment ahead of this June 16, 2011 FPKI TWG meeting. Jeff Jarboe led the TWG in the review of all comments received. Each comment was discussed, and recommendations updated.

ACTIONS

a. The FPKIMA will update the FPKI CITE document per comment review decisions, and will release the first version of the document.

Agenda Item 4
PKI Repository Requirements Evolution
Wendy Brown / Chris Louden

Wendy Brown presented the current FPKI certificate policy and certificate profile protocol requirements for repositories, the sample repository usages, the challenges to the current requirements, and a draft proposal to modify the repository protocol requirements to make LDAP optional and HTTP mandatory. Consensus was reached that making LDAP an optional protocol and HTTP mandatory is a valid proposal that holds value to the FPKI community.

ACTIONS

a. The FPKIMA will develop change proposals for the FBCA and Common Policy Certificate Policies and Certificate Profiles, and will submit them to the FPKI Policy Authority (FPKIPA) Certificate Policy Working Group (CPWG).

Agenda Item 5
Time Stamping Authority Discussion with Microsoft
Matt Kotraba / Mike Burk (Microsoft)

Matt Kotraba provided an overview and current status of the Microsoft Root Certificate Program (MRCP) requirement to establish a Timestamp Authority (TSA) in conjunction with asserting the code signing Extended Key Usage (EKU) in the Windows Trust Store for Publicly distributed Certification Authorities (CAs) such as Common CA. Mike Burk, Microsoft Program Manager for Windows Security, summarized Microsoft's rationale for including the TSA requirement in the MRCP, and provided details on how Microsoft products are designed to validate signed code with and without timestamps.

Several follow-up questions (for Microsoft) were raised by the FPKI TWG (see list below). Mike Burk will research and provide Microsoft's response.

1. Related to Timestamps, clarification was requested on:
    a. How Microsoft products (E.g. Microsoft Outlook) handle timestamps for non-code signing signatures (e.g. signed emails)?
    b. How Microsoft products process signed code when the code signing EKU is not present?
    c. What "time" is verified against the timestamp and is time compared even if a timestamp is not present?
2. Unrelated to Timestamps, what is the Microsoft process or point of contact for the FPKI TWG to report PKI bugs or errors in Microsoft products?

ACTIONS

a. Matt Kotraba will coordinate with Mike Burk to ensure answers to the follow-up questions are provided to the FPKI TWG community.
b. Gary Moore will lead, with assistance from Santosh Chokhani, the drafting of a FPKI TWG position paper that details the following points:

1. The FPKI TWG position on dealing with expired and/or revoked certificates used for signing code by providing a payload with the signature that includes the necessary Certificate Revocation Lists (CRLs) and CA certificates at the time the signature was applied.
2. Handling of signed code with no EKU.
3. Should perform certificate validation for the TSA signing certificate.
4. FPKI TWG objection to standing up a TSA for the FPKI community that will not be leveraging the TSA.

Agenda Item 6
Transition Framework: FPKIMA Release Strategy
Matt Kotraba

Matt Kotraba provided the FPKI TWG with an update on the FPKIMA approach to managing future technology transitions of the Trust Infrastructure. The FPKIMA is currently drafting a Release Strategy, incorporating community input from the SHA-256 Lessons Learned, and the March 2011 FPKI TWG. The Release Strategy identifies a methodology for analyzing Trust Infrastructure requirements, allocating and scheduling requirements to release versions, conducting development and interoperability testing, and capturing operational feedback after deployment. The FPKI TWG agreed to review the Release Strategy at the September 2011 FPKI TWG.

ACTIONS

a. FPKIMA will complete the initial draft of the FPKIMA Release Strategy for the FPKI Trust Infrastructure, and will coordinate FPKI TWG comments ahead of the September FPKI TWG.

Adjourn Meeting
Chris Louden

Chris Louden led a discussion of potential topics for the next TWG meeting in September (see list below). FPKI TWG members can contact Matt Kotraba if they have any additional suggestions.

Potential September TWG Topics:

1. Update on Path Validation Bug
2. Update on Timestamp Authority Position Paper
3. Community-wide Public Encryption Certificate Lookup & Retrieval
4. Release Strategy Comment Review
5. Storing of Encryption Key History on card
6. Off-line Root
7. Combining Federal Bridge CA and Common Policy CA

Chris Louden adjourned the FPKI TWG meeting at 2:35 p.m. EST.

Action Item List

No.	Action Item	Point of Contact	Start Date	Target Date	Status
1	Update the FPKI CITE guidelines and coordinate comments with the FPKI TWG.	FPKIMA (Jeff Jarboe)	3/17/2011	4/30/2011	Complete
2	Establish a mailing list and group collaboration calendar to coordinate testing activities.	FPKIMA (Matt Kotraba)	3/17/2011	8/31/2011	Open
3	Draft a transition framework and coordinate comments with FPKI TWG members.	FPKIMA (Matt Kotraba)	3/17/2011	8/31/2011	Open
4	Coordinate with the FPKI TWG and consolidate the list of FPKI community questions for Microsoft	FPKIMA (Matt Kotraba)	3/17/2011	4/1/2011	Complete
5	Coordinate a Code Signing Summit with Microsoft and forward an invitation to the FPKI TWG	FPKIMA (Matt Kotraba)	3/17/2011	4/30/2011	Complete
6	Identify standard operating procedures for FPKI affiliate code signing certificate services	FPKI TWG Members (with Code Signing Services)	3/17/2011	4/30/2011	Complete
7	Coordinate Microsoft TSA follow-up questions with Mike Burk and distribute Microsoft response with FPKI TWG	FPKIMA (Matt Kotraba)	6/16/2011	6/30/2011	Open
8	FPKI TWG position paper on the Microsoft TSA requirement	Gary Moore	6/16/2011	8/31/2011	Open
9	Update FPKI CITE guidelines and release first version to the FPKI TWG and CITE members	FPKIMA (Jeff Jarboe)	6/16/2011	6/30/2011	Open
10	Develop change proposals for making LDAP optional and HTTP mandatory and submit them to the FPKIPA CPWG.	FPKIMA (Jeff Jarboe)	6/16/2011	6/30/2011	Open