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

March 17, 2011

9:30 a.m. – 3:30 p.m.

Agenda

9:30	Welcome & Opening Remarks Introductions	Cheryl Jenkins
9:40	FPKI TWG Meeting Logistics	Chris Louden
9:50	FPKI Affiliate Test Environment	Wendy Brown
11:00	High-level Strategies for Transition Planning	Chris Louden
12:00	Lunch	All
1:00	Time Stamping with Code Signing Signature	Matt Kotraba/ Wendy Brown
2:30	Open Discussion of New Issues	Chris Louden
3:30	Adjourn Meeting	Cheryl Jenkins

ATTENDANCE LIST

Organization Supported	Name	Email	P-Present/ T-Teleconference
CertiPath	Steve Howard	steve.howard@certipath.com	P
Department of Defense	Allison Scogin	allison.scogin@disa.mil	T
Department of Defense (Contractor)	Santosh Chokhani	schokhani@cygnacom.com	P
Department of Homeland Security (Contractor)	Larry Shomo	lawrence.shomo@associates.dhs.gov	T
Department of Justice	Scott Morrison	scott.k.morrison@usdoj.gov	T
Department of State (Contractor)	Charles Froehlich	froehlichcr@state.gov	T
Department of State	Deb Edmonds	edmondsdd@state.gov	P
Department of State	Derrick Head	headdl@state.gov	P
Department of State	Tom Gee	geete@state.gov	P
DigiCert	Scott Rea	scott.rea@digicert.com	T
Entrust	Gary Moore	gary.moore@entrust.com	P
GSA (Contractor)	Brant Petrick	brant.petrick@gsa.gov	P
GSA	Cheryl Jenkins	cheryl.jenkins@gsa.gov	P
GSA (Contractor)	Wendy Brown	wendy.brown@pgs.protiviti.com	P
GSA (Contractor)	Yuriy Dzambasow	yuriy@dzambasow.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)	Tim Pinegar	tim.pinegar@pgs.protiviti.com	P
SAFE-BioPharma	Gary Wilson	gwilson@safe-biopharma.org	T
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
Treasury	Todd Johnson	todd.johnson@bpd.treas.gov	T
USPTO (Contractor)	Amit Jain	amit.jain@uspto.gov	T

Agenda Item 1
Welcome & Opening Remarks
Introductions--All Attendees
Cheryl Jenkins

The Federal Public Key Infrastructure Technical Working Group (FPKI TWG) met at 1640 King Street Suite 400, Alexandria, VA. Chris Louden called the meeting to order at 9:40 a.m. and introduced those in person and via teleconference. Cheryl Jenkins provided opening remarks to the FPKI TWG and thanked all members for taking time out to attend.

Agenda Item 2
FPKI TWG Meeting Logistics
Chris Louden

Chris Louden reviewed three logistical points for the operation of the FPKI TWG:

a. Over the past couple of years, the FPKI TWG did not maintain regularly-scheduled sessions. Moving forward, the FPKI Management Authority (FPKIMA) will host quarterly FPKI TWG meetings with special sessions added as necessary. This schedule was agreed to by the members present.

b. The FPKI TWG is a collaborative forum with community participation. Prior to each quarterly session, Matthew Kotraba will reach out to FPKI TWG members for new topics. At any time, FPKI TWG members can submit suggested topics to Matthew Kotraba for upcoming meetings.

c. Contact information to include full name and e-mail address should be sent to Matthew Kotraba for those who want to be added to the FPKI TWG listserv.

ACTIONS

a. The FPKIMA to schedule quarterly meetings.

Agenda Item 3
FPKI Affiliate Test Environment
Wendy Brown

Wendy Brown presented the current status of the FPKIMA Affiliate test environment and then led a discussion focused on ways to enhance the test environment.

The consensus was that the FPKI Affiliate test environments are needed and should mirror the Affiliate's production environment by including the Certification Authority (CA) hierarchy and repositories (as required in production). However, the Service Level Agreement (SLA) needs to be modified to be less stringent, allowing for more flexibility on how each Affiliate implements their test environment. There was some concern over the cost of maintaining a test environment. To address this concern, more flexibility will be added to the requirements and SLA. Currently, Affiliate participation is voluntary. The following modifications should be addressed in either the revised test environment requirements or the SLA:

a. Flexibility needs to be maintained in the way Affiliates implement their test environment to meet requirements.

b. Affiliates are encouraged to use test policy Object Identifiers (OIDs).

c. Affiliates should provide private/public key pairs and end entity certificates (public key) for other Affiliates to test certificate path validation and interoperability. However, each Affiliate can choose if and how they will provide access to private keys (e.g., open public access on the Internet, provide as requested, or not provide private keys at all).

d. The SLA should include a set of core hours during which Affiliates will provide technical support for testing, with a caveat that testing does not interfere with production activities.

e. Language is needed in the SLA to distinguish between the hours an Affiliate lab should be available (i.e. test environment availability) and the number of hours a system administrator is actively working in a lab (i.e. technical support and maintenance). Test environment availability can include unmanned time. Affiliates can decide whether or not to deploy monitoring systems during unmanned hours.

There was consensus to establish a new mailing list and group-collaboration calendar to coordinate testing activities. The calendar will be used for advanced scheduling of tests and maintenance. The group agreed that contact information should be published in a controlled manner rather than published openly on the Internet.

Treasury was interested in the scope of technical assistance in support of other Federal Identity, Credential, and Access Management (FICAM) Subcommittee (SC) initiatives such as logical access control systems (LACS). FICAM activities involve the same parties, and PKI is the trust anchor. The FPKI Affiliate test environment could potentially be the environment to support PKI for ICAM.

ACTIONS

a. The FPKIMA will update the FPKI Affiliate test environment requirements document which includes the SLA and send to the FPKI TWG listserv for comments.

b. The FPKIMA will establish a mailing list and/or group-collaboration calendar to coordinate testing activities. In addition, the FPKIMA will coordinate with FPKI TWG members to identify each Affiliate's test environment POCs.

Agenda Item 4
High-level Strategies for Transition Planning
Chris Louden

Chris Louden presented a high-level Transition Framework that when completed will assist the FPKI technical community in effectively and systematically managing the evolution of the FPKI and its services.

The concept of versioning the FPKI was discussed. Versioning could be used to identify the features and requirements for FPKI. This approach aligns with industry practices. The benefits of versioning include:

a. Helping industry understand impending FPKI changes and which features are currently supported.

b. The FPKI version concept could be incorporated into the procurement process to ensure vendor products meet the requirements of a particular FPKI version(s) before the product is acquired.

c. The National Institute for Standards and Technology (NIST) PKI Test Suite (PKITS) versions could be aligned to FPKI versions to assist FPKI Affiliates and vendor testing activities.

d. New requirements placed in FPKI versions can assist FPKI Affiliates in planning out fiscal-year budgets versus managing new requirements through unfunded requirements.

The FPKI TWG agreed that communication with vendors regarding transition planning should be made collectively as an FPKI community.

Matt King provided status update on *SHA-256 Lessons Learned* documentation. The FPKI Policy Authority is finalizing lessons learned for presentation to the CIO Council.

ACTIONS

a. The FPKIMA will draft a Transition Framework and submit document to the FPKI TWG for comments.

Agenda Item 5
Time Stamping with Code Signing Signatures
Matt Kotraba / Wendy Brown

Wendy Brown and Matthew Kotraba summarized the Microsoft Time Stamping Authority (TSA) requirement for Certification Authorities (CAs) asserting the code signing Extended Key Usage (EKU) in the Microsoft Root Certificate Program. The requirement was received from Microsoft and passed to the Certificate Policy Working Group (CPWG), which requested a technical impact assessment from the FPKI TWG.

The discussion opened by polling FPKI TWG members to see which organizations are operating code signing certificate services. DHS, DoD, DoS, and Treasury have code signing certificate services. The FPKI TWG determined that there is currently not enough information to fully assess the impact of the Microsoft TSA requirement or make any recommendations on how to address the requirement. The group agreed that a Code Signing Summit between the FPKI TWG and Microsoft should be set up to further discuss the TSA requirement. Affiliates with code signing certificate services should research their standard operating procedures to discuss their specific implementation of code signing certificates with the FPKI TWG and Microsoft.

ACTIONS

a. Prior to the summit, the FPKIMA will consolidate FPKI-community questions for Microsoft.

b. The FPKIMA will coordinate, and schedule the Code Signing Summit with Microsoft and the FPKI TWG.

c. FPKI Affiliates with code-signing certificate services should identify their standard operating procedures to discuss their specific implementation of code signing certificates with the FPKI TWG and Microsoft. Specifically, what procedures (if any) are in place for:

    1. How code signers handle expired or revoked certificates? Is code re-signed when a certificate expires or is revoked?

    2. What is the certificate lifespan when a certificate is issued (e.g., expiration date is one year from issuance)?

    3. How is code actually signed? Are signatures applied to code made through native applications and/or third party solutions?

    4. What code is being signed (i.e., stand-alone code or Visual Basic/Macros embedded in Microsoft Office applications such as Excel, Word, Access)?

Agenda Item 6
Open Discussion
Chris Louden

Open discussion with the FPKI TWG members was led by Chris Louden covering a number of topics. Discussion topics included:

a. **FPKI Issues Tracking**: Chris Louden discussed the FPKIMA Technical Advisory Group recommendation to track issues at the FPKI level rather than at each agency. A list of issues was reviewed and discussed at a high level.

b. **Constraining Transitive Trust:** Santosh Chokhani led a discussion on constraining transitive trust deliberately through PKI controls available in certificates (Path Length Constraint, Skip Certs, and Name Constraints) to manage trust, interoperability, and security. However, there is not unity across the FPKI community on how these controls should be used in certificates.

c. **Proposal for a new EKU for Claim Signers**: Chris Louden introduced a proposal for a new EKU for Claim Signers that need to sign attributes or claims about entities. Trust in systems is managed through PKI Trust Anchors and Policy OIDs. However, many applications are managing certificate uses through EKUs. The issuance of Personal Identity Verification (PIV) and PIV-Interoperable (PIV-I) certificates introduced the need for a certificate EKU to assert a signer of PIV and PIV-I attributes. Individual single purpose EKUs, PIV Signer and PIV-I Signer were established to meet this requirement rather than establishing a single EKU to cover any claim signer. FICAM initiatives are introducing attribute signers that will require an EKU to assert attribute claims about entities. The Claim Signer EKU could be used for these attribute signers. The FPKI TWG members agreed with this proposal and believe it will help provide a universal EKU for all future claim signers.

Adjourn Meeting
Chris Louden

Chris Louden adjourned the FPKI TWG meeting at 3:15 p.m.

Action Item List

No.	Action Item	Point of Contact	Start Date	Target Date	Status
1	Update the test environment requirements document and draft SLA and coordinate comments with the FPKI TWG participant list.	FPKIMA (Wendy Brown)	3/17/2011	4/30/2011	Open
2	Establish a mailing list and/or group collaboration calendar to coordinate testing activities, and coordinate with FPKI TWG members to identify each affiliates test environment POCs.	FPKIMA (Matt Kotraba)	3/17/2011	4/30/2011	Open
3	Draft a transition framework and coordinate comments with FPKI TWG members.	FPKIMA (Matt Kotraba)	3/17/2011	5/31/2011	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	Open
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	Open
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	Open