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

## December 20, 2011

**9:00 a.m. – 12:00 p.m. EST**

---

| | | |
|---|---|---|
| 9:00 | Welcome & Opening Remarks<br>Introductions | Matt Kotraba |
| 9:05 | CertiPath brief on Microsoft Policy Mapping Issue | Jeff Barry<br>Santosh Chokhani |
| 10:05 | Comment Review: FPKI TWG Recommendations to Enhance Trust Store Management, White Paper | Matt Kotraba<br>Dave Silver |
| 12:00 | Adjourn Meeting | Matt Kotraba |

**Attendance List**

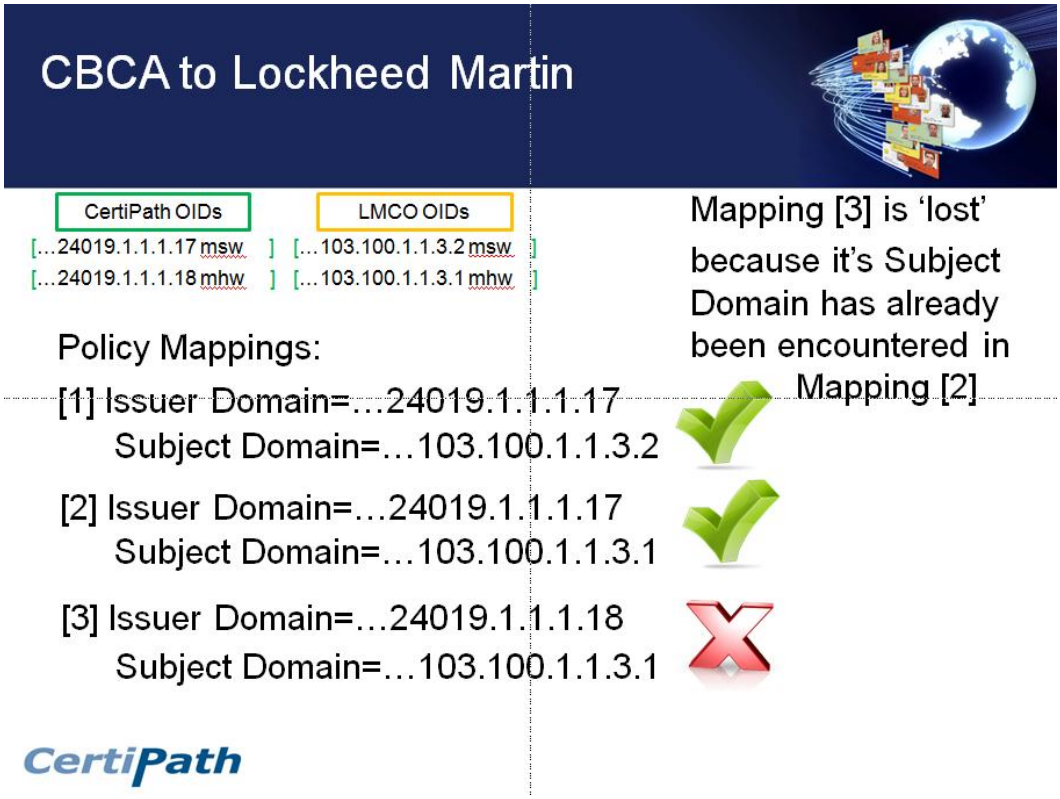
| Organization Supported | Name | Email | P-Present/ T-Teleconference |
|---|---|---|---|
| CertiPath | Jeff Barry | jeff.barry@certipath.com | P |
| CertiPath | Judy Spencer | Judy.Spencer@certipath.com | P |
| Department of Defense (Contractor) | Curt Spann | spann_curt@bah.com | T |
| Department of Defense (Contractor) | John Salgado | Salgado_John@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 | Neal Fuerst | Neal.Fuerst@ASSOCIATES.HQ.DHS.GOV | T |
| Entrust | Gary Moore | gary.moore@entrust.com | P |
| eValid8 | Jim Schminky | james.schminky@evalid8.com | P |
| GSA | Darlene Gore | darlene.gore@gsa.gov | T |
| GSA (Contractor) | Matt King | matthew.king@pgs.protiviti.com | P |
| GSA (Contractor) | John DiDuro | john.diduro@pgs.protiviti.com | P |
| GSA (Contractor) | Matt Kotraba | matthew.kotraba@pgs.protiviti.com | P |
| GSA (Contractor) | Wendy Brown | wendy.brown@pgs.protiviti.com | P |
| GSA (Contractor) | Dave Silver | dave.silver@pgs.protiviti.com | T |
| GSA (Contractor) | Jeff Jarboe | Jeff.jarboe@pgs.protiviti.com | P |
| Safe-Biopharma | Gary Wilson | gwilson@SAFE-BIOPHARMA.ORG | T |
| SSA | Amy Harding | Not available | P |
| Treasury | Jason Hall | Jason.Hall@bpd.treas.gov | T |

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

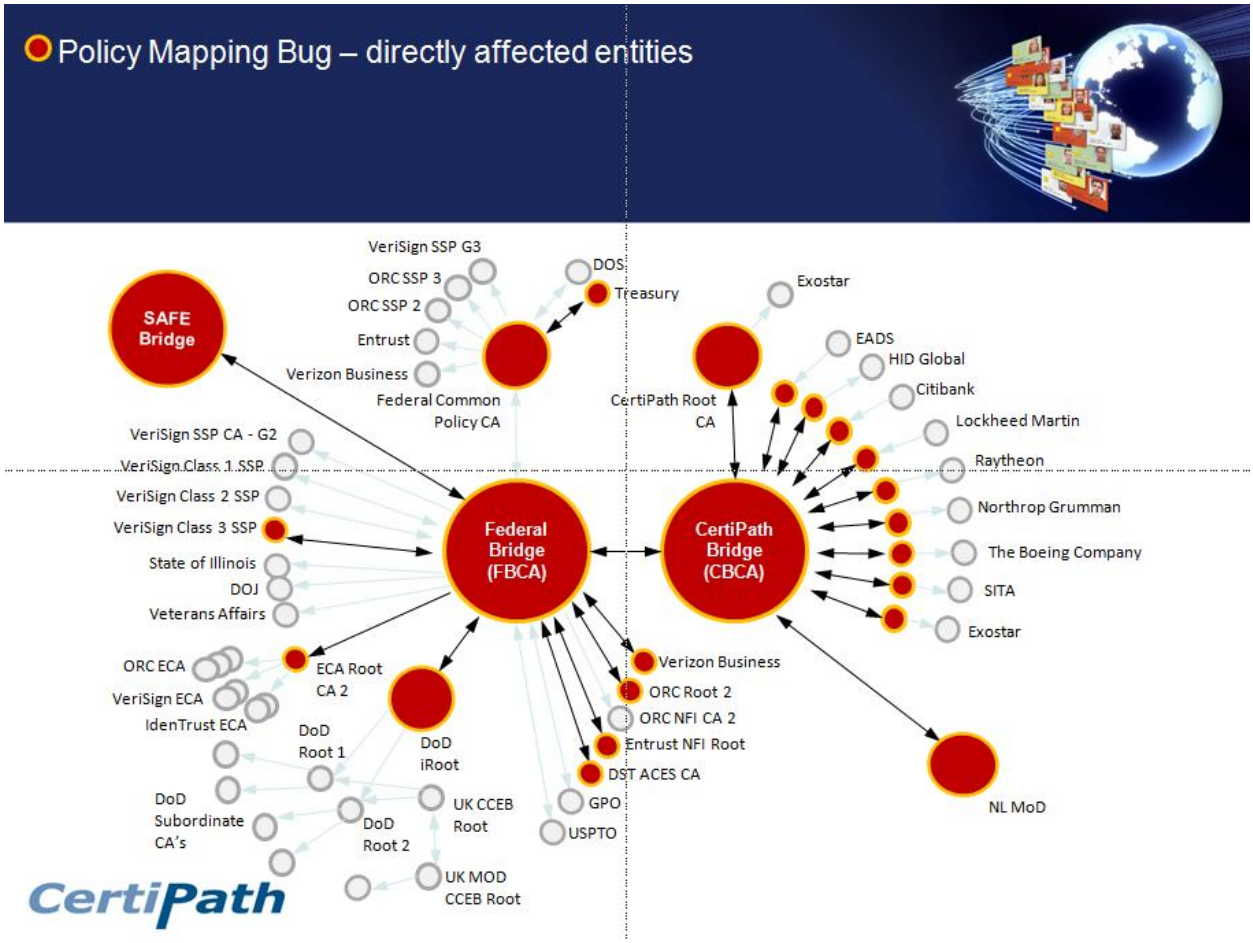
The Federal Public Key Infrastructure (FPKI) Technical Working Group (TWG) met at Protiviti Government Services, 1640 King Street, Suite 400, Alexandria, VA. Matt Kotraba called the meeting to order at 9:00 a.m. EST and introduced those in person and via teleconference.

## Agenda Item 2
## CertiPath brief on Microsoft Policy Mapping Issue
## Jeff Barry

Jeff Barry presented a policy mapping issue, discovered by CertiPath, in the Microsoft Cryptographic Application Programming Interface (CAPI) used in Windows system for PKI processing. The issue occurs when multiple policies from the Certificate Issuer domain are mapped to the same policy in the subject domain, CAPI only picks the first of the mappings. The issue is depicted below.



The policy mapping issue is magnified as the number of bridges and mappings increases through a trust path. The picture below shows the affected entities of the CertiPath and Federal Bridge PKIs.




CertiPath is scheduled to meet with Microsoft and National Institute of Standards and Technology (NIST) to discuss this issue on December 22, 2011. CertiPath extended an invitation to the FPKI, as was done at the December FPKIPA meeting, to attend the session. NIST is looking to modify the PKI Test Suite (PKITS) to include testing for this issue.

**ACTIONS**

1. CertiPath will present the results of the December 22, 2011 Microsoft/NIST/CertiPath meeting to the FPKI TWG.

## Agenda Item 3
## Comment Review: FPKI TWG Recommendations to Enhance Trust Store Management, White Paper
## Matt Kotraba

Matt Kotraba lead the review of TWG member comments pertaining to the FPKI TWG white paper entitled *Recommendations to Enhance Trust Store Management*. Consensus was reached on all comments. Matt Kotraba and Dave Silver will make the final edits per the TWG review and finalize the document for publication to the TWG, CPWG, and FPKIPA.

**ACTIONS**

- Matt Kotraba and Dave Silver to finalize recommendations white paper and distribute the final paper to the TWG, CPWG, and FPKIPA.

## Open Discussion

Time allowed the introduction of new topics and a review of the TWG docket.

- CodeSigning EKU Security Issue – Through the TWG interactions with Microsoft (reference: Timestamping Requirements for CodeSigning and the white paper entitles *FPKI TWG Code Signing and Timestamp Authority Recommendations for Microsoft*), CertiPath has identified a potential major security issue in the way Microsoft CAPI processes signed code. The issue would allow for end entity certificates to be used to digitally sign code even though those certificates were not intended for code signing. The TWG concluded that a small group of TWG members should meet with Microsoft to review this issue and determine if the issue is valid or if there are any misunderstandings regarding how CAPI processes signed code.
- A CertiPath update on the December 22, 2011 CertiPath/NIST/Microsoft meeting was identified as topic for the January 2012 TWG meeting.

**ACTIONS**

1. 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 regarding Microsoft CAPI's code signing processes.
2. Add CertiPath's issue update to the January 2012 TWG meeting agenda.

## Agenda Item 4
## Adjourn Meeting
## Matt Kotraba

The next FPKI TWG meeting is scheduled for Tuesday, January 24, 2012 from 12:30 p.m. to 3:30 p.m. EST. The meeting location is 1640 King Street, Suite 400, Alexandria, VA. Teleconference and Live Meeting will be provided for remote attendees.

The February 2012 TWG meeting was moved to Thursday, February 23, 2012 due to the Presidents Day holiday, which shifted the FPKIPA and CPWG schedules. February's meeting will held from 9:00 a.m. to 12:00 p.m. EST.

Matt Kotraba adjourned the FPKI TWG meeting at 11:20 a.m. 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 | Open |
| 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's issue update to the January 2012 TWG meeting agenda. | FPKIMA | 12/20/2011 | 12/20/2011 | Closed |