Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

September 15, 2011

9:30 a.m. – 3:30 p.m.

9:30	Welcome & Opening Remarks Introductions	Chris Louden
9:40	Public Encryption Certificate Lookup & Retrieval	Matt Kotraba Kyle Villano Jeff Berry
11:00	Encryption Key History	Gary Moore Jeff Jarboe
12:00	Lunch	
1:00	Microsoft Timestamp Authority Position Paper Update	Matt Kotraba Santosh Chokhani Gary Moore
1:10	Developing Trust Store Management Guidance on the use of 3rd Party CAs (Prompted by DigiNotar CA Compromise)	Matt Kotraba
2:30	Microsoft Path Building Anomalies	Santosh Chokhani
3:15	Community Interoperability Test Environment (CITE) Update	Matt Kotraba
3:30	Adjourn Meeting	Chris Louden

Attendance List

Organization Supported	Name	Email	P-Present/ T-Teleconference
CertiPath	Jeff Barry	jeff.barry@certipath.com	P
CipherSolutions	Ahuja Vijay	vijay@ciphersolutions.com	T
DEA	Sherrod Briggs	Sherrod.N.Briggs@usdoj.gov	T
Department of Defense (Contractor)	Curt Spann	spann_curt@bah.com	T
Department of Defense (Contractor)	Dan Jeffers	jeffers_daniel@bah.com	T
Department of Defense (Contractor)	Santosh Chokhani	schokhani@cygnacom.com	P
Department of State	Deb Edmonds	edmondsdd@state.gov	T
Department of State	Derrick Head	headdl@state.gov	T
DHS	Larry Shomo	Lawrence.Shomo@associates.dhs.gov	P
DHS	Matthew Ambs	Matthew.Ambs@ASSOCIATES.DHS.GOV	T
DOE	Michele Thomas	Michele.Thomas@hq.doe.gov	T
DOJ	Scott Morrison	Scott.k.morrison@USDOJ.GOV	T
Entrust	Gary Moore	gary.moore@entrust.com	P
GSA	Darlene Gore	darlene.gore@gsa.gov	T
GSA (Contractor)	Brant Petrick	Brant.Petrick@gsa.gov	T
GSA (Contractor)	Chris Louden	chris.louden@pgs.protiviti.com	P
GSA (Contractor)	Dave Shepherd	DSHEPHERD@lmi.org	P
GSA (Contractor)	Giuseppe Cimmino	giuseppe.cimmino@pgs.protiviti.com	P
GSA (Contractor)	John DiDuro	john.diduro@pgs.protiviti.com	P
GSA (Contractor)	Matt King	matthew.king@pgs.protiviti.com	P
GSA (Contractor)	Matt Kotraba	matthew.kotraba@pgs.protiviti.com	P
HHS	Toby Slusher	tus8@CDC.GOV	P
IRS	Srinivas Ganta	Srinivas.N.Ganta@irs.gov	T
IRS	Willie Spence	Willie.Spence@irs.gov	T
NASA	Terry Wyatt	terry.wyatt@nasa.gov	T
NASA	Tim Baldridge	tim.baldridge@nasa.gov	T
NRC	David Sulser	david.sulser@nrc.gov	P
SSA	Edward Spaay	Edward.Spaay@ssa.gov	T
Treasury	Drew McLain	Anthony.McLain@bpd.treas.gov	T
Treasury	Kurt Weaver	kurt.weaver@bdp.treas.gov	T
TSCP	Kyle Villano	Kyle.Villano@exostar.com	P
Verizon	Russ Weiser	russ.weiser@verizon.com	T
Not available	Lee Robinson	Not available	T

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

The Federal Public Key Infrastructure (FPKI) Technical Working Group (TWG) met at Protiviti Government Services, 1640 King Street, Suite 400, Alexandria, VA. Matt Kotraba called the meeting to order at 9:30 a.m. EST and introduced those in person and via teleconference.

Matt Kotraba discussed the FPKI TWG moving to monthly half-day sessions to ease the scheduling burden of all-day sessions, facilitate greater attendance, and allow for more frequent meetings to progress topics. The group agreed to the new scheduling approach and recommended the meeting be in the morning and in Alexandria, VA.

Chris Louden highlighted the significant breakthrough made in Microsoft acknowledging the design flaws of the Microsoft Crypto API (CAPI) path development engine. This accomplishment has been years in the making. Leveraging the TWG to bring to bear the power of the entire FPKI community to move technical issues forward applies to all vendors, not just to Microsoft.

Agenda Item 2
Public Encryption Certificate Lookup and Retrieval
Matt Kotraba, Kyle Villano, Jeff Barry

Matt Kotraba introduced the overall FPKI TWG objective for Encryption Certificate Lookup and Retrieval, which is to enable end user discovery of encryption certificates across the Federal PKI community. The current practices in place are cumbersome for end users and lead to the increased probability of sensitive emails being sent unencrypted. The TWG session focused on detailing an existing implementation at CertiPath using Transglobal Secure Collaboration Program (TSCP) Secure Email (SE) v.1 technical specification.

Kyle Villano, TSCP, and Jeff Barry, CertiPath, presented the TCSP SE technical specification, CertiPath's deployment of Community Service Provide-Lite (CSP-Lite) trusted directory service [http://www.certipath.org/certipath-bridge/member-resources/community-service-provider], the challenges with TSCP SE v.1, and the future of TSCP SE v.2.

- Important TSCP websites:
  - Home page – http://www.tscp.org
  - TSCP SE – http://www.tscp.org/index.php/implement/secure-e-mail
  - TSCP Implementation Guidance – http://www.tscp.org/images/stories/library/diysecureemailv2-3.pdf
  - LDAP Proxy Software – http://sourceforge.net/projects/ldap-proxy/
  - TSCP Membership – http://www.tscp.org/index.php/membership

FPKI TWG Discussion:

- Santosh Chokhani referenced an issue with the Microsoft Outlook client that was created during an Outlook update released last summer. The problem caused issues with the Outlook client not mining the encryption certificate from SMIME messages. The problem was subsequently patched in another Outlook update. However, Agencies may still experience the problem if they had patched Outlook using the first update but not one of the later updates that includes the fix. No hotfix was ever produced for this issue because it was patched in a regular Outlook update.
- Gary Moore referenced a server-based mining tool provided by Entrust that is being used to keep a repository of encryption certificates for Agencies and other organizations who have implemented the solution locally. Gary will provide the FPKI TWG with details on this solution.
- The use of outbound LDAP is a limitation within the Federal community. The use of HTTP was explored. Kyle Villano, TSCP, mentioned that TSCP had not specifically tested the use of HTTP, but believed it feasible to do so between an LDAP Proxy and the backend Directory Service. However, Kyle has not seen any email clients that leverage HTTP for communication between the email client and proxy or backend directory service. Santosh Chokhani referenced RFC 4387, http://www.rfc-editor.org/rfc/rfc4387.txt, which was written to address Certificate Store Access via HTTP.
- Tim Baldridge raised a concern over the ease of data mining from the outside to these directory services. Providers need to ensure they are not publishing unnecessary or extra identity information such as Universally Unique Identifier (UUID) or Federal Agency Smart Credential Number (FASC-N).
- The trust model deployed with CertiPath CSP-Lite implementation is managed manually through business processes. CSP-Lite members must already be cross-certificated with CertiPath.
- TSCP SE v.2 will be demonstrated in October. The demo will include the use of visual labels to aid end users in following the proper policies for encryption. The visual labels are achieved through a plug-in to the email client and maps to a policy table to support the specific instructions for end users.
- Several actions were identified toward meeting the overall objective:
    - The FPKI TWG owes a recommendation to the FPKIPA and ICAMSC on how to achieve the overall encryption certificate discovery and retrieval.
    - Following the TSCP SE guidance, one possibility is to have the FPKIMA manage a central lookup directory for trusted Agency directories, which contain the end user encryption certificates. This solution should be tested through the FPKI Community Interoperability Test Environment (CITE) to identify test cases, implementation challenges, and specific recommendations for FPKIPA and ICAMSC. The FPKIMA could possibly run a proxy for Agencies who do not have their own.

ACTIONS

- Gary Moore will provide FPKI TWG members a brief on the Entrust server-based encryption certificate mining tool.
- Matt Kotraba will coordinate a test of the TSCP SE solution through CITE. This will involve developing a Tiger Team (of FPKI TWG members).
    - Matt Kotraba will send a message to FPKI TWG members asking for Agency support of the CITE testing. NRC and NASA tentatively agreed to support the testing through CITE.

Agenda Item 3
Encryption Key History
Gary Moore

Gary Moore, Entrust, presented the details on the Entrust implementation of Encryption Key History on-card and server-side overflow. This solution is available today by those using Entrust CAs.

TWG Discussion:

- Using the Entrust solution, several Legacy PKIs (e.g. DHS and NASA) were able migrate their old encryption keys during the transition to a Shared Service Provider (SSP). These Agencies are able to leverage the key history and overflow services.
- The Entrust solution uses the PKIX Certificate Management Protocol (CMP) for communications between the client and CA during key recovery.
- No standardized EKU was available for the overflow certificate when the Entrust solution was developed.
- The Entrust solution was developed prior to the release of NIST SP 800-73-3, or any other standard. The Entrust solution differs in one key area from 800-73-3. 800-73-3 requires that key material be duplicated to a separate directory; and the Entrust solution keeps all key material protected at the secure CA database.
- NIST published a NIST Interagency Report (NISTIR) on “Maintaining and Using Key History on PIV cards”, http://csrc.nist.gov/publications/nistir/ir7676/nistir-7676.pdf. This paper complements 800-73-3 by providing some of the rationale for the design of the mechanism for storing retired Key Management Keys on PIV cards.
- The group was not aware of the specific policy requirements of the FBCA and Common Policy CPs. Specifically the group was interested in the policies for key recovery and requirements for storing key history of med-hardware keys on card.
- A point for future consideration is to adjust the FBCA and Common Policy CPs because 800-73-3 has specific functionality referenced.
- Another point for future consideration is to lead the authorship of an RFC on how to deal with key overflow.

ACTIONS

a. Jeff Jarboe will contact NIST (Cooper / McGregor) to set up a brief to discuss key history and overflow design choices in 800-73-3. The brief should be focused on the assumptions and decision factors for the 800-73-3 key history and overflow design, and identification of commercial products that have implemented this design.
b. Jeff Jarboe will coordinate a review of the FBCA and Common certificate policies to identify the policy requirements for key history and recovery.

Agenda Item 4
Microsoft Timestamp Authority Position Paper Update
Matt Kotraba, Santosh Chokhani, Gary Moore

Matt Kotraba provided an updated status of the FPKI TWG Microsoft Timestamp Authority (TSA) Position Paper. The FPKIPA Certificate Policy Working Group (CPWG) reviewed the paper and all comments were resolved at the September 8 CPWG. The paper was presented at the September 13 FPKIPA meeting and received endorsement of FPKIPA members. On September 14, Matt Kotraba sent the paper to Tom Albertson, Microsoft Root Certificate Program, Mike Burke, Microsoft Windows Security Program Manager, and Paul Fox, Microsoft PKI support team. The TWG recognized the contributions of Santosh Chokhani and Gary Moore in authoring the position paper.

How Microsoft responds to the position paper will affect how the TWG should follow-up. If Microsoft does not retract the TSA requirements, the TWG could potentially leverage FPKI Affiliates with Premier and Partner level support agreements to escalate the recommendations from the paper within Microsoft.

ACTIONS

- Matt Kotraba will follow-up with Microsoft, and distribute their response to the FPKI TWG.

Agenda Item 5
Developing Trust Store Management Guidance on the use of 3rd Party CAs (Prompted by the DigiNotar CA Compromise)
Matt Kotraba

Matt Kotraba presented the background on the DigiNotar compromise to the TWG.

- A high-level FPKI brief on the DigiNotar compromise was presented by Deb Gallagher to the Information Security and Identity Management Sub Committee (ISIMSC).
- The method used by the auditor of DigiNotar, Fox-IT, to identify fraudulent certificates was to review the DigiNotar Online Certificate Status Protocol (OCSP) server logs. It was recognized by the TWG that this method alone is

insufficient to identify fraudulent certificates because once the hacker compromised the CA they could have inserted any Uniform Resource Identify (URI) they wished into the OCSP URI on the certificate. This would allow the hacker to point the relying party to any OCSP service including one run by the hacker or none at all, focusing relying parties to default to Certificate Revocation List (CRL) checking.

- Curt Spann referenced a Microsoft Knowledge Base (KB) article on the required certificates needed for the Windows Operating System to run. See http://support.microsoft.com/kb/293781.
- Curt Spann and Tim Baldridge discussed Microsoft's approach to managing untrusted certificates. There are three levels (from highest to lowest: Enterprise, Local Machine, and User Profile) within the Windows trust store to publish untrusted certificates.
    - In Windows, Group Policy can be used to remove CA certificates from trust store ONLY if that CA was pushed to the trust store via Group Policy. In the case of the DigiNotar Root CA, in most cases it was pushed through the public trust process and not via Group Policy. Therefore DigiNotar cannot be able to remove via Group Policy. An alternative approach is to add the DigiNotar Root CA to the Untrusted Certificate store via Group Policy. This approach does not require the certificate to be removed from the Trusted Root CAs store since the Untrusted Certificate store takes precedence over the Trusted Root CAs store. This approach has the added benefit of using Group Policy in the future to remove the DigiNotar Root CA from the Untrusted Certificate store if you wish to trust the Root CA again.
- A question was raised regarding what trust store management guidance has been published by Federal Desktop Core Configuration (FDCC) and the US Government Configuration Baseline (USGCB), which replaced FDCC for Windows 7 and later. The following Windows configuration settings have been found in the FDCC and USGCB.
    - USGCB for Windows 7 has the automatic updates feature enabled (CCE-9403-7), security updates will be downloaded and notification given to the user to install. However, if an enterprise is using a patch management system, they can disable this setting and note it in the Agency policy deviation report. This setting does not mention Root Certificates by name.
    - FDCC for Windows XP (CCE-5054-2) and Vista (CCE-3454-6) requires enabling the "Turn off Automatic Root Certificate Updates" setting (HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot!DisableRootAutoUpdate). So in the case of XP and Vista the default setting is to manage the Root Store manually. This setting was not found in the Windows 7 USGCB. The assumption is automatic Root Certificate updates are left on for Windows 7 unless the Enterprise deviates from the standard.
- US Computer Emergency Readiness Team (USCERT) has made a post on DigiNotar. http://www.us-cert.gov/current/#fraudulent_diginotar_ssl_certificate.

USCERT encourages users and administrators to apply vendor updates to help mitigate the risk.

ACTIONS

a. Matt Kotraba will contact NIST to identify the trust store management guidance that has been published through USGCB and legacy FDCC.
b. Matt Kotraba will research the language in the FICAM Segment Architecture and Roadmap to identify its guidance on trust store management.
c. Matt Kotraba will 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.
d. A tiger team (of FPKI TWG members) should develop a technical recommendation paper identifying the current status of Federal guidance, and recommendations to improve Federal guidance and align existing Federal processes to include trust store management, such as USCERT and USGCB. Matt Kotraba will contact the FPKI TWG to identify members for the tiger team.

Agenda Item 6
Microsoft Path Building Anomalies
Santosh Chokhani

Santosh Chokhani reviewed the history of a critical Path Building design flaw in Windows XP and later that allows Microsoft CAPI to select longer invalid paths over valid shorter paths (Windows XP), and longer valid paths over valid shorter paths (Windows Vista and later). Microsoft PKI Support Group has acknowledged the issue. However, in order for them to take action, a design change request is needed from Microsoft Premier Support or Microsoft Partner level organizations. The more organizations who submit design change requests will help the Microsoft PKI Support Group justify the business case to assign resources within Microsoft.

The TWG was polled to see which members with Microsoft Premier Support or Microsoft Partner agreements are willing to submit design change requests. The following organizations volunteered to support the effort:

- NRC – David Sulser
- NASA – Tim Baldridge
- Verizon – Russ Weiser
- NIH – Deb Bucci (Previously identified outside of TWG)
- CertiPath – Jeff Barry

ACTIONS

a. Santosh Chokhani will provide a short one (1) page description of the Microsoft Path Building issue for those with Premier or Partner support to submit as part of the Design Change Request.
b. Matt Kotraba will coordinate the artifacts necessary for Premier and Partner organizations to submit to Microsoft. Organizations should send their helpdesk

ticket numbers to Matt Kotraba to ensure these tickets are properly identified so Microsoft understands that these tickets are all related.

c. Matt Kotraba will send a note to the FPKI-TTIPS list to identify who has a Microsoft Premier or Partner level support to submit the design change request

Agenda Item 7
FPKI Community Interoperability Test Environment (CITE) Update
Matt Kotraba

A short update on the FPKI CITE was provided by Matt Kotraba.

- The FPKI CITE guidelines, developed through the FPKI TWG, were released and posted on idmanagement.gov, http://www.idmanagement.gov/fpkima/documents/CITE_Participation_Guide.pdf.
- The FPKI CITE guidelines is a living document. Appendix A includes Test Policy Object Identifiers (OID). Participants should send updates for Appendix A to Jeff Jarboe, jeff.jarboe@pgs.protiviti.com.
- Points of contacts are needed for the FPKI-CITE@listserv.gsa.gov, please contact Matt Kotraba, matthew.kotraba@pgs.protiviti.com, to have POCs added.
- The TSCP SE solution for Public Encryption Certificate Lookup and Retrieval (Agenda Item 2) will be tested leveraging CITE.

ACTIONS
None.

Agenda Item 8
Adjourn Meeting
Chris Louden

The next FPKI TWG is tentatively scheduled for Tuesday October 25 (details pending). The group agreed that the primary focus of the next FPKI TWG should be a continuation of the following topics:

1. Trust Store Management
2. Public Encryption Certificate Lookup and Retrieval

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
2	Establish a mailing list and group collaboration calendar to coordinate testing activities.	FPKIMA (Matt Kotraba)	3/17/2011	8/31/2011	Closed
3	Draft a transition framework and coordinate comments with FPKI TWG members.	FPKIMA (Matt Kotraba)	3/17/2011	8/31/2011	On hold
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	Closed
8	FPKI TWG position paper on the Microsoft TSA requirement	Gary Moore	6/16/2011	8/31/2011	Closed
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	Closed
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	Closed
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
12	Send a message to the FPKI TWG members asking for Agency support of the CITE testing of TSCP SE Public Encryption Certificate Lookup and Retrieval	FPKIMA (Matt Kotraba)	9/15/2011	10/7/2011	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

No.	Action Item	Point of Contact	Start Date	Target Date	Status
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
15	Follow-up with Microsoft regarding the TSA position paper and distribute Microsoft's response to the FPKI TWG.	FPKIMA (Matt Kotraba)	9/15/2011	10/7/2011	Open
16	Contact NIST to identify the trust store management guidance that has been published through USGCB and legacy FDCC.	FPKIMA (Matt Kotraba)	9/15/2011	10/15/2011	Open
17	Research the language in the FICAM Segment Architecture and Roadmap to identify its guidance on trust store management.	FPKIMA (Matt Kotraba)	9/15/2011	10/15/2011	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	Open
19	Contact the FPKI TWG to identify members for the Trust Management Guidance tiger team.	FPKIMA (Matt Kotraba)	9/15/2011	10/15/2011	Open
20	Draft a short one (1) page description of the Microsoft Path Building issue for those with Premier or Partner support to submit as part of the Design Change Request.	Santosh Chokhani	9/15/2011	9/16/2011	Closed
21	Coordinate the artifacts necessary for Premier and Partner organizations to submit a design change request to Microsoft to fix the path building flaws identified in Windows.	FPKIMA (Matt Kotraba)	9/15/2011	9/16/2011	Closed

No.	Action Item	Point of Contact	Start Date	Target Date	Status
22	Send a message to the FPKI-TTIPS list to identify who has a Microsoft Premier or Partner level support to submit the design change request	FPKIMA (Matt Kotraba)	9/15/2011	9/30/2011	Open