Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

January 24, 2012

12:30 a.m. – 3:30 p.m. EST

12:30	Incident Management Process (joint session with CPWG)	Jeff Jarboe
1:30	Welcome & Opening Remarks Introductions	John DiDuro
2:00	CertiPath debrief on Microsoft Policy Mapping Issue meeting.	Jeff Barry Santosh Chokhani
2:30	Relying Party CRL caching and impacts of proposed FPKIMA HTTP Response Header changes.	Giuseppe Cimmino
3:00	Encryption Certificate Lookup	Wendy Brown
3:15	Actions and Next Steps	John DiDuro Wendy Brown
3:30	Adjourn Meeting	John DiDuro

Attendance List

Organization	Name	T-Teleconference P-Present A-Absent
NASA	Baldridge, Tim	P
CertiPath	Barry, Jeff	P
Verizon Business	Blanchard, Deb	T
GSA (Contractor)	Brown, Wendy	P
DoD (Contractor)	Chokhani, Santosh	T
Treasury	Curtis, Dave	T
GSA (Contractor)	DiDuro, John	T
State Department	Edmonds, Deb	T
State Department (Contractor)	Froehlich, Charles	P
DHS (Contractor)	Fuerst, Neal	T
DoD (Contractor)	Hansen, Maryam	P
USPTO	Jain, Amit	T
GSA (Contractor)	Jarboe, Jeff	P
State Department (Contractor)	Jung, Jimmy	P
GSA (Contractor)	King, Matt	P
GSA (Contractor)	Louden, Chris	T
Entrust	Moore, Gary	P
DOJ	Morrison, Scott	T
DigiCert	Rea, Scott	T
DHS (Contractor)	Shomo, Larry	T
GSA (Contractor)	Silver, Dave	T
Health and Human Services/Center of Disease Control	Slusher, Toby	T
CertiPath	Spencer, Judith	P
Nuclear Regulatory Commission	Sulser, Dave	P
Exostar	Villano, Kyle	T
SAFE	Wilson, Gary	T
Treasury Department	Wood, Dan	P
NASA	Wyatt, Terry	P

Agenda Item 1
Incident Management Process
(Joint session with CPWG)
Jeff Jarboe

Mr. Jeff Jarboe presented outstanding comments to the joint TWG/CPWG session for discussion and final adjudication. These comments were the few that the FPKI Incident Management Process tiger team needed further input on. Mr. Jarboe started with scope clarification –the Incident Management Process document aligns with ITIL terminology and concepts as much as possible. Accordingly, the document focuses in "incident management", which is separate and distinct from "problem management". The former focuses on resolving the immediate incident and impacts currently happening to the FPKI Community, while the latter focuses on root-cause analysis to prevent similar incidents from reoccurring.

Mr. Jarboe then walked the joint session through the several comments that needed discussion. Each item was addressed, either upholding the tiger team's planned adjudication, or specifying an alternative decision. One comment not cited for discussion was noticed, and upon discussion was reversed (changing "risk" to "vulnerability" in the Incident Types table was overruled after discussing their meanings and relationships in context of FIPS 199). All decisions were documented in the master comment sheet. The tiger team will now continue revising the document per today's decision. Document revision has progressed significantly, and is currently on schedule.

The suggestion was made that creation of an incident reporting template should be considered to ensure a consistent set of information per incident. At a minimum, the template should capture:

- Incident Description;
- Where the incident is occurring / being reported from;
- Whether there are any links to public articles; and
- Name of the person reporting the incident.

ACTIONS: None

Agenda Item 2
Welcome & Opening Remarks
Introductions--All Attendees
John DiDuro

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

Subsequent to the joint TWG/CPWG discussion, which was part of the CPWG meeting, Mr. John DiDuro called the TWG meeting to order at approximately 1:30 pm EST, and

introduced those in person and via teleconference. Mr. Chris Louden introduced Mr. DiDuro as the new TWG lead/coordinator, and noted that there would be no changes in direction or support. Mr. Louden also noted that the TWG and CPWG meetings are now being coordinated (e.g., today's CPWG in the morning, and the TWG session in the afternoon).

Agenda Item 3
CertiPath debrief on Microsoft Policy Mapping Issue meeting
Jeff Barry and Santosh Chokhani

Mr. Jeff Barry presented a debrief of the late December 2011 meeting between CertiPath, NIST, and Microsoft. Mr. Trevor Freeman is the key Microsoft point of contact for the PKI community, The meeting focused on known CAPI issues:

1. Policy mapping issue
2. Path length/Rating
3. Name constraints
4. EKU
    a. Code signing
    b. Intermediate EKU processing

All four issues affect anyone doing PKI in a federated environment.

There was a brief discussion about the policy mapping issue. When there are many issuer policy OIDs mapped to a single subject policy OID, only the first mapping is used by CAPI. The other mappings are ignored (i.e., additional mappings after the subject domain is first encountered are ignored). This can happen at any point in the certificate chain. We may need to be deliberate about ordering in a given cross-certificate. Where exactly their bug is may determine the best way to address/fix the issue. For example, the first mapping should be the peer-to-peer mapping (Medium HW to Medium HW by rule). Certipath's approach is incremental improvements – reordering bridge certificates upon reissuance. Microsoft claims that multiple mappings within a cross-certificate is beyond the RFC standard, and as proof stated that PKITS doesn’t test for it.

The name constraint issue is that name constraints are not being enforced on intermediate CAs. It is enforced only on end-entity certificates. nameConstraints cannot be parsed by Apple when it is critical. Microsoft says that an unconstrained name form is not permitted if there are any name constraints. Microsoft does not view this as an issue because a workaround (registry patch) exists. Therefore, Microsoft action on this issue is unlikely.

Mr. Freeman reluctantly agreed that the EKU issues extend the attack vector beyond acceptability, but didn’t commit that Microsoft would do anything about it. In addition, Microsoft states that the codesigning EKU is not required even on the end-entity certificate used for code signing.

Mr. Dave Cooper and Mr. Tim Polk are considering PKITS enhancements such as adding tests for the policy mapping, path length, and nameConstraints as these are path validation related. However, EKU on cross-certificates may be held in metadata and therefore may be out of scope for PKITS tests.

The TWG then discussed the best way for the FPKI Community to use leverage to force Microsoft to make changes. A two-fold approach was recommended:

1) Orchestrate a campaign that mobilizes federal agencies to flood Microsoft with problem tickets (all agencies, not just those with platinum-level support contracts); and
2) The TWG aggregates problem tickets and sends the package to Mr. Freeman, who will champion the fix within Microsoft.

It is important to note that problem reports should be couched as a security concern. Tickets, and especially the aggregation package, should point to areas where Microsoft incorrectly processes RFC guidance – those will rise to the top of the Microsoft queue and get the attention of staff at the Redmond headquarters.

Mr. Freeman left open the possibility that Bridge CA representatives may be looked upon differently within Microsoft. While small in number, it was noted that we collectively represent a huge community of Microsoft users. To get Microsoft's attention, we have to figure out how to show that we represent 3-5% of Microsoft's customer base. This is hard to do, but possible when we extend our U.S. federal base to include international communities such as AeroSpace Defense and BioPharma.

NIST has a mechanism to generate Internal Reports – short instructional pieces – published as best practices. These are similar in detail to Microsoft TechNet articles. Mr. Polk expressed an interest in publishing a NIST IR for Best Practices for Trust Anchor Management.

ACTIONS

1. Ms. Wendy Brown will look at the order of certificate mapping in cross-certificates issued by the FPKI Trust Infrastructure CAs.
2. Mr. John DiDuro will facilitate a TWG/NIST follow-up meeting to discuss PKITS changes that address the Microsoft CAPI issues discussed above and planning (targeting Feb/March 2012 timeframe). We also need to encourage the TWG to provide inputs.
3. The TWG needs to develop a strategy to handle current and future issues with Microsoft products.

Agenda Item 4
Relying Party CRL caching and impacts of proposed FPKIMA HTTP Response Header changes
Giuseppe Cimmino

Mr. Giuseppe Cimmino, FPKIMA Platform Team lead, briefed the TWG about efforts to improve overall FPKI resiliency, including scalability, reliability, efficiency, and security. FPKI repository usage continues to grow. There were 1.2 billion transactions last reporting month. Transactions used to be in the millions per month.

LDAP has real weaknesses (easily attacked) that can cause real security issues if we continue using it. Therefore, a key FPKIMA objective is to move towards HTTP, and away from LDAP.

The question was asked: are there any RFCs that specify what to do with HTTP headers in regards to CRLs? Mr. Cimmino only found something in regards to the use of OCSP in RFC 5019.

The TWG finds the objective of moving away from LDAP URIs to only HTTP satisfactory. Mr. Tim Baldridge noted this is a move towards the best commercial practice of removing LDAP URIs out of cross-certificates. Mr. Baldridge then asked the broader question of how do we implement this guidance beyond the FPKIMA, specifically, NASA would like their SSP's to follow suit. It was also noted that there is potential to generate a new RFC as a result of implementing these techniques.

Mr. Baldridge opined that the objection Mr. Cooper made to the FPKIMA about removing LDAP URIs from cross-certificates is that common policy should be subordinate to FIPS 201 which still mandates LDAP URIs. FPKI Profile clarifications must first be made to get the Profiles to agree with the policy change of making LDAP optional. There is some urgency to get FIPS 201 updated to account for this approach. Mr. Baldridge will take this issue to the ICAM AWG to recommend to NIST that it make LDAP optional in the next FIPS 201-2 public draft.

ACTIONS

4. Ensure that 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.

Agenda Item 5
Encryption Certificate Lookup
Wendy Brown

Ms. Wendy Brown, FPKIMA Community Team Lead, briefed the TWG on the planned effort to identify and test viable encryption certificate lookup models for use by the FPKI Community.

Two models have already been identified for testing: (1) TSCP model, and (2) LDAP proxy chaining model.

Several test partner volunteers have been identified, but the FPKIMA would welcome more volunteers. Once volunteers are identified, the group will refine requirements and selection criteria. The objective is to identify a solution that allows email clients to search by email address or recipient name, obtain an encryption certificate, and send encrypted email to that recipient.

Test partners will have some responsibilities, including providing a repository, using email clients that can look up encrypted certificates and that can send encrypted emails, and providing read access to their Repository.

Various tests will be performed, and could be as simple as finding an encrypted certificate and sending encrypted emails.

Several decisions need to be made (1) what certificates should be used (e.g., issuing test certificates, using productions certificates in the test environment), (2) which email clients should be used, (3) what are the partner repository requirements (e.g., LDAP, HTTP), and (4) what type of read (e.g., anonymous read, authenticated read and by what means). Ms. Brown indicates that using production certificates in the test environment is preferred.

NASA has both test and production LDAP repositories with anonymous read. Accordingly, NASA is now a test partner. Additional test partners were noted (e.g., NCR, CertiPath).

It should be noted that this method encourages the use of LDAP where the previous briefing (by Mr. Cimmino) discourages use of LDAP. However, Mr. Cimmino's briefing was infrastructure-centric. Ms. Brown's briefing is client-centric (i.e., enabling ease of encrypted email).

This approach opens up the possibility of the FPKIMA running a proxy for email look-up via LDAP.

ACTIONS

5. Ms. Brown to schedule a planning meeting with test volunteers.

Agenda Item 6
Acton and Next Steps
John DiDuro

ACTIONS

6. Mr. DiDuro to create and publish a TWG list of documents written to-date.

Agenda Item 7
Adjourn Meeting
John DiDuro

Mr. DiDuro adjourned the TWG meeting at approximately 3:30 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	Open
39	Create and publish a TWG list of documents written to-date.	TWG (J.DiDuro)	1/24/2012	February 2012	Open