

[Primary Menu](#)

Federal Public Key Infrastructure Policy Authority (FPKIPA)

The FPKIPA serves the interest of U.S. Federal Government organizations as relying parties and promotes interoperability between federal and non-federal entities by:

- Setting policy governing the FPKI Trust Infrastructure;
- Approving applicants for cross certification with the FBCA; and
- Providing oversight to the Certified PKI Shared Service Provider (SSP) Program.

Activities

- **Approve Policies and Practices** – Approve Federal Bridge Certification Authority (FBCA) and Federal Common Policy Certification Authority Certificate Policies (CPs), including revisions; approve FPKI Trust Infrastructure Certification Practice Statements.
- **Approve Entity Cross-Certification** – Establish and administer criteria and methodology for cross-certification with the FBCA; approve cross-certifications and execute Memoranda of Agreement (MOAs); maintain the FPKI Certification Applicant Requirements and the Common Policy CPS Evaluation Matrix.
- **Maintain Compliance** – Ensure cross-certified entities are compatible with the FBCA CP (or the FCPCA CP for Federal Legacy CAs).
- **Agreement with FPKI Management Authority** – Oversee the FPKI Management Authority (FPKIMA) to issue and revoke cross-certificates, ensure adherence to the FPKI CPs, and provide documentation to be archived.
- **Interoperability Practices** – Coordinate legal, policy, technical, and business practices and issues related to FPKI Trust Infrastructure.

Membership

Members are appointed by each federal agency's CIO, and the group operates under the authority of the Federal CIO Council through the Information Security and Identity Management Committee (ISIMC) and the Identity, Credential, and Access Management Subcommittee (ICAMSC). See the [FPKIPA Charter \(/wp-content/uploads/sites/1171/uploads/FPKIPA_charter_1.0_Final.pdf\)](#). (PDF, February 2015) for information on membership requirements, voting rights, etc.

Working Groups

The following working groups support the work of the FPKIPA.

- [FPKI Certificate Policy Working Group \(CPWG\) \(/cpwg\)](#).
- [FPKI Shared Service Provider Working Group \(SSPWG\) \(/sspwg\)](#).
- [FPKI Technical Working Group \(TWG\) \(/twg\)](#).

Meetings

The FPKIPA meets in the morning on the second Tuesday of each month. Notes from past meetings will be listed here as they become available.

Page Reviewed/Updated: October 11, 2017



(<https://gsa.gov>)

[Contact Us \(/contact us\)](#)

[Privacy Policy \(/privacy-policy\)](#)

[Website Policies \(/website policies/\)](#)



(<https://cio.gov>)

[USA.gov \(https://usa.gov\)](#) | [Whitehouse.gov \(https://whitehouse.gov\)](#) | [FOIA.gov \(https://foia.gov\)](#)



Federal Public Key Infrastructure Policy Authority Charter

Version 1.0

February 1, 2015

BACKGROUND AND PURPOSE

BACKGROUND

The Federal Public Key Infrastructure (FPKI) is supported by the FPKI Policy Authority (PA) and the FPKI Management Authority (MA). GSA's Office of Government-wide Policy currently provides secretariat and subject matter expertise support for the PA, while the MA is run by GSA's Federal Acquisition Services and provides operational support and maintains the FPKI Trust Infrastructure in accordance with the FPKI Certificate Policies and Certification Practice Statements approved by the PA.

The PA was codified by the Federal Chief Information Officers Council in 2000 to serve as the Federal Bridge governing body. The PA includes entities operating enterprise Public Key Infrastructures (PKIs) cross-certified with the Federal Bridge Certification Authority (FBCA) or the Federal Common Policy Certification Authority (FCPCA) or who have acquired PKI services under the Shared Service Provider (SSP) Program, and who have demonstrated their interest in participating in the work of the PA.

FPKI VALUE STATEMENT

The FPKI provides numerous services that directly benefit federal agency business needs and objectives,¹ including fundamental high-assurance trust services for a wide variety of customers. It contains the Federal Government's PKI trust anchor and facilitates trust of Personal Identity Verification (PIV), PIV-Interoperable (PIV-I), and other government and non-government credentials. As a result, the FPKI is essential for federal agency physical and logical access solutions and is of great importance to citizens, businesses, and organizations that need access to federal agency services and facilities.

The FPKI is needed for federal agencies to comply with HSPD-12 and Executive Office of the President (EOP) [Office of Management and Budget \(OMB\) Memorandum M-11-11](#), accept PIV-I Cards, and accept third-party credentials as discussed in [National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#) and directed by [OMB VanRoekel Memorandum dated October 6, 2011](#). In addition, the FPKI is a key enabler of electronic business process flows within and between organizations and supports other Federal Identity, Credential, and Access Management (FICAM) initiatives, such as Backend Attribute Exchange.

AUTHORITY

The PA operates under authority of the Federal CIO Council through the Information Security and Identity Management Committee (ISIMC) and the Identity, Credential, and Access Management Subcommittee (ICAMSC).

The Federal CIO Council or its assignee issues and updates this charter of operations; appoints the PA leadership; and oversees FPKI responsibilities, work plans, and priorities.

¹ See [The Realized Value of the FPKI](#) for federal agency use cases and benefits attained.

PURPOSE

The PA sets policy governing the FPKI Trust Infrastructure; approves applicants for cross certification with the FBCA, including PIV-I issuers, and provides oversight for the Certified PKI SSP Program. The PA serves the interest of U.S. Government organizations as relying parties and promotes interoperability between federal and non-federal entities.

RESPONSIBILITIES OF THE FEDERAL PKI POLICY AUTHORITY

The PA has the following responsibilities:

CP/CPS CHANGE AND APPROVAL

- Approving the [FBCA Certificate Policy \(CP\)](#), including revisions
- Approving the [FCPCA CP](#), including its revisions
- Approving the [EGCA CP](#), including its revisions
- Approving the [FPKI Trust Infrastructure Certification Practices Statements \(CPS\)](#)

APPROVAL OF ENTITY CROSS-CERTIFICATION

- Establishing and administering the *Criteria and Methodology for Cross-Certification with the U.S. FBCA* [[CRITS&METHODS](#)] for entities wishing to cross-certify with the FPKI, including the approval of all entity cross-certifications and execution of resultant Memoranda of Agreement (MOA)
- Maintaining the FPKI Certification Applicant Requirements (mapping criteria for the FBCA) and the Common Policy CPS Evaluation Matrix to ensure continued accuracy and relevance in relation to the supported policies

MAINTAIN COMPLIANCE

- Ensuring cross-certified entities remain compatible with the FBCA CP (or the FCPCA CP for Federal Legacy CAs) by implementing the enforcement mechanisms in the [[CRITS&METHODS](#)]
- Ensuring that Certified SSPs comply with the ongoing requirements for participation including requirements for maintaining compliance as described in the [SSP Roadmap](#)

AGREEMENT WITH FPKI MANAGEMENT AUTHORITY

Establishing and maintaining a relationship with the FPKI Management Authority (MA), to include:

- Directing the MA concerning the issuance and revocation of cross-certificates
- Ensuring MA continued adherence to the FPKI CPs
- Providing documentation to the MA for archives

INTEROPERABILITY PRACTICES

Coordinating legal, policy, technical, and business practices and issues related to FPKI Trust Infrastructure interoperability.

MEMBERSHIP AND ORGANIZATION

MEMBERSHIP

Membership in the PA is open to federal agencies that have cross-certified with the FBCA or FCPCA, federal agencies using PKI certificate services acquired through an approved SSP, cross-certified non-federal government PKIs and PKI bridges that have a fully-executed MOA or contract with the federal government, and ex officio members as designated below.

Each federal agency representative shall be appointed by the CIO of their agency.

Membership terminates if and when the Entity (Shared Service Providers, Bridges Cross Certified with the FPKI) ceases to operate its cross-certified CA or PKI SSP model or chooses not to participate in the PA.

Voting membership for the PA is reserved for federal entities. All other members are non-voting.

Voting Membership

Voting membership for the FPKIPA is reserved for federal entities:

FPKI Cross Certified Federal Entities

All federal agencies, independent commissions, and organizations that operate self-signed PKIs that have successfully completed the process of cross-certifying with the FPKI Trust Infrastructure in accordance with [[CRITS&METHODS](#)] are eligible to be voting members of the FPKIPA.

Agencies Acquiring Certificate Services through a Certified PKI SSP

Federal agencies acquiring PKI certificate services from a Certified PKI SSP are eligible to be voting members of the FPKIPA.

General Criteria for All Voting Members

Voting membership in the FPKIPA for eligible federal entities is granted and maintained under the following circumstances:

- a) The agency requests to become a new voting member of the FPKIPA, and
- b) The agency makes the requisite commitment of time and resources as evidenced by regular FPKIPA and working group participation.

Ex Officio Membership

The following have ex officio membership:

- (1) OMB and designees from the Federal CIO Council
- (2) Co-chairs of the ICAMSC
- (3) Program Managers of MA and PA
- (4) Other representatives as appointed by the Co-Chairs of the PA.

Ex officio membership does not confer voting privileges, but are welcome to participate on working groups and subcommittees at their discretion.

COMMITTEES/WORKING GROUPS

The Co-Chairs of the PA may create or dissolve working groups to support its activities. Each group established under the PA shall have a Chair or Co-Chairs appointed by the PA Co-Chairs and announced to the PA membership. A working group Chair must be a federal employee; however, a non-federal employee supporting a voting member organization may be appointed as a Co-Chair.

The current existing working groups of the PA are:

FPKI Certificate Policy Working Group (CPWG)

Reviews and maintains Applications for Cross-Certification, CPs, CP Change Proposals, and auditor reports of entities that apply for or seek to maintain cross-certification with the applicable FPKI Trust Infrastructure CA at a specific level of assurance, and recommends to the PA the acceptance or rejection of these entity applications, CPs, and audit reports.

The CPWG also maintains FPKI CPs, administrative and guidance documents (e.g. Criteria and Methodology for Cross-Certification with the U.S. Federal Bridge Certification Authority (FBCA), FPKI Certification Applicant Requirements) and recommends changes to those documents to the PA.

PKI Shared Service Provider Working Group (SSPWG)

Oversees the processes involved in the Certified PKI Shared Service Provider (SSP) Program. These processes are documented in the SSP Roadmap document. SSPWG Membership is limited to federal employees and direct-support contractors on behalf of their agencies, as well as approved PKI SSP vendors.

FPKI Technical Working Group (TWG)

Reviews and provides advice about technical issues related to the FPKI at the request of the PA, CPWG, or Federal PKI MA.

LEADERSHIP

PA Co-CHAIRS

There shall be two co-chairs of the PA. Both will be appointed by the Federal CIO Council or its assignee. The Federal CIO Council will also determine which Co-Chair shall be the signatory executor of all PA documents, such as CPs, MOAs, LOAs, etc.

The Co-Chairs shall, at a minimum, be responsible for:

- Chairing PA meetings
- Serving as liaison in keeping the Federal CIO Council or its assignees informed of PA activity

Federal Public Key Infrastructure Policy Authority Charter

- Ensuring the PA adheres to the Federal CIO Council-approved responsibilities, work plans, and priorities and coordinating all FPKI activities, such as promoting the use of PKI to serve the interest of the Federal Government and other organizations (i.e. commercial, international, etc.)
- Determination of remedies/actions to be taken for noncompliance and/or unacceptable risk, or to restore Federal Bridge Certification Authority (FBCA) and Federal Common Policy CA (FCPCA) interoperability following cross-certificate revocation.
- Re-issuance of a Member's cross-certification under extraordinary circumstances.
- Sending compliance audit letter notifications

OPERATIONS

MEETINGS

PA meetings shall be held on a regular schedule as determined by the PA Co-Chairs. The meeting time and location may be modified as needed.

The quorum necessary for the PA to transact official business shall be two-thirds (2/3) of the voting membership. A transmitted proxy to an attending member shall also count toward a quorum.

VOTING

The Co-Chairs shall decide when a vote is to be taken, either during a meeting or outside a meeting by email. The Co-Chairs will first ask for a general vote of all members in favor and all members opposed. Only for more controversial or split votes will a roll call vote be used. A Voting Member may provide a proxy to another Voting Member during a single meeting.

Voting Members may request a vote without a meeting or the Co-Chairs call for online discussion and/or voting, (i.e., "Call for an Electronic or Email Vote"). Voting Members shall have at least five business days to vote. The Co-Chairs may request a shorter timeframe when the need is urgent.

Electronic Voting

When a member votes by electronic means (e.g., email), the electronic vote shall be signed to indicate the member's intent to vote and confirm that member's identity. The electronic vote should contain a valid PKI digital signature. Failure to use the above methods shall cause the electronic vote to be considered invalid and not counted in the tally. The Co-Chairs may waive the requirement to use a valid PKI digital signature for a voting member in a case-by-case basis.

[Primary Menu](#)

Certificate Policy Working Group (CPWG)

The Federal Public Key Infrastructure (FPKI) Certificate Policy Working Group (CPWG) serves as a policy advisory group to the FPKI Policy Authority (FPKIPA). The CPWG provides recommendations on policy mappings and changes to the Federal Bridge Certification Authority (FBCA) and Federal Common Policy Certification Authority (FCPCA) Certificate Policies. CPWG activities include:

- Facilitating proposed changes to the FPKI Certificate Policies.
- Facilitating the process for organizations wishing to cross certify with the FPKI.
- Addressing and resolving specific issues through policy analysis and modification.

Membership

The CPWG is open to employees and designated contractors from federal agencies, as well as commercial and non-profit participants.

- To join, [send us an email \(mailto:icam@gsa.gov\)](mailto:icam@gsa.gov) and include the text "Request to Join CPWG" in the subject line.

Meetings

The CPWG meets as needed. Attendees can participate either in-person or via teleconference.

Page Reviewed/Updated: February 6, 2018



(<https://gsa.gov>)

[Contact Us \(/contact-us\)](/contact-us)

[Privacy Policy \(/privacy policy\)](/privacy-policy)

[Website Policies \(/website-policies/\)](/website-policies/)



(<https://cio.gov>)

[USA.gov \(https://usa.gov\)](https://usa.gov) | [Whitehouse.gov \(https://whitehouse.gov\)](https://whitehouse.gov) | [FOIA.gov \(https://foia.gov\)](https://foia.gov).

[Primary Menu](#)

Shared Service Provider Working Group (SSPWG)

The Shared Service Provider (SSP) Working Group (WG) makes recommendations to the Federal Public Key Infrastructure Policy Authority (FPKIPA) on policy mappings and proposed changes related to the Federal Public Key Infrastructure Shared Services Program.

Activities

- Identify proposed changes to the Federal Public Key Infrastructure Common Policy that impact the Shared Services Program.
- Analyze and modify policy to address and resolve issues that impact the Shared Services Program.

Membership

The SSPWG meets on an as needed basis, and is only open to approved SSPs.

Page Reviewed/Updated: December 22, 2016



(<https://gsa.gov>)



(<https://cio.gov>)

[Contact Us \(/contact-us\)](/contact-us)

[Privacy Policy \(/privacy-policy\)](/privacy-policy)

[Website Policies \(/website-policies/\)](/website-policies/)

USA.gov (<https://usa.gov>) | Whitehouse.gov (<https://whitehouse.gov>) | FOIA.gov (<https://foia.gov>).

[Primary Menu](#)

FPKI Technical Working Group (TWG)

The TWG focuses on advancing Public Key Infrastructure (PKI) technology. It investigates and resolves complex technical issues and proposed modifications to the Federal PKI (FPKI).

Activities

- Identify and scope technical issues that impact the operation of the FPKI
- Address security concerns and vulnerabilities that could weaken the FPKI Trust Fabric
- Identify technical improvements to enhance the security and operational capabilities of the FPKI

Membership

This group is open to technical participants from federal agencies and their contractors. There are no formal membership requirements, and anyone from a federal agency or who supports an agency may attend.

- To join, [send us an email \(mailto:fpki@gsa.gov\)](mailto:fpki@gsa.gov) and include the text **"Request to Join TWG"** in the subject line.

Meetings

The group meets quarterly, in-person, at GSA Headquarters, 1800 F Street NW, Washington DC. Attendees can also participate via teleconference.

- The next meeting is scheduled for June.

Notes from Past TWG Meetings

- [April 2018 \(http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKI-TWG-201804-Minutes.pdf\)](http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKI-TWG-201804-Minutes.pdf). (PDF)

- [January 2018 \(http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKITWG-201801-Minutes.pdf\)](http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKITWG-201801-Minutes.pdf). (PDF)
- [July 2017 \(http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKI-TWG-201707-Minutes.pdf\)](http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKI-TWG-201707-Minutes.pdf). (PDF)
- [April 2017 \(http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKI-TWG-201704-Minutes.pdf\)](http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKI-TWG-201704-Minutes.pdf). (PDF)
- [July 2015 \(/wp-content/uploads/sites/1171/uploads/FPKI-TWG-Minutes-July2015.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI-TWG-Minutes-July2015.pdf). PDF)
- [March 2015 \(/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-TWG_20150325.pdf\)](/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-TWG_20150325.pdf). (PDF)
- [December 2014 \(/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-20141219_0.pdf\)](/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-20141219_0.pdf). (PDF)
- [July 2014 \(/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-TWG_20140730_0.pdf\)](/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-TWG_20140730_0.pdf). (PDF)
- [June 2014 \(/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-TWG_20140611.pdf\)](/wp-content/uploads/sites/1171/uploads/Minutes_FPKI-TWG_20140611.pdf). (PDF)
- [June 2012 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_Meeting_Minutes_062112.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_Meeting_Minutes_062112.pdf). (PDF)
- [May 2012 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_Meeting_Minutes_051512.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_Meeting_Minutes_051512.pdf). (PDF)
- [March 2012 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_032212.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_032212.pdf). (PDF)
- [February 2012 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_0212.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_0212.pdf). (PDF)
- [January 2012 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_012412.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_012412.pdf). (PDF)
- [December 2011 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_122011.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_122011.pdf). (PDF)
- [October 2011 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_102511.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_102511.pdf). (PDF)
- [September 2011 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_091511.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_091511.pdf). (PDF)
- [June 2011 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_061611.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes_061611.pdf). (PDF)
- [March 2011 \(/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes031711.pdf\)](/wp-content/uploads/sites/1171/uploads/FPKI_TWG_minutes031711.pdf). (PDF)

Page Reviewed/Updated: May 1, 2018



(<https://gsa.gov>)

[Contact Us \(/contact-us\)](/contact-us)

[Privacy Policy \(/privacy policy\)](/privacy-policy)

[Website Policies \(/website-policies/\)](/website-policies/)



(<https://cio.gov>)

[USA.gov \(https://usa.gov\)](https://usa.gov) | [Whitehouse.gov \(https://whitehouse.gov\)](https://whitehouse.gov) | [FOIA.gov \(https://foia.gov\)](https://foia.gov).



Federal Public Key Infrastructure Technical Working Group

**Wednesday
April 17, 2018**

1:30 p.m. – 3:00 p.m.

GSA 1800 F Street NW, Room 3334

| <u>Time</u> | <u>Topic</u> | <u>Presenter</u> |
|--------------------|---|-------------------------|
| 1:30 | Welcome & Opening Remarks | TWG Chair |
| 1:35 | The Federal PKI Trust Strategy | FPKIMA |
| 1:55 | CAB Forum F2F Synopsis | FPKIMA |
| 2:05 | ICAM Day Synopsis | FPKIMA |
| 2:15 | Subject Key Identifier Attack Vector Overview | FPKIMA |
| 2:30 | Community Question & Answer | TWG |
| 3:00 | Adjourn | TWG Chair |

FPKI TWG April 17, 2018 Meeting Minutes

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call or may not have identified their organization. There were approximately 47 individuals on the call.

| Name | Organization |
|-------------------|------------------------|
| Ambs, Matt | Supporting DHS |
| Barrett, Tony | NASA |
| Bliss, Mike | GPO |
| Brown, Wendy | Supporting FPKIMA |
| Delgado, Mark | DHS |
| Cimmino, Guiseppe | Supporting DHS - USCIS |
| DiDuro, John | Supporting FPKIMA |
| DiSenna, Ridley | NASA |
| Donald, India | GSA – FPKIMA |
| Evans, Frazier | Supporting FPKIMA |
| Garcia, Gladys | DHS |
| Gore, Darlene | GSA - FPKIMA |
| Goss, Brandon | NASA |
| Head, Derrick | DOS |
| Holmes, Matt | Independent |
| Horenstein, Keith | DHS |
| Hobson, Kevin | DoE |
| Jung, Jimmy | Slandala |
| Keady, Thomas | SSA |
| Kennedy, Debbie | GSA – FPKIMA |
| Kluegel, D. Lynn | DoE - LANL |
| Lloyd, Dan | NASA |
| Myers, Kenneth | Supporting FPKIMA |
| Newhouse, Bill | NIST |
| Regenscheid, Andy | NIST |
| Salgado, John | Supporting DoD |
| Schuler, Brian | NASA |
| Stone, Wayne | NASA |
| Williams, Matt | Exostar |
| Wyatt, Terry | NASA |

Welcome and Opening Remarks

Mrs. Darlene Gore, General Services Administration (GSA) and Technical Working Group (TWG) Chair, opened the meeting and thanked everyone for attending. She introduced new FPKIMA team members, Debbie Kennedy and India Donald, and moved to the first agenda item.

Agenda Item 1 - The Federal PKI Trust Strategy

Mr. Kenneth Myers, supporting GSA, opened the agenda item. The FPKIMA developed the FPKI Trust Strategy based on current challenges in FPKI public trust and confusion around how the FPKI should be structured and used. This brief was presented at the FPKI Policy Authority (FPKIPA) and Certificate Policy Working Group (CPWG). The FPKIMA is seeking TWG input to the strategy and clarification of how FPKI is used within the government and with the public. The FPKI faces three current public trust challenges with Google Certificate Transparency (CT), Microsoft technical constraints, and Apple distrust of Symantec CAs. Each challenge was briefed to the ICAMSC and CISO Council. Based on those challenges and potential future ones, the FPKIMA developed a trust strategy focused on specific trust domains, use cases, and PKI architecture.

The FPKIMA identified three trust domains:

- 1) Public – Driven by industry requirements which the government must follow to be included for citizen to government use cases. A typical use case is a citizen accessing a public government website or receiving digitally signed documents from the government. End devices in this domain are controlled by the user or the application trust store.
- 2) Interoperable – Driven by federally-defined requirements for government to government or government to business use cases. A typical use case is cross-agency collaboration or with mission partners for digitally signed documents, email, or internal collaboration websites. End devices in this domain are controlled by either the government or a mission partner and can be modified through enterprise policies.
- 3) Only Locally Trusted (OLT) – Driven by agency-defined requirements for internal use cases. A typical use case is inner-agency collaboration or agency IT management. End devices in this domain are controlled by the agency and can be modified through enterprise policies.

Certificates in the public domain can be trusted through the interoperability and OLT domains, but OLT should not be trusted or used in other domains. The FPKIMA included an interoperable and public trust use cases analysis and a public trust analysis based on findings from <https://analytics.usa.gov/>. They found the most used platform, operating system, and browser to target and prioritize public trust store engagement. Next, applications/browsers were analyzed for specific inclusion requirements and supported PKI uses. The final recommended approach provided the following:

- 1) The public trust domain should have four CAs based on browser use cases for people, devices, code integrity, and time stamping. These CAs may be roots or may be technically constrained under one root.
- 2) The interoperable domain should have one or two roots to differentiate between people and device use cases.
- 3) The OLT domain is agency defined and out of scope. The FPKI may provide guidance and best practices to assist agencies.

Agenda Item 2 - CAB Forum F2F Synopsis

Mr. Myers presented the next agenda item on the recent Certification Authority (CA) / Browser (CAB) Forum quarterly Face to Face (F2F) meeting at the AWS offices in Herndon, VA. There were approximately 60 individuals representing Certificate Authorities, Browsers, and Webtrust Auditors.

There were representatives from around the globe bringing different perspectives to the meeting. The CAB Forum is currently focused on TLS certificates and the methods in validating a TLS applicant. While the group has discussed future working groups for client and S/MIME, they are not ready to move forward on those initiatives.

Google is moving forward on enforcing Certificate Transparency (CT) enforcement on April 30th, 2018. Google's Chrome browser will start displaying errors for sites if the associated TLS certificate has a path to a publicly trusted root and does not meet Google CT log requirements. Google informed the community that they were going to include any PKI roots distributed by applications in all Chrome versions supporting certificate transparency. There was a presentation on a New WebTrust for Registration Authorities audit standard.

Agenda Item 3 - ICAM Day Synopsis

Mr. Frazier Evans, supporting GSA, opened the next agenda item on the 2018 ICAM Day. The morning keynotes focused on mobile credential use is moving forward. The challenge are the platforms and how the certificates will be used.

Cybersecurity Acquisition Breakout - There was a discussion concerning procuring ICAM professional services on the GSA Schedule 70. ICAM Day attendees agreed procuring products was possible, the challenge was obtaining the integration and professional services. Several attendees discussed labor rates and categories in Schedule 70 SIN 51 did not correlate to ICAM professional services. There was an extended discussion on the potential need for a new SIN or additional labor categories for professional services and maybe distinct professional services such as ICAM architect, ICAM implementation, etc.

PACS Breakout - There was a lively discussion about Enterprise PACS and visitor management. The attendees were interested in agency success stories and lessons learned. The most common unanswered question focused around if there is a single cross-platform solution to manage multiple vendor PACS components from a common interface.

Login.gov Breakout - The Login.gov shared identity service allows citizens to create a federally issued, non-PKI identity which can be used across multiple government services. The service provides multifactor authentication via the use of One Time Passwords (OTP). The OTP can be generated on the registered device, sent to the device either via SMS, or the system will call to the user with the code. A citizen only need an email and a phone number to create an account. The onboarding process for an agency application is less than 90 days. The Login.gov credential is non-PKI level of assurance 3 and only supports one email address. Login.gov is privacy first and strives to maintain only the minimum amount of information needed. The most recent government adopter is USAjobs.gov.

Agenda Item 4 - Subject Key Identifier (SKI) Attack Vector Overview

The Register posted an article (https://www.theregister.co.uk/2018/02/06/x509_certificate_attack/) on a potential attack vector using a PKI certificate extension to either deliver malicious payload or extract enterprise data. Website links in the article provided additional details. The key points were:

- 1) Malicious payload or commands could be sent without an actual session being established because many Relying Parties do not look at the actual extensions detection is difficult
- 2) This attack vector requires the processing of commands that are embedded in the extension to setup the cover channel.
- 3) The demo attack requires that the target machine be compromised so that the covert channel can be built

Matt Ambs, supporting the Department of Homeland Security (DHS), asked when the client certificate is used. The malware that is installed on the target machine could create new self-signed certificates that included data to exfiltrate from the targeted environment. Also discussed was the possibility of a compromised "Trusted" CA which could be used to deliver malicious code to infected machine, by leveraging "unvalidated" extensions. It was explained this could be possible if the CA did not validate the contents of the SKI or another x.509 extension. The only way for the Relying Party to detect this would be to look at the actual size of the certificates being presented. This type of attack has limited potential in Federal PKI because of the certificate profile conformance testing but is still a potential attack vector for either non-FPKI or a compromised FPKI certificate. Gladys Garcia, DHS, appreciated the presentation explaining she is always looking for PKI threat vector scenarios.

Agenda Item 5 – Community Question and Answer

The floor was opened to open discussion items. An update was requested from agencies who were in the middle Microsoft Certificate Trust List (CTL) testing. The participating agencies include DHS, DoD, SSA, NASA, Treasury, NRC and NIH. Terry Wyatt, NASA, provided the following observations:

- They are testing with multiple versions of Edge, IE, and Chrome
- With Server Authentication for Common Policy set to disallow server authentication (serverAuth), it breaks every NASA website validation even if Federal Common Policy CA (FCPCA) had been published to the enterprise root store. The Microsoft CTL effectively overrides enterprise trust decisions
- If another root path exists and serverAuth is enabled, the browser is able to properly validate the website certificate (example; manually publishing the Treasury Root to the enterprise trust store). This seems to work for both IE and Chrome.
- Certificate / Path validation is dependent on the tool being used. Certutil versus the browser have provided different results based on testing. Browsers seem to find a valid path if it exists even if there are multiple bad paths. Certutil does not.
- While testing, remember to clear both the browser cache and SSL state. Previous validations continuing to be used and Chrome appears to cache the serverAuth state.

NASA also stated it was unlikely that they would move sites to the new federal Public TLS root after having successfully moved to a commercial provider. NASA also provided many questions for Microsoft during the next CTL Meeting.

- 1) Can we do parallel CTL testing of disallowed, notBefore, and totally removing the FCPCA from the CTL.
- 2) Windows Server versions are excluded, but what happens if an IIS server gets the new CTL?
- 3) What controls the authentication/validation path in Server to Server authentication situations? The behavior of the CTL seems to be on CAPI validation so why are we just testing website and not any certificate that may include the serverAuth extension?
- 4) Could the government work with Microsoft to change the behavior to allow the Enterprise Trust store to override the CTL or to have a registry setting that would allow the enterprise to configure the behavior of the CTL within the enterprise? (Example: Enterprise Trust store overrides the CTL)
- 5) Can we turn off CTL checking as an enterprise? If we do, how do we maintain CTL updates or define our own CTL?

Adjourn

Mr. Myers thanked the presenters and everyone who participated for the lively discussion and closed the meeting.



Federal Public Key Infrastructure Technical Working Group

**Wednesday
January 24, 2018**

1:30 p.m. – 3:00 p.m.

GSA 1800 F Street NW, Room 3002

| <u>Time</u> | <u>Topic</u> | <u>Presenter</u> |
|--------------------|-------------------------------|-------------------------|
| 1:30 | Welcome & Opening Remarks | TWG Chair |
| 1:35 | Microsoft Root Program Impact | FPKIMA |
| 2:15 | Feedback Session: | |
| | 1) CITE | FPKIMA |
| | 2) Monthly Statistical Report | |
| 3:00 | Adjourn | TWG Chair |

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

| Name | Organization |
|------------------|----------------|
| Baldrige, Tim | DoD |
| Barrett, Tony | NASA |
| Brown, Wendy | Supporting GSA |
| Chokani, Santosh | Supporting DoD |
| Clements, Chris | Supporting DHS |
| Cooper, Matt | Supporting GSA |
| DiDuro, John | Supporting GSA |
| Evans, Frazier | Supporting GSA |
| Fontana, Bob | Supporting GSA |
| Goss, Brandon | NASA |
| Head, Derrick | DOS |
| Jarboe, Jeff | Supporting GSA |
| Keating, Tom | Supporting SSA |
| Lloyd, Dan | NASA |
| Myers, Kenneth | Supporting GSA |
| Salgado, John | Supporting DoD |
| Schuler, Brian | NASA |
| Smith, Toma | GSA |
| Stone, Wayne | NASA |
| Voiner, Jeff | GSA |
| Williams, Matt | Exostar |
| Weiser, Russ | Verizon |
| Wyatt, Terry | NASA |

Welcome and Opening remarks (Kenneth Myers)

Mr. Kenneth Myers, supporting the General Services Administration (GSA) and Technical Working Group (TWG) Secretariat, opened the meeting and thanked everyone for attending.

Agenda Item 1 – Microsoft Root Program Impact (FPKIMA)

The Federal Common Policy Certification Authority (FCPCA) or Common is distributed in the default Microsoft Windows Operating System as part of its Trusted Root Program. Microsoft updates its program requirements annually to remain compliant with the CA/Browser (CAB) Forum and other industry standards / groups. One recent change is Microsoft intends to constrain government root CAs, such as Common, to the top-level domain of the country (*.gov and *.mil). The impact is limited to FPKI server authentication certificates on windows-based browsers (except Mozilla Firefox), but have a broader impact in cross-government websites. The FPKI Policy Authority (FPKIPA) was briefed and developed two options:

- 1) Turn off Server Authentication Trust for Common (recommended approach)
 - a. For internet websites, users will receive a warning when browsing to a website secured with an FPKI server certificate.
 - b. For intranet websites, the enterprise administrator can propagate a group policy object (GPO) to re-establish trust.
 - c. Lowest risk because the capability can be re-enabled by administrators or users.
 - d. Potential to increase agency cost from procuring commercial server certificates.
- 2) Government domain constraint
 - a. For internet and intranet websites, only a fully qualified domain name or IP address in the certificate will validate properly. Any other entry in the subject alternative name (e.g. Local name, unresolvable address, etc.) will present a browser error. Require agencies to potentially reissue or redesign intranets to comply.
 - b. Microsoft will implement the constraint through a Microsoft Certificate Trust List (CTL) which can only be altered through creating and maintaining a customer CTL by enterprise administrators.
 - c. In addition, all FPKI CAs must comply with the following requirements:
 - i. Separate issuing CAs based on Server, Code Signing, SMIME, and Time Stamp.
 - ii. Enable online certificate status protocol for server certificates
 - iii. Publicly posting practice statements and security incident post-mortem reports.
 - iv. All CAs issuing server certificates must undergo a WebTrust for SSL audit in addition to the FPKI audit.

The group discussed the pros and cons and agreed with the recommended approach. The new public server infrastructure will add a public server capability to the FPKI. The FPKIPA also presented this topic to the ICAMSC with a final decision to be made by the Federal CISO Council at their Jan 24th meeting.

Follow-on Activities

- 1) Following feedback from the Federal CISO Council, the FPKI will notify Microsoft to remove the server authentication trust bit from Common.

Agenda Item 2a – Feedback: CITE (FPKIMA)

The Community Interoperable Test Environment or CITE is the FPKI interoperability testing environment. It also has additional testing capabilities to support path validation and discovery, certificate profiles updates, technology platform changes, and functional testing. CITE is a mimic of the production FPKI environment with a Test Federal Bridge and Test Common as well as a directory, http repository, and an OCSP responder to support the GSA APL. The Approved Products List (APL) FIPS 201 also uses the CITE HTTP repository to host test artifacts. CITE has experienced a decrease in use after a moratorium was placed on new applications and the proposed plan to move future interoperability testing to the bridge partners. The FPKIMA asked the TWG for feedback on what kind of testing might be missing in CITE as well as what can the FPKIMA implement to improve CITE value. Currently, Treasury and DoD are the only active users requesting new test certificates. Feedback included:

- 1) Bob Fontana, supporting GSA, was concerned where the APL artifacts would be hosted if CITE was decommissioned. He then added he was working on a self-contained VM and script for FPKI partners to either install or execute to create the APL test environment.
- 2) A request was made if CITE is decommissioned to maintain the FPKI Test OIDs.
- 3) One suggestion was made to make available test end-entity certificates with private key information to test application signature and authentication.
- 4) Tim Baldridge, DoD, added even though CITE is not fully leveraged today, the FPKI needs an interoperability environment in the future whether that is the FPKIMA hosted CITE or something else.
- 5) The FPKIMA requested people send an email expressing their opinion on whether CITE is necessary and if so, what could be done to make it more valuable to the community.

Potential Follow-on Activities

- 1) The FPKIMA may present the feedback at the next FPKIPA meeting to determine the future need for CITE.

Agenda Item 2b – Monthly Statistical Report (FPKIMA)

The FPKIMA distributes a monthly statistical report with four pieces of information for the Trust Infrastructure, federal agency PKI, and affiliates.

FPKI TWG January 24, 2018 Meeting Minutes

- 1) Compliance Status
- 2) Technical Issues
- 3) FPKI Trust Infrastructure Certificate Activity
- 4) Six-month availability status of directories and repositories

The FPKIMA requested feedback from the group on how to improve its value. Feedback included:

- 1) Knowing when certificate actions will take place in advance is very useful.
- 2) Real-time availability information is more useful than a monthly static report. It can be used to test whether network issues are internal or external.
- 3) All certificate activity, not just limited to the FPKIMA, is helpful.
- 4) A list of AIA, SIA, CDP, OCSP, and DN is helpful. The only way to currently get it is when an agency encounters that certificate.

Potential Follow-on Activities

- 1) The FPKIMA will develop a project to automate the monthly statistical report.

Adjourn

Mr. Myers thanked the presenters and everyone who participated for the lively discussion and closed the meeting.



Federal Public Key Infrastructure Technical Working Group

**Wednesday
July 19, 2017**

1:30 p.m. – 3:00 p.m.

Teleconference

Time Topic

1:30 Welcome & Opening Remarks
1:35 FPKI TLS/SSL Browser Testing
2:05 USDA PIV Validation Challenges
2:35 ACME Protocol Overview
2:50 Domain Constraint Testing Follow-up
3:00 Adjourn

Presenter

Kenneth Myers
Eric Mill
John Shuey
FPKIMA
FPKIMA
Kenneth Myers

Teleconference

<https://meet.gsa.gov/fpkitwg/> - Passcode: fpkitwg

Number: 1-866-928-2008 – Code: 778967#

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

| Name | Organization |
|------------------|---------------------|
| Name | Organization |
| Ambbs, Matt | Supporting DHS |
| John Shuey | USDA |
| David Dixon | USDA |
| Eric Mills | GSA |
| Giuseppe Cimmino | Supporting DHS |
| Ken Myers | Supporting GSA |
| Wendy Brown | Supporting GSA |
| Maria Holland | Supporting GSA |
| Cooper, Matt | CertiPath |
| Chris Clements | Supporting DHS |
| Paul Evans | DoE |
| Lynn Klugel | DOE |
| Head, Derrick | State |
| Wyatt, Terry | NASA |
| Jung, Jimmy | Slandala |
| Todd Johnson | Treasury Department |
| Mark Delgado | Supporting DHS |
| Alan Bonsia | Supporting DHS |
| LaChelle Levan | GSA |
| Dan Lloyd | NASA |
| John Salgado | Supporting DoD |
| Karim Said | NASA |
| Toby Slusher | HHS |
| Toma Smith | GSA |
| Carl Wallace | Redhound |
| Jeff Jarboe | Supporting GSA |
| Mel Holden | Verizon |
| Tony Barrett | USDA |
| Glenn Lee | DoE |
| Dave Sulser | NRC |

Welcome and Opening Remarks (Kenneth Myers)

Ms. Darlene Gore, GSA / TWG Chair, was unable to attend the meeting and allowed Mr. Kenneth Myers, supporting GSA, to chair this session. Mr. Myers opened the meeting and thanked everyone for attending. He then turned it over to Mr. Eric Mill for the first topic.

Agenda Item 1 – FPKI TLS/SSL Browser Testing

Mr. Eric Mill opened with an overview of industry's take on the Federal PKI and the Web PKI community. Mr. Eric pointed out Mozilla does a public review process for Root CA inclusion and other browsers tend to piggyback on the Mozilla process. Mozilla requires disclosure of any issuing CA that is capable of issuing certificates that may be used in TLS sessions by Firefox browsers.

A while back, Eric and Todd Johnson performed some scans of the Web PKI looking for TLS certificates issued under the FPKI and investigated which had paths to publicly trusted roots in the Mozilla/NSS trust store. They discovered 2 roots, one managed by Identrust and the other by a Symantec CA; both had issued cross-certificates to the FBCA. Eric brought these to the attention of the vendors and Mozilla because Mozilla requires organizations operating root CAs in their trust store to publicly identify all subordinate CAs in a public database and the Federal Common Policy CA (FCPCA) has not been accepted into the Mozilla/NSS trust store. As a result, Identrust revoked their cross-certificate to the FBCA and Symantec allowed theirs to expire without renewal.

The perception is certificates issued by the federal government are mainly identity certificates for humans. However, the FPKI also issues device certificates for agency web sites.

Some of the agencies believe that EV certs are required. However, Eric talked about slides from the FPKIMA State of the Union session that were presented by Mr. Ryan Sleevi from Google. Ryan feels there is only one type of certificate that exists in the Web PKI and that is DV certificates and technical constraints are what matter. Eric is in agreement with this sentiment and, in relation to the new NPE effort, there is an effort to convince agencies that may have a preference for EV certificates that there is no actual benefit to the added cost for EV. There is no government-wide policy that would require EV over DV certificates for public-facing web sites.

After Eric's presentation, LaChelle highlighted that browsers ignore the policies. Todd clarified that Mozilla is capable of distinguishing policy OIDS but they chose not to process policy mappings in the certificate path.

Agenda Item 2 – USDA PIV Validation Challenges

Mr. John Shuey and Mr. David Dixon provided an overview of USDA eAuthentication, which is the department's solution for web-based access control. It uses CA SiteMinder and Identity Manager to provide a front-end authentication mechanism for about 450 web applications. These applications are both internal- and external-facing; some of the external ones may be accessed by citizens that have business with USDA. The system has been integrated with some GSA programs that will be used by agencies government-wide. Multi-factor authentication is supported, either through direct PIV authentication or via federated SAML assertions on the back end, to the various applications. It manages user accounts with just-in-time account provisioning.

They provided some highlights of issues they had encountered with enabling the system to accept PIV credentials from different agencies across the government. USDA had to add the self-signed root certificates for Treasury, State, and DoD in order for users configured with these Trust Anchors to be prompted for their credentials. Additionally, agencies with SSL intercept mechanisms had to open their firewalls to allow connection to the USDA eAuthentication application.

Additional issues they encountered included DOD CACs that do not contain a PIV Authentication certificate and users who do not know how to distinguish their authentication certificate from their digital signature when both certificates are presented as possible credentials.

Todd Johnson brought up that Treasury also used SiteMinder, but in a different configuration which allowed redirection to an Apache server that is configured for optional client certificates. This configuration does not require a hint list to be sent to the client, so the client is able to select a certificate without the application needing the additional CA certificates in its own trust store.

USDA is not yet supporting PIV-I or other cross-certified credentials in addition to PIV. This may be planned as a future enhancement.

The discussion of lessons learned is useful for agencies not yet accepting external credentials. Other agencies are invited to share what they have learned when implementing applications that accept both government-wide and external FPKI credentials at future TWG meetings.

Agenda Item 3 – ACME Protocol Overview

Ms. Maria Holland opened the session with an overview of ACME. ACME is a protocol that a certification authority (CA) and an applicant can use to automate the process of verification and certificate issuance. The main objective is a cost-effective and automated means to verify domain ownership. ACME allows a client to request certificate management actions using a set of JavaScript Object Notation (JSON) messages carried over HTTPS. ACME functions much like a traditional CA, in which a user creates an account, requests a certificate, and proves control of the domains named in that certificate, in order for the CA to sign the requested certificate.

Mr. Karim Said from NASA provided additional input on NASA's use of the ACME program. NASA is using Lets Encrypt to obtain commercial TLS certificates. NASA had more organizational problems and less technical problems with moving to ACME. One of their issues was trying to get everyone on the same page. To do this, they organized weekly meetings and wrote a white paper. NASA uses Certbot for their client because Certbot supports Linux. They created a GitHub page to collaborate on information sharing for configurations and client information. Let's Encrypt is now the 2nd biggest issuer of certs at NASA behind DigiCert.

After the meeting, Ken Myers forwarded NASA's ACME whitepaper to the TWG list. The ACME presentation by Karim is posted on the OMB Max website.

Agenda Item 4 – Domain Constraint Testing Follow-up

Mr. Ken Myers gave an update on Microsoft Domain Constraint. He has been following up with the agencies and SSPs to find out the impact Microsoft's domain constraints will have on them. Microsoft's trust store program is moving to constrain all government CAs to the Top Level Domain by country. This includes Japan, India and Korea's government CAs. For the FPKI, each DNSName in the subjectAltName extension of a certificate issued under the FCPCA has to end with .gov, .mil or .us once this constraint is implemented. Microsoft is trying to protect the users of browsers on the "Web PKI." If malicious certificates are found, they want a way to cut off that root.

The constraint will only impact server authentication certificates for clients using Windows 10 and browsers with the Microsoft Trust store such as Edge, Internet Explorer and possibly Chrome.

Microsoft met with the FPKI and federal representatives to understand the impacts this change might have on some of the agencies like DHS. Microsoft agreed to put this FCPCA Domain Constraint change on hold until Microsoft can come up with an "opt in, opt out" solution or other alternative.

Participants asked about the alternative suggestion that the FPKIMA had made when they sent notice of the proposed change to the community. The alternative was to request that Microsoft remove the property to trust the FCPCA for use as a root for server authentication rather than implement the domain constraint. This change would mean external users with Microsoft browsers would see an error when encountering any TLS certificate issued under the FPKI. However, it would allow agencies to set the server authentication trust bit on the FCPCA for internal use, similar to the way they manage trust for smartcard authentication through group policies.

If the FPKI had to choose between the proposed technical constraints of domain names that could not be overridden or removing the server authentication trust bit which could be changed at the enterprise level, participants' recommendation is to remove the trust bit.

Adjourn

Mr. Myers thanked everyone for attending and adjourned the meeting.



Federal Public Key Infrastructure Technical Working Group

**Wednesday
April 06, 2017**

1:00 p.m. – 3:00 p.m.

Teleconference

Time Topic

1:00 Welcome & Opening Remarks
1:05 USDA Derived PIV Overview
2:35 Certificate Transparency
3:00 Adjourn

Presenter

Kenneth Myers
USDA
FPKIMA
TWG Chair

Teleconference

<https://meet.gsa.gov/fpkitwg/> - Passcode: fpkitwg

Number: 1-866-928-2008 – Code: 778967#

FPKI TWG April 6, 2017 Meeting Minutes

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

| Name | Organization |
|-----------------|-----------------------|
| Ambs, Matt | Supporting DHS |
| Baldrige, Tim | DoD |
| Brown, Ben | WidePoint |
| Brown, Wendy | Supporting GSA |
| Cooper, Matt | CertiPath |
| Delgado, Marc | Contractor |
| Evans, Paul | NASA |
| Guzman, Jake | Contractor |
| Hall Jason | Treasury Department |
| Head, Derrick | DOS |
| Holland, Maria | Supporting GSA |
| Jarboe, Jeff | Supporting GSA |
| Johnson, Todd | Treasury Department |
| Jones, Adam | WidePoint |
| Jung, Jimmy | Slandala |
| Kalantir, Ray | Contractor |
| Klugel, Lynn | DOE - Los Alamos Labs |
| Levan, LaChelle | GSA |
| Lloyd, Dan | NASA |
| Mike Boorum | WidePoint |
| Myer, Brandon | USDA |
| Reese, Simone | USDA |
| Santosh Chokani | Libre Security |
| Shomo, Larry | Supporting DOS |
| Slusher, Toby | HHS |
| Vanhell, Dan | Contractor |
| Wallace, Carl | Redhound |
| Williams, Matt | Exostar |
| Wyatt, Terry | NASA |

Welcome and Opening remarks (Darlene Gore)

Ms. Darlene Gore, GSA / TWG Chair, was unable to attend the meeting and allowed Mr. Kenneth Myers, supporting GSA, to chair this session. Mr. Myers opened the meeting and thanked everyone for attending. He then turned it over to Ms. Simone Reese, USDA, for the first topic.

Agenda Item 1 – USDA Derived PIV Overview (USDA)

Ms. Reese opened her agenda item with an overview of the USDA Derived PIV offering which is called Mobilelinc. It is designed for both derived PIV and derived credentials following NIST 800-157. It will allow for different mobile platforms including both Android and iOS. The intent of the topic is to gather feedback on the USDA Derived PIV approach and collect any suggestions or best practices to integrate before the system is launched. The system plans to support 26k – 30k USDA mobile devices issued only to USDA employees and contractors. The system uses a Mobile Device Management (MDM) application to authorize and coordinate issuance of a Derived PIV from an Entrust MSO CA. It is unclear if it will eventually be the same CA as PIV issuance, but currently it is a test CA. The private key associated with the Derived PIV will be protected on the mobile device in a manner that requires a proprietary Software Development Kit (SDK) for access. The only use case addressed will be authentication, but email signing is on the roadmap. A USDA employee with a valid PIV card may request a Derived PIV through a web portal. The private key is generated on a device with a FIPS approved module. Mobilelinc has both an ATO and the NIST 800-79-2 Derived PIV Issuer ATO. A maximum of three Derived PIV may be requested. The serial number is tied with an identifier on the device and uses the same UPN that matches the PIV card for the access management system to allow access to various USDA applications. Due to the need for the proprietary SDK for access, the USDA Derived PIV will not be able to validate to other agencies' applications. A use case for other agencies accessing USDA applications is on the development roadmap. When the device is returned to USDA, all certificates are revoked even if the private key has not been compromised.

Comments for USDA

- 1) Look into using an open source protocol such as Simple Certificate Enrollment Protocol (SCEP). Purebred (Github.com/purebred) is another example. Any proprietary method runs the risk of potential security risks.
- 2) It may be very difficult to migrate away from the MDM SDK to meet cross-agency authentication to USDA applications for Derived PIV issued outside of USDA. Consider an open source protocol and native key storage methods.
- 3) Consider the impact of revoking certificates. The current size of the Entrust CRL is around 17mb which causes network availability issues for some systems with constrained network connections. If the private key is still protected, consider allowing the certificate to expire after the private key is successfully destroyed. USDA countered they use the Certificate Revocation List (CRL) entry as a method to account for returned credentials.

Potential Follow-on Activities

- 1) Future TWG to discuss Subject DN
- 2) Future TWG on the use of User Principal Name (UPN) or other extension for access management (Tim Baldrige, DoD)
- 3) Future TWG on Derived Credential key storage to allow different agency applications to access the Derived PIV certificate
- 4) Policy or guidelines of when to let an end entity certificate expire versus revocation when the private key is still protected.

Agenda Item 2 – Certificate Transparency (FPKIMA)

Ms. Wendy Brown opened the session with an overview of Certificate Transparency. It is a Google project, specific to the Google Chrome browser, to fix structural flaws in the SSL certificate ecosystem (<https://www.certificate-transparency.org/>). The primary flaws in the SSL ecosystem pertain to a wide range of security attacks against HTTPS connections such as website spoofing, server impersonation, and man-in-the-middle attacks. The intent of Certificate Transparency is to provide a framework to make SSL certificate issuance open and public for review. It aids in detecting false, misleading, or mis-issued certificates by a Certification Authority that is not following industry standards or has gone rogue. The most prominent driver for Certificate Transparency was the DigiNotar compromise. DigiNotar and its subsidiaries were compromised and issued hundreds of fraudulent SSL certificates to well-known websites allowing hackers to stage malicious Man-in-the-Middle attacks.

Certificate Transparency is a blockchain type technology that uses a merkle tree to record SSL certificates for later review. It is comprised of certificate logs, monitors and auditor components. The Certificate Log is the actual merkle tree which logs certificate requests. Logs are cryptographically assured, publicly audited, and append-only records of certificates issued by publicly trusted CAs. Anyone can submit a certificate as well as query a log to verify the log is behaving properly and certificates have been logged properly. A list of available certificate logs can be found at <https://www.certificate-transparency.org/known-logs>.

Monitors are publicly run servers that periodically verify the new log entries in the certificate logs. They are usually operated by companies and organizations to monitor their domains and watch for unusual certificates. One free monitor is run by Comodo and can be found at <https://crt.sh>. Auditors verify the log proofs to ensure the integrity of the certificate log. It can be used to log certificates that are encountered but not found in a log.

The basic process of certificate activity is as follows:

- 1) Before issuing a certificate, the CA will request a signed certificate timestamp (SCT) from either one or multiple certificate logs. The SCT is a timestamp of when the request to log the certificate was made. It is essentially a promise that the certificate will be logged.
- 2) The CA issues the certificate and may imbed the SCT(s) in the certificate.

- 3) During the TLS handshake, Google Chrome will verify that it receives at least two SCTs either in the certificate, with the TLS handshake or through certificate pinning. Chrome will validate that at least 2 SCT are from logs that are either currently trusted or were trusted at the time of certificate issuance.

Google Chrome has published a policy that by April 2018, it will only validate SSL certificates that are logged. If it is not logged, the user will receive a security warning page potentially with no option to click through the warning. Other browsers (Microsoft, Mozilla, and Apple) have shown an interest, but not have published a formal policy requiring CT. LaChelle Levan, GSA, mentioned <https://analytics.usa.gov> provides a snapshot of current HTTP traffic to government domains. Chrome is the most widely used browser ahead of Safari and Internet Explorer. She pointed out this was HTTP traffic not originating from government domains. Even if this requirement only applies to Chrome, in order to allow consistent user experience to federal websites, the government websites must follow the Chrome policy.

Adjourn

Mr. Myers thanked everyone for attending and adjourned the meeting.



Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By SRA International

**Wednesday
July 8, 2015**

1:00 p.m. – 3:00 p.m.

Teleconference

Time Topic

| | |
|------|---|
| 1:00 | Welcome & Opening Remarks |
| 1:05 | Microsoft Certificate Reputation Program |
| 2:00 | DHS SSL Wildcard Certificates in Support of Microsoft SharePoint 2013 |
| 2:45 | TWG Updates |
| 3:00 | Adjourn |

Presenter

| |
|--------------------------|
| Ola Bello |
| Anoosh Saboori |
| Mike Ambs Larry Shomo |
| Kenneth Myers |
| Ola Bello |

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

| Name | Organization |
|-------------------|---------------------|
| Ambs, Matt | DHS |
| Anand, Neha | Symantec |
| Baldrige, Tim | DoD |
| Bello, Ola | GSA FPKIMA |
| Blanchard, Debb | ORC |
| Brown, Wendy | GSA FPKIMA |
| Cimmino, Giuseppe | GSA FPKIMA |
| Chokani, Santosh | CygnaCom |
| Cotton, Michael | Microsoft |
| Johnson, Todd | Treasury |
| Jung, Jimmy | State |
| McBride, Terry | Treasury |
| McLain, Drew | Treasury |
| Mill, Eric | GSA |
| Myers, Kenneth | GSA FPKIMA |
| Robinson, Buddy | Treasury |
| Saboori, Anoosh | Microsoft |
| Salgado, John | DoD |
| Shomo, Larry | DHS |
| Spence, Willie | IRS |
| Weaver, Kurt | Treasury |
| Wyatt, Terry | NASA |

Welcome and Opening remarks (Ola Bello)

The FPKI TWG met to receive two information presentations which could impact the Federal PKI (FPKI). Mr. Kenneth Myers opened the meeting and thanked everyone for attending and added Mr. Ola Bello, TWG Chair, was delayed by another meeting, but would join shortly. He then turned it over to Mr. Anoosh Saboori, Microsoft, to discuss the first agenda item.

Agenda Item 1 – Microsoft Certificate Reputation Program (Anoosh Saboori)

Mr. Saboori introduced the agenda topic with a general overview of the PKI threat landscape and then a description of the Microsoft Certificate Reputation or Cert Rep program. The current PKI threat landscape includes fraudulent certificate use on fake and real web sites, unreliable certificate revocation list (CRL) checking, and applications ignoring CRL issues. The intent of the Cert Rep program is to monitor public PKI certificates for anomalies and other possible issues to protect end users and certificate authorities (CAs). The program currently encompasses three components:

- 1) Microsoft Trust Store Program for trusted root CA certificates.
- 2) A blacklist for identifying untrusted intermediate certificates. This blacklist is automatically pushed to Windows computers which are configured to request it every 16 hours. This feature is turned on by default. One of the TWG members asked about Window client and servers which have automatic updates turned off for security reasons. Mr. Saboori replied the only way to receive the blacklist updates is to have the auto update feature enabled. The automatic update is controlled via a registry setting, Mr. Saboori will provide additional information about this configuration to the TWG at a later date.
- 3) The smart screen feature included in Windows Internet Explorer to capture SSL certificates for analysis and notification.

Mr. Saboori then explained the smart screen feature from multiple member questions. The smart screen feature is a data collection point in Internet Explorer which captures SSL certificates that validate to a third party root. Back end Microsoft servers analyze the certificate for anomalies and verifies it has not been issued from a compromised CA. Microsoft analyzes the certificates looking for patterns that may indicate issues and learn to distinguish between false positives or actual issues. Microsoft is concerned with the tradeoffs between the need to perform this analysis and the requirement to preserve the privacy of users. Website owners are notified through the BING Webmaster Tool and Microsoft is working on other forms of notification for CA operators to include possible information sharing agreements as well. Browser clients do not receive any feedback at this time. Mr. Todd Johnson asked if the smart screen feature also captures internal certificates and who is told if an anomaly is found. Mr. Johnson was concerned smart screen was exfiltrating private certificates that were not meant to be publicly analyzed. Treasury issues internal certificates under the Treasury root which has a path to Common Policy which is in the Microsoft Trust Store. Mr. Johnson also

asked if Microsoft has analyzed the certificates for weak keys and if that analysis could be shared? Mr. Saboori did not have this information and would follow-up with the TWG when he finds it and if he can share the information. Mr. Myers thanked Mr. Saboori for presenting the topic.

Agenda Item 2 – DHS SSL Wildcard Certificates in Support of Microsoft SharePoint 2013 (Matthew Ambs)

Mr. Larry Shomo, DHS, opened the topic with a background of the situation. DHS has invested in Microsoft SharePoint and with the latest upgrade to SharePoint 2013 one of the system requirements is to issue SSL wildcard certificates. This alleviates the need to issue hundreds of individual certificates to each SharePoint website. DHS also has an internal policy that all certificates are issued from a DHS CA under Common Policy. Mr. Matthew Ambs, DHS, continued the topic to add the current Common Certificate Policy (CP) is very vague around SSL and device certificates, but does not specifically state a wildcard certificate is not allowed. Microsoft recommends the wildcard “*” is more than one level down from the department root for sufficient risk mitigation (i.e. *.sharepoint.dhs.gov). DHS was looking to the TWG on a consensus to the best technical mitigation to use SSL wildcards which are policy compliant.

DHS is proposing the FPKIPA update section 3.11 and 3.1.5 of the Common Policy CP to specifically address SSL wildcards and recommends the wildcard be placed at least three levels down from the top level domain (i.e. *.sharepoint.dhs.gov) for proper risk mitigation. DHS shared their current proposal which includes the use of 6 levels and registering a DNS A Record for the FQDN following the wildcard. A discussion around the use of the subjectAltName (SAN) versus the subject DN followed, as well as the tradeoffs between issuing a certificate to each server vs a single certificate issued to an entire server farm with a single DNS A record.

Mr. Tim Baldrige, DoD, added since the current policy does not state wildcards are not allowed, DHS can issue SSL wildcard certificates that they think meet the uniqueness criteria as set forth in the Common Policy CP. Mr. Baldrige asked the group if anyone objected to the TWG sending a formal request to the FPKIPA to have the Common Policy CP updated to address wildcard certificates. No one objected to the motion. Mr. Bello took the group consensus as an action and thanked DHS for presenting.

ACTION: The TWG will send a formal request to the FPKIPA to update the Federal Common Policy CP to address SSL wildcards.

Agenda Item 3 – TWG Updates

- 1) **GSA CyberSprint** – In support of the OMB directed CyberSprint, the FPKIMA is assisting GSA in identifying gaps in FPKI services. A survey was distributed to the FPKIPA and ICAMSC listservs for any suggestions of what services are needed or not offered in the FPKI. If you have any suggestions, please send your responses to fpki-help@gsa.gov or the TWG listserv. Mr. Baldrige added he is co-chair of the OMB Multi-Factor Authentication (MFA) Tiger Team and the White House is taking this initiative very seriously. Any input on how to enable PIV for (MFA) to share is greatly appreciated.
- 2) **OMB HTTPS Memo** – OMB released a new memo requiring all public facing websites to use SSL certificates by end of calendar year 2016. Mr. Johnson added the FPKIPA should coordinate with OMB to address those public websites which cannot have SSL certificates due to availability concerns such as HTTP repository pages. No action was taken at this time.

Adjourn

Mr. Bello thanked the presenters and everyone who participated for the lively discussion and closed the meeting.



Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By SRA International

**Friday
March 25, 2015**

1:00 p.m. – 2:30 p.m.

Teleconference

Time Topic

| | |
|------|--|
| 1:05 | Welcome & Opening Remarks |
| 1:05 | Microsoft Trust Store Program / Certificate Reputation Program |
| 1:35 | High Speed PACS & Active Directory Smart Card Mapping |
| 2:20 | Apple Over the Air Vulnerability |
| 2:30 | Adjourn |

Presenter

| |
|---------------|
| Ola Bello |
| Jody Cloutier |
| Tim Baldridge |
| Carl Wallace |
| Ola Bello |

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

| Name | Organization |
|-------------------|--------------|
| Ambs, Matt | DHS |
| Anand, Neha | Symantec |
| Baldrige, Tim | DoD |
| Bello, Ola | FPKIMA |
| Blanchard, Debb | Verizon |
| Brown, Wendy | FPKIMA |
| Cimmino, Giuseppe | FPKIMA |
| Cloutier, Jody | Microsoft |
| Curtis, Dave | Treasury |
| DiSenia, Ridley | NASA |
| Edmunds, Debbie | State |
| Goss, Branden | NASA |
| Head, Derrick | DOS |
| Johnson, Todd | Treasury |
| Kane, Joe | USPS |
| McBride, Terry | Treasury |
| Monaghan, Jess | USPS |
| Myers, Kenneth | FPKIMA |
| Silver, Dave | GSA |
| Shomo, Larry | DHS |
| Wallace, Carl | DoD |
| Weiser, Russ | Verizon |
| Wood, Dan | Treasury |

Welcome and Opening remarks (Ola Bello)

The FPKI TWG met via teleconference to receive three information presentations which could impact the Federal PKI (FPKI). Mr. Kenneth Myers informed the audience there was a last minute agenda change and the presentation by Mr. Tim Baldrige would be conducted first due to a scheduling conflict. Mr. Ola Bello opened the meeting and thanked everyone for calling in and gave a brief update of the TWG. Mr. Bello then turned it over to Mr. Tim Baldrige to discuss the next agenda item.

Agenda Item 1 – High Speed PACS Pilot and Active Directory Mapping (Tim Baldrige)

Mr. Baldrige representing the Department of Defense (DoD) presented two presentations on High Speed Physical Access Control Systems (PACS) Lessons Learned and Subject Name Mapping in Windows Smart Card Logon.

High Speed PACS Lessons Learned

The DoD is currently piloting Common Access Card (CAC) high speed contactless interfaces at different turnstile access points for “touch & go” CAC access. They are testing the use of Secure Messaging (SM) which is a simplified profile of a secure open protocol specified in the National Institute of Science and Technology (NIST) Special Publication (SP) 800-73-4 and the InterNational Committee for Information Technology Standards (INCITS) 504. Both are awaiting final approval. Each standard fully specify the contactless interface for full certificate usage and can manage all transactions other than card management over the contactless interface.

The benefit of using this standard is significant increase in validation speed ranging from 100 – 300 milliseconds compared to the 2 – 5 seconds currently experienced in enterprise PACS (EPACS). The speed advantage can only be achieved through an Elliptical Curve Cryptography (ECC) issuing CA and a Card Authentication Key (CAK) issued from this ECC CA. The CAK is the only interoperable 1-factor, strong authentication solution that also conducts revocation checking. Validation is only done to an “endorsement key” which is the PIV content signing key, this ties the key on the card to the cardholder. Currently Washington Metro Area Transit Authority (WMATA) has a proof of concept implementation using the CAC as a fare card. The CAK is linked to a backend funds accounting system so money amounts are not written to the card itself.

Active Directory Mapping

Mr. Baldrige presented a second topic on PIV subject name mapping to multiple windows accounts using the password hint function through a registry edit. There was general discussion on the purpose of mapping multiple PIV/CAC to one account (operations center use case) or mapping multiple accounts to one PIV/CAC (system

admin use case). Mr. Baldrige said he has written a Windows PowerShell script to automate setup and can share it with anyone who wants to test it.

A question was asked if middleware or virtual software would support the hint function as well and there was a general response that it varies between products. Mr. Baldrige asked if any members were interested in writing a white paper to send to software providers to add this functionality to their products. Treasury, NASA, and DHS indicated they were interested in supporting the white paper development. Mr. Myers thanked Mr. Baldrige and then introduced Mr. Cloutier representing Microsoft for the next agenda item.

Action Item – Mr. Baldrige took an action with support from Treasury and DHS to develop a lessons learned white paper on how to map a PIV card to multiple logons using the security hint mechanism and how to get this is function with various middleware products.

Agenda Item 2 – Microsoft Trust Store Program (Jody Cloutier)

Mr. Cloutier apologized that he had a previous conflict during his new presentation time and would cede his agenda item back to the TWG. Mr. Myers apologized for the agenda change and informed the group this agenda item would be presented at the next TWG. Mr. Myers introduced Mr. Carl Wallace supporting DoD for the next agenda item.

Agenda Item 3 – Apple Over the Air (OTA) Vulnerability (Carl Wallace)

This presentation is limited only to installing certificates and private keys on Apple devices over the air to a mobile device management (MDM) service. The vulnerability presented is a weakness in:

- 1) The cryptography used by the Apple root CA (1024-bit key)
- 2) Apple root CA was expired but still issuing certificates
- 3) The method used by the Apple protocol (SCEP) to validate the device to/from the MDM was not binding the transaction to the device or the MDM
- 4) Apple root CA's can only be validated by name and date on the Apple website instead of through keys or hashes
- 5) The payload used during the registration process (P12) were not encrypted
- 6) The Apple protocol allows multiple ways of encoding the information transmitted and allows the encoding strategy to change during a single registration. Therefore a MITM can capture the SCEP, obtain the key and pass on a P12 format.

Mr. Wallace was able to conduct a successful man-in-the-middle (MITM) attack and compromise the registration session of multiple Apple devices. He also informed the group he has submitted a bug report to Apple who replied they investigated the issue and found it was not a vulnerability. The bug reported was submitted through the DoD

CIO office. If other agencies submit similar reports it may add weight to convince Apple they need to address this issue. The presentation was not shared and can be obtained by contacting Mr. Wallace directly. Mr. Myers thanked Mr. Wallace for his presentation.

The question was raised whether similar testing had been conducted with other devices such as Blackberry, Android, Microsoft, etc. Is the vulnerability inherent to the SCEP protocol or just the Apple implementation of MDM? Mr. Wallace said it was a factor of the manner in which the Apple over-the-air MDM was implemented and he had recommendations for the vulnerability could be mitigated.

Adjourn

Mr. Myers thanked everyone and asked if there were any questions. Mr. Baldrige suggested adjusting the meeting the time and length to a morning session on a day different than a Wednesday and making the meeting longer. Mr. Bello took the suggestion for consideration and thanked everyone for calling in.



Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By SRA International

**Friday
December 19, 2014**

10:30 a.m. – 12:00 p.m.

Teleconference

Time Topic

| | |
|-------|--|
| 10:30 | Welcome & Opening Remarks |
| 10:35 | Certificate Policy Change Request – ECU |
| 10:40 | Greatest Common Divisor / Collision Detection Presentation |
| 12:00 | Adjourn |

Presenter

| |
|--------------|
| Ola Bello |
| Wendy Brown |
| Todd Johnson |
| Ola Bello |

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

| Name | Organization |
|-------------------|--------------|
| Baldrige, Tim | DoD |
| Bello, Ola | FPKIMA |
| Brown, Wendy | FPKIMA |
| Chokhani, Santosh | DoD |
| Cimmino, Giuseppe | FPKIMA |
| Donohue, Paul | OMB |
| Foradori, Keith | DEA |
| Hansen, Maryam | DoD |
| Johnson, Todd | Treasury |
| Jung, Jimmy | State |
| Liston, Matthew | Treasury |
| McBride, Terry | Treasury |
| Myers, Kenneth | FPKIMA |
| Robinson, Buddy | Treasury |
| Salgado, John | DoD |
| Shorter, Scott | Electrosoft |
| Sulser, David | NRC |
| Wallace, Carl | DoD |
| Wyatt, Terry | NASA |

Agenda Item 1 - Welcome and Opening remarks (Ola Bello)

The FPKI TWG met via teleconference to discuss a potential new certificate threat. Mr. Kenneth Myers introduced the new chair of the TWG, Mr. Ola Bello. Mr. Bello thanked everyone for calling in today and looks forward to working with the TWG members in the future. Mr. Bello then turned it over to Wendy Brown to discuss the next agenda item.

Agenda 2 – Certificate Policy Change Request ECU (Wendy Brown)

Ms. Brown briefly described the two change requests presented in the Certificate Policy Working Group (CPWG).

1. The first change proposal is a modification to the *Federal Public Key Infrastructure (FPKI) X.509 Certificate and CRL Extensions Profile [FPKI-Prof]*. This change request makes the use of anyECU optional when ECU is asserted in the Key Management certificate to mitigate a potential risk in code signing certificates.
2. The second change proposal is a modification to the *FPKI X.509 Certificate and CRL Extensions Profile for PIV-I*. This change request makes the use of anyECU optional when ECU is asserted in PIV-I Authentication and PIV-I Digital Signature certificates.

Ms. Brown explained the TWG previously discussed making the ECU extension mandatory in all end-entity certificates and prohibiting the inclusion of the anyECU value, but was unable to reach consensus. These change proposals are a compromise position that allows issuing CAs to include the ECU without asserting anyECU which essentially allows the certificate to be used for any purpose, intended or not. CPWG is requesting the TWG review the requests and provide comments to the CPWG.

There was a question whether a similar change proposal was being proposed for PIV. The answer is there could be, again the change would only be to the *X.509 Certificate and CRL Extensions Profile for the Shared Service Provider Program*, as ECU is not mentioned in the Certificate Policy itself.

The change proposals were not reviewed in detail during the meeting.

Agenda 3 – Greatest Common Divisor / Collision Detection (Todd Johnson)

Mr. Todd Johnson introduced the agenda item by explaining there has been extensive work in academia and the commercial space around detecting certificate anomalies and the TWG should integrate the work being done to increase the security of the FPKI. The presentation will cover two topics:

1. **Batch Greatest Common Divisor (GCD)** – This method divides certificate public key by a list of known GCDs to determine if the random number generator

(RNG) is flawed. If the result of computation has a weak RNG then the output may show non-random sequences for further investigation.

2. **Digest Collisions** – This is another method to detect anomalies and is most prevalent with MD5 and SHA-1 certificate keys. The greatest benefit for this method is to detect malicious forgeries such as in digitally signed documents.

Microsoft has a Certificate Reputation (CertRep) program through the Internet Explorer “SmartScreen” program which tests web browser and code signing certificates. Some academic papers on this topic include:

- “Ron was Wrong, Whit is Right”
- “Mining your Ps and Qs: Detection of Widespread Weak Keys in Network Devices”
- “Factoring RSA keys from Certified Smart Cards: Coppersmith in the Wild”

A number of questions were asked about practical application in the FPKI and a few suggestions were made for potential actions which include:

1. Contact Microsoft to present the CertRep program to the TWG
2. Contact CA operators and vendors about their efforts in GCD or Collision Detection to analyze current and future certificates for weak RNG anomalies

Agenda Item 4 - Wrap-up and Adjourn Meeting (Ola Bello)

Suggestions were made for topics for future meetings:

- Mr. Johnson requested Mr. Tim Baldrige give his Smartcard Alliance presentation on the CAC WMATA pilot.
- Presentation on the Treasury SCVP service, possibly include other vendor SCVP demonstrations and any Agency requirements for SCVP
- Possible follow-up discussion on GCD analysis:
 1. How do we securely share information about weaknesses found?
 2. How do we ensure commercial entities doing this type of analysis will share discovered information with the FPKI?

Mr. Bello thanked those in attendance and closed the meeting as it had run twenty minutes over.

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

**Wednesday
July 30, 2014**

1:00 p.m. – 2:30 p.m.

General Services Administration 1800 F Street Northwest Washington, DC

| | | |
|------|---|-----------------|
| 1:00 | Welcome & Opening Remarks | Darlene Gore |
| 1:10 | New FPKI Certificate Profile Draft | Wendy Brown |
| 1:45 | Control of Outbound HTTP when Validating External Certificates* | Open Discussion |
| 2:00 | Evolving PKI-Related RFCs* | Wendy Brown |
| 2:20 | TWG Updates | Kenneth Myers |
| 2:30 | Adjourn | Darlene Gore |

***These two topics were tabled for the next formal TWG due to the Certificate Profile discussion running long.**

FPKI TWG July 30, 2014 Meeting Minutes

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or not identified their organization.

| Name | Organization |
|---------------------|-------------------|
| Ambs, Matthew | DHS |
| Baldrige, Tim | DoD |
| Berry, Jeff | Certipath |
| Brown, Wendy | Protiviti, FPKIMA |
| Carson, Michael | Symantec |
| Cobb, Lee | Energy |
| Cooper, David | NIST |
| Donahue, Paul | OMB |
| Cimmino, Giuseppe | Protiviti, FPKIMA |
| Chokhani, Santosh | Cygnacom |
| Gerhardt, Andrew | Verizon Business |
| Gore, Darlene | GSA |
| Head, Derrick | State |
| Huza, Christopher | HHS |
| Johnson, Todd | Treasury |
| Louden, Chris | Protiviti, FPKIMA |
| McBride, Terry | BAH, Treasury |
| Myers, Kenneth | Protiviti, FPKIMA |
| Shomo, Larry | DHS |
| Sikder, Faysal | CertiPath |
| Slusher, Tobi | HHS |
| Spainhour, Benjamin | USPTO |
| Wallace, Carl | Redhound |
| Weiser, Russ | Verizon Business |
| Wood, Daniel | Treasury |
| | |
| | |
| | |
| | |
| | |

Agenda Item 1 - Welcome and Opening remarks (Darlene Gore)

The FPKI TWG met at GSA, 1800 F Street Northwest, Washington DC. Ms. Darlene Gore opened the meeting by thanking everyone for attending. Mr. Kenneth Myers reviewed the agenda and then introduced the Ms. Wendy Brown to present the Federal PKI Certificate Profile draft presentation.

Agenda 2 – FPKI Certificate Profile Document Draft (Wendy Brown)

Ms. Brown introduced the discussion by covering the background of the document and intent of combining the certificate profiles into a single document. There was a consensus on aligning Signature and Public Key Algorithms across Common Policy and the FBCA CP. Since Common Policy (and PIV-I) allow a subset of what is allowed in the FBCA CP, this means recommending a change to the FBCA CP. It was pointed out that commercial PKIs are looking at additional algorithms and ECC Curves. When new algorithms or ECC Curves are widely accepted by commercial products, there may need to be further discussion about adding them to the FPKI CPs and certificate profiles.

There was a discussion about the proposal to make the Digital Signature bit optional in keyUsage when nonRepudiation is asserted in order for applications to more easily distinguish certificates meant for Authentication from those intended for Signature. There was concern this might cause problems with applications. Mr. Paul Donohue briefly went over his findings during informal testing of certificates using the proposed keyUsage, Mr. Donohue's test certificates all had the anyEKU or no EKU asserted. If the TWG wants to recommend this change, we would need to conduct formal testing to see how applications treat the suggested keyUsage change when the appropriate EKU are also asserted. However, the consensus of the group was that specified appropriate EKU in certificates would accomplish the same goal and is the preferred recommendation.

There was consensus of those attending that requiring appropriate EKU on all certificates would enhance security, because it would ensure that certificates were used for their intended purpose. However, Dave Cooper had sent an email stating:

“With the exception of the Card Authentication certificate the certificates on the PIV Card have to be general-purpose certificates. Including an EKU without anyExtendedKeyUsage by definition restricts the types of applications with which the keys can be used and that is contrary to HSPD-12 and FIPS 201.

As just one example, Section 6.3.1 of FIPS 201-2, in accordance with HSPD-12, states that the PIV Authentication certificate may be used for physical access. There is no key purpose OID defined for this. Even if we defined a new key purpose OID this would not help as applications would not recognize it.”

Todd Johnson and others said we would have to be very explicit about what EKUs should be asserted on the different types of certificate and we would need to be flexible about adding additional EKUs if they are defined for future applications. And if a future application requires a specific new EKU, there would be a lag before certificates would contain the new EKU. In addition, make sure the Code Signing Certificate Profile needs to include appropriate information about the life-time-signing EKU and the use of timestamps. In addition, there was a suggestion to consider defining a specific FPKI code signing policy OID. The suggestion to update the proposed certificate profile to include EKU and set up a follow-on meeting to discuss with Dave Cooper and NIST was taken for action.

A side conversation took place about the commercial PKI use of also putting EKU on CA Certificates to technically constrain the type of certificates a CA can issue and whether this is something the FPKI should consider. Santosh Chokhani stated we could not do that as it is a violation of the standard. He suggested using the Microsoft defined Application-Policy extension instead and he volunteered to contact Microsoft to get more information about the Application-Policy extension.

Chris Loudon asked the CertiPath representative if they have tested Physical Access Control Systems (PACS) PIV Authentication certificates without the anyEKU asserted and Jeff Barry confirmed all Approved Product List (APL) tested PACS work correctly without anyEKU assertion and have no known interoperability issues. He added as a bridge, CertiPath made this change for security purposes in March 2012 after the Microsoft vulnerability was discovered and have been operating in the FPKI environment without any interoperability issues since the change. The Microsoft vulnerability in question is that certificates with anyEKU/or noEKU asserted are valid when used for code signing in a Microsoft OS, and possibly other, environments. The solution of setting EKUs more explicitly in CertiPath's certificate profiles was determined to be the most effective approach to mitigate the vulnerability over time that is not a Microsoft specific solution.

There was consensus that if inhibitAnyPolicy is included in CA certificates, not setting it as critical would enhance interoperability. If policyConstraints are included the extension should be set critical. In addition, cross-certificates issued to the FBCA should set inhibitPolicyMapping skipCerts = 2 if the issuing CA wants relying parties that use that CA as a trust anchor to be able to trust certificates through the FBCA that are issued by one of the peer bridge's members.

ACTIONS:

1. Update proposed certificate profiles with consensus decisions and redistribute
2. Schedule another TWG meeting to discuss remaining proposed changes
3. Schedule a meeting with NIST to discuss the EKU recommendation
4. Follow-up with Santosh Chokhani for more information on using Microsoft Application Policy Extensions

5. The FPKIMA will investigate formal interoperability testing procedures for the proposed certificate profiles.

Agenda 3 – TWG Updates and Future Discussion Topics (Kenneth Myers)

Before closing the meeting, Mr. Myers displayed a list of proposed topics for future meetings and requested participants send topics of interest for discussion at a future TWG to either himself or the entire list. One of the topics displayed was the continuing need for two-way cross-certificates. A short discussion of existing DoD utilities for managing Relying Party trust stores was started by Tim Baldrige who said InstallRoot and TAMP are available on a DISA web page and suggested a valuable service for the FPKIMA to offer would be tailoring these tools for use by the FPKI Community.

Agenda Item 4 - Wrap-up and Adjourn Meeting (Darlene Gore)

Ms. Gore thanked everyone for attending and adjourned the meeting.

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

**Thursday
June 21, 2012**

9:00 a.m. – 12:30 p.m.

| | | |
|-------------|---|--|
| 9:00 | Welcome & Opening Remarks | John DiDuro Jeff Voiner |
| 9:15 | Enhanced Monitoring and Testing | Wendy Brown Jeff Jarboe |
| 10:15 | Tagging Certificate URL's for Analytics | Giuseppe Cimmino |
| 10:45 | Flamer/SkyWiper | TWG Discussion |
| 11:00-12:30 | EKU and Technical Constraints | Joint Session with CPWG Wendy Brown Jeff Barry Dave Cooper |

FPKI TWG June 21, 2012 Meeting Minutes

Attendance List

| Name | Organization | T-Teleconference P-Present |
|-------------------|----------------------|-------------------------------|
| Barry, Jeff | CertiPath | P |
| Bravo, Kathleen | IRS | T |
| Brown, Wendy | FPKIMA, Contractor | P |
| Cimmino, Giuseppe | GSA, Contractor | P |
| Cooper, David | NIST | P |
| DeAntonio, Damien | DHS, Contractor | P |
| DiDuro, John | GSA, Contractor | P |
| Donald, India | GSA, Contractor | P |
| Edmunds, Debbie | State | T |
| Gore, Darlene | GSA FPKIMA | T |
| Hansen, Maryam | BAH (DoD Contractor) | P |
| Head, Derrick | State | T |
| Hildebrand, Jeff | GPO | P |
| Jarboe, Jeff | GSA, Contractor | P |
| King, Matt | GSA, Contractor | P |
| Louden, Chris | GSA, Contractor | P |
| Rea, Scott | DigiCert | T |
| Robinson, Buddy | Treasury | T |
| Salgado, John | DoD | T |
| Samayoa, Manny | Entrust | T |
| Shomo, Larry | DHS, Contractor | P |
| Sikder, Faysal | CertiPath | P |
| Silver, Dave | GSA, Contractor | T |
| Slusher, Toby | HHS | T |
| Spence, Willie | IRS | T |
| Thomas, Michelle | Energy | T |
| Vargo, Peter | GSA, Contractor | P |
| Wallace, Carl | DoD, Contractor | T |
| Wilson, Gary | SAFE-BioPharma | T |
| Wyatt, Terry | NASA | T |

**Agenda Item 1
Welcome and Opening remarks
John DiDuro**

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

Mr. John DiDuro called the TWG meeting to order at approximately 9:00 am EST, and introduced those attending in person and via teleconference.

Mr. DiDuro welcomed the TWG and mentioned that due to competing events, this TWG meeting was moved from its originally-scheduled date of Tuesday, June 19, 2012. Even with the date change, there was very good participation from TWG members.

**Agenda Item 2
Enhanced Monitoring and Testing
Wendy Brown and Jeff Jarboe**

Ms. Wendy Brown and Mr. Jeff Jarboe presented the Enhanced Path Quality Monitoring and Testing overview. This initiative is a way to improve the user experience with the FPKI, and is complementary to the FIPS 201 testing done within GSA OGP. The TWG approved the overall approach and recommends that the FPKIPA Chair make it official. Ms. Brown stated that the testing program is a free offering at this point in time, but that may change if a large number of vendors desire participation.

The TWG discussed the potential Personally Identifiable Information (PII) impact on the use of sample production certificates for the operational testing. Mr. Jeff Barry from CertiPath suggested that the FPKIMA investigate a different approach to CITE, one where the FPKIMA establishes a simulated CA for each FPKI Affiliate CA rather than asking Affiliates to maintain a test environment connected to CITE. The alternative approach would create a more complete simulation of production in CITE, which would should operational testing. However, the alternative approach would not provide the same level of assurance of production path quality as with performing operational testing of vendor products in the production environment.

Several TWG members volunteered to assist with developing the Operational Test Suite that will be used for product testing.

ACTIONS:

1. Ms. Brown to obtain approval from the FPKIMA System Owner to pursue enhancement to AIA web crawler to automate path quality report generation.
2. Mr. Jarboe to finish PDVal process document and obtain TWG review.
3. Ms. Brown to draft initial operational test plan and invite TWG members to participate in the test plan development.
4. Ms. Brown to provide status reports to TWG (frequency to be determined).

Agenda Item 3
Tagging Certificate URL's for Analytics
Giuseppe Cimmino

Mr. Giuseppe Cimmino described the option of providing a unique URL for the corresponding p7c in each cross-certificate issued by the FBCA, which would allow the FPKIMA to obtain information about FPKI Repository usage. The consensus was that this may be perceived as an attempt to track individual usage, and would not yield very useful information. In addition, there may be a negative impact on a relying party's ability to rely on cached files. No PKI's represented at this TWG meeting are pursuing this level of analysis.

ACTIONS: None.

Agenda Item 4
Flamer/SkyWiper
TWG Discussion

Mr. Peter Vargo outlined the Flamer/SkyWiper malware vulnerability and described the importance of this exploit to the FPKI Community. A known prefix MD5 hash attack collision was used. There was consensus that SSL validation via MD5 hashing should no longer be tolerated, and that SHA-1 should be deprecated. It was noted that SHA-1 cannot be used within the FPKI after December, 2013.

There was then discussion about ways to counter future, similar attacks. The discussion included browser patches and configurations regarding acceptance of MD5 SSL certificates, and "protected" EKU. The TWG consensus is that generally-available commercial fixes, such as MD5-Shield, are sufficient to protect the FPKI Community.

ACTIONS: None.

Agenda Item 5
EKU and Technical Constraints
Joint Session with CPWG
Wendy Brown, Jeff Barry and Dave Cooper

A joint TWG/CPWG session was held to discuss EKUs and Technical Constraints. CertiPath introduced an approved change to their policy that lists optional and restricted EKUs for each of their certificate profiles. Mr. Barry presented alternatives for mitigating a vulnerability in the way Microsoft validates signatures on code, which is the driver for the change proposal. Mr. Barry then presented a list of pros and cons for each alternative.

Mr. Dave Cooper suggested that the FPKI Community might be morphing our PKI to address the issue rather than addressing the issue with Microsoft directly. Mr. Jeff

Hildebrand asked about the risks and benefits of addressing the issue using the EKUs. Mr. Barry suggested that specifying parameters around EKUs was the right compensating control for CertiPath but it may not be the right choice for the FPKI. Mr. Cooper suggested there might be a great risk of harm rather than improved security posture by requiring the EKUs. Mr. Hildebrand added that simplicity is the goal, use of the ECU adds complexity, and most applications check policy OIDs rather than EKUs.

In addition, due to the lifespan of certificates already issued, a change to the FPKI Trust Infrastructure certificate profiles that mandates inclusion of EKUs on all certificates containing a key usage of digital signature will not address the vulnerability issue for at least 3 years. Further, since Microsoft will continue to trust code-signing certificates past their expiration dates, the vulnerability issue will continue unless Microsoft changes the way it validates code signatures.

Mr. Cooper also noted that the PIV-I profile mandates inclusion of “anyEQU,” so there may be a risk that some PIV-I cards would become non-interoperable. Mr. Chris Loudon suggested that if these options are not acceptable, other options need to be explored. Reducing the attack surface is beneficial, but the FPKI Community needs to be concerned about uncovering unknown impacts. Therefore, our goal should be to stimulate long-term solutions. Mr. Gary Wilson suggested that evaluation of real risk is important so as not to create unviable solutions.

Ms. Maryam Hansen noted that the DoD believes further discussion and significant testing is required prior to the FPKI making any decision on adopting Certipath’s approach in specifying EKUs.

ACTIONS:

5. Mr. DiDuro will resend the white paper to the CPWG and TWG mail lists that provides detail about the Code Verification vulnerability issue.
6. Mr. DiDuro will resend the CertiPath Certificate Policy that includes the ECU change proposal to the FPKI TWG and CPWG for determination of impacts and issues.

**Agenda Item 6
Adjourn Meeting
John DiDuro**

Mr. DiDuro adjourned the TWG meeting at 12:15 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 |

FPKI TWG June 21, 2012 Meeting Minutes

| 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 ECU 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 (Wendy Brown) | 1/24/2012 | March 2012 | Closed |
| 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 (John DiDuro) | 1/24/2012 | March 2012 | Open |

FPKI TWG June 21, 2012 Meeting Minutes

| 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 (Wendy Brown) | 1/24/2012 | February 2012 | Closed |
| 39 | Create and maintain a TWG list of documents written to-date. | TWG (John DiDuro) | 1/24/2012 | March 2012 | Ongoing |
| 40 | Ms. Metzger Schoen to investigate future testing with the PKI Interoperability Test Tool (PITT) for path-validation. | S. Metzger Schoen | 3/22/2012 | TBD | Open |
| 41 | Add "permit nameConstraint" as potential work-around to CAPI issue and report findings | CertiPath (Jeff Barry) | 5/15/2012 | TBD | Open |
| 42 | Distribute ECU table from the CertiPath CP for TWG review and comment. | TWG (John DiDuro) | 5/15/2012 | Resend to TWG and CPWG prior to next TWG | Open |
| 43 | Obtain approval from system owner to pursue enhancement to AIA web crawler to automate path quality report generation. | FPKIMA (Wendy Brown) | 6/21/2012 | TBD | Open |
| 44 | Finish PDVal process document and obtain TWG review. | FPKIMA (Jeff Jarboe) | 6/21/2012 | TBD | Open |

FPKI TWG June 21, 2012 Meeting Minutes

| No. | Action Item | Point of Contact | Start Date | Target Date | Status |
|-----|---|-------------------------|------------|-------------|--------|
| 45 | Draft initial operational test plan and invite TWG members to participate in the test plan development. | FPKIMA (Wendy Brown) | 6/21/2012 | TBD | Open |
| 46 | Provide status reports to TWG on Enhanced Monitoring and Testing initiative (frequency to be determined). | FPKIMA (Wendy Brown) | 6/21/2012 | TBD | Open |
| 47 | Distribute the white paper to the CPWG and TWG mail lists that provides detail about the Code Verification vulnerability issue. | TWG (John DiDuro) | 6/21/2012 | 7/17/2012 | Open |

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

**Tuesday
May 15, 2012**

12:30 pm – 3:30 pm

| | | |
|-------|-------------------------------------|---|
| 12:30 | Device OID Mapping | Joint Session with CPWG Wendy Brown |
| 1:00 | Welcome & Opening Remarks | John DiDuro Jeff Voiner |
| 1:15 | OCSP Stapling | Tim Moses |
| 2:00 | Microsoft Relationship Development | Jeff Barry |
| 2:45 | Use of ECU in End User Certificates | Santosh Chokhani |
| 3:30 | Wrap-up and Adjourn Meeting | John DiDuro |

FPKI TWG May 15, 2012 Meeting Minutes

Attendance List

| Name | Organization | T-Teleconference P-Present |
|-------------------|-----------------------|-------------------------------|
| Baldrige, Tim | NASA | T |
| Barry, Jeff | CertiPath | P |
| Brown, Wendy | FPKIMA, Contractor | P |
| Chokhani, Santosh | DoD, Contractor | P |
| Cozzens, Scott | Treasury | T |
| DeAntonio, Damien | DHS | T |
| DiDuro, John | GSA, Contractor | P |
| Edmunds, Debbie | State | T |
| Hansen, Marianne | BAH (DoD Contractor) | P |
| Hildebrand, Jeff | GPO | P |
| Jarboe, Jeff | GSA, Contractor | P |
| Jeffers, Dan | DoD, Contractor (BAH) | T |
| Keating, Amy | SSA | T |
| King, Matt | GSA, Contractor | P |
| Moses, Tim | Entrust | T |
| Salgado, John | DoD | T |
| Shomo, Larry | DHS, Contractor | P |
| Silver, Dave | GSA, Contractor | T |
| Slusher, Toby | HHS | T |
| Spence, Willie | IRS | T |
| Spencer, Judy | CertiPath | T |
| Sulser, Dave | NRC | P |
| Thomas, Michelle | Energy | T |
| Wyatt, Terry | NASA | T |

**Agenda Item 1
Device OID Mapping
Joint Session with CPWG
Wendy Brown**

The FPKI TWG met at Protiviti Government Services, 1640 King Street, Suite 400, Alexandria, VA beginning with a joint session with the CPWG.

Mr. John DiDuro called the TWG meeting to order at approximately 12:30 pm EST, and introduced those in person and via teleconference.

Ms. Wendy Brown explained that when the new device policy object identifiers (OIDs) were added to the Federal Bridge Certification Authority (FBCA) and Federal Common Policy Certification Authority (FCPCA) certificate policies (CPs), the cross-certificates between the FBCA and FCPCA were re-issued to include the new OIDs. The policy mapping extension mapped common-device to FBCA mediumDevice and common-deviceHW to FBCA mediumDeviceHW. This created a potential problem for certificate paths of Affiliates that previously had a device policy OID mapped to common-device. The initial rule the Federal Public Key Infrastructure Management Authority (FPKIMA) followed was that a policy cannot be mapped to something else and be passed on directly. Ms. Brown presented examples highlighting the issue, as well as options for mitigating the issue including the re-issuance of cross-certificates between the FBCA and FCPCA.

Mr. Tim Baldrige supported the suggestion that both the FBCA and FCPCA should contain all the OIDs from both CPs. Simplification via a single policy and single set of OIDs is preferred. Mr. Santosh Chokhani said he never understood why there were two separate CPs, and that it would make sense for the CPs to be combined.

It was suggested it would be cleaner to re-issue the cross-certificates between the FBCA and the affected Affiliate CAs. Mr. Jeff Barry agreed with this approach, and indicated that CertiPath, not seeing the need for an immediate correction, would be willing to re-issue their cross-certificate during their June 2012 key signing ceremony.

Mr. Baldrige suggested that the FPKI Community be notified when new cross-certificates have been issued.

ACTIONS for CPWG:

1. CertiPath will correct the OID mapping in their next certificate signing ceremony, which is scheduled for June 2012.
2. The FPKIMA will coordinate with affected Affiliates to have corrected cross-certificates issued.
3. When the new cross-certificates have been issued, the FPKIMA will inform the FPKI Community (via the FPKIPA email list) why the reissuance was necessary.

Agenda Item 2
Welcome and Opening remarks
John DiDuro

Mr. DiDuro welcomed the TWG and mentioned that due to competing events (primarily the DoD Identity Management Conference in Anaheim, CA), this TWG meeting has lower than normal attendance.

Agenda Item 3
OCSP Stapling
Tim Moses

Mr. Tim Moses, a Certification Authority/Browser (CAB) Forum participant, presented a provocative discussion about certificate revocation – that it doesn't work within a publicly-trusted Public Key Infrastructure (PKI). Mr. Moses discussed several revocation issues to support the claim.

Mr. Moses introduced the concept of "hard fail"¹ and asserted that it is desirable to PKI relying parties. To implement hard fail, relying parties, applications, operating systems, certification authorities (CAs), and subscribers need to work together.

Mr. Moses provided an overview of Online Certificate Status Protocol (OCSP) stapling, where a subscriber obtains an OCSP response and sends it with (i.e., stapled to) the certificate during a Transport Layer Security (TLS) handshake. He then provided a potential path toward community-wide adoption of hard fail via OCSP stapling, and presented evidence that most browsers are beginning to support stapling (browsers ask for the OCSP stapling, but do not necessarily fail when not supplied). However, very few web servers return OCSP stapling at this time. In addition, stapling provides revocation information about the end-entity certificate, but not the CA certificates in the path. There is a new Internet Engineering Task Force (IETF) work item to allow multi-stapling to address the entire certificate path.

Mr. Moses concluded by challenging the TWG to support a transition strategy toward hard fails and adoption of OCSP stapling by subscribers.

During the discussion, points were raised (from the TWG perspective) that availability rather than hard fail is more desirable. In addition, it was noted that there is no effective way to ascertain the opinion of relying parties regarding the hard fail notion.

ACTIONS: None.

¹ If revocation information is not returned in a timely manner, the application should act as it would if the certificate had been revoked .

Agenda Item 4
Microsoft Relationship Development
Jeff Barry

Mr. Barry described some continued issues with Microsoft's Cryptographic Application Programming Interface (CAPI) and how CertiPath is leveraging its findings on building a cooperative relationship with Trevor Freeman (Microsoft lead for federal government), which may lead to escalation of this issue to Microsoft senior management. Mr. Barry pointed out that while the fix process within Microsoft is slow, CertiPath interoperability testing's ability to discover CAPI issues is progressing quickly.

To get Microsoft to address issues, it is important to highlight to them the business impact (i.e., cannot accept PIV-I) on the FPKI Community. Accordingly, the CertiPath Policy Management Authority (PMA) will be sending waves of similarly-formatted bug reports to Microsoft.

Mr. Barry discussed a recently-discovered issue where nameConstraints in the path causes Windows 7 CAPI to return a nameConstraints error if the end-entity certificate contains a Uniform Resource Name (URN) for Universally Unique Identifier (UUID). This means that Personal Identity Verification - Interoperable (PIV-I) Authentication certificates (which require UUID) issued by PIV-I issuers approved through the CertiPath Bridge do not validate back to the FCPCA.

ACTIONS

4. CertiPath will test adding a "permit nameConstraint" as a potential work-around to the latest CAPI issue, and will report back their findings.

Agenda Item 5
Use of EKU in End User Certificates
Santosh Chokhani

Mr. Chokhani described how any digital signature certificate without an explicit Extended Key Usage (EKU) can be used for signing anything (e.g., code, time). Mr. Chokhani then described the merits of optional EKUs versus required EKUs, and preventing misapplication of an EKU when using a special-use certificate. One needs to ensure that applications looking at EKU (a) have the appropriate settings specified, and (b) avoid AnyEKU to not override the intent of limiting what can be used for codeSigning.

ACTIONS

5. Distribute the EKU table from the CertiPath CP for TWG review and comment.

**Agenda Item 6
Adjourn Meeting
John DiDuro**

Prior to adjournment, Mr. Baldrige asked for volunteers to help test some software code he is willing to share to get an independent, third-party review of an active project's development effort. In exchange for the code, Mr. Baldrige requires a quick turnaround on the test results.

Mr. DiDuro adjourned the TWG meeting at approximately 3:20 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 |

FPKI TWG May 15, 2012 Meeting Minutes

| 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 ECU 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 |

FPKI TWG May 15, 2012 Meeting Minutes

| 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 | Closed |
| 39 | Create and maintain a TWG list of documents written to-date. | TWG (J.DiDuro) | 1/24/2012 | March 2012 | Ongoing |
| 40 | Ms. Metzger Schoen to investigate future testing with the PKI Interoperability Test Tool (PITT) for path-validation. | S. Metzger Schoen | 3/22/2012 | TBD | Open |
| 41 | Add "permit nameConstraint" as potential work-around to CAPI issue and report findings | CertiPath (Jeff Barry) | 5/15/2012 | TBD | Open |
| 42 | Distribute ECU table from the CertiPath CP for TWG review and comment. | TWG (J. DiDuro) | 5/15/2012 | 5/30/2012 | Open |

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

**Thursday
March 22, 2012**

1:00 p.m. – 3:30 p.m.

| | | |
|------|--|--|
| 1:00 | Welcome & Opening Remarks | Chris Loudon Jeff Voiner |
| 1:15 | FPKI Technical Working Group Update | John DiDuro |
| 1:45 | Authority Information Access (AIA) Crawler | Sandy Metzger Schoen |
| 2:45 | RSA Conference Re-Cap | Chris Loudon Giuseppe Cimmino Open to all participants |
| 3:15 | Actions and Next Steps | Wendy Brown John DiDuro |
| 3:30 | Adjourn Meeting | John DiDuro |

FPKI TWG March 22, 2012 Meeting Minutes

Attendance List

| Organization | Name | T-Teleconference P-Present A-Absent |
|------------------|---|---|
| Verizon Business | Blanchard, Deb | T |
| GSA (Contractor) | Brown, Wendy | P |
| DoD (Contractor) | Chokhani, Santosh | T |
| GSA (Contractor) | Cimmino, Giuseppe | P |
| GSA (Contractor) | DiDuro, John | P |
| State Department | Edmonds, Deb | T |
| DHS (Contractor) | Fisher, Dave | T |
| State Department | Head, Derick | T |
| GSA (Contractor) | Louden, Chris | P |
| GSA (Contractor) | Metzger Schoen, Sandy | P |
| GSA (Contractor) | Packham, Jordan | P |
| ??? | Robinson, Lee | T |
| DoD (Contractor) | Salgado, John (works with Dan Jeffers) | T |
| DHS (Contractor) | Shomo, Larry | P |
| ??? | Spencer, Willie | T |
| DoE | Thomas, Michelle | T |
| NASA | Wyatt, Terry | T |

Agenda Item 1
Welcome and Opening Remarks
Chris Loudon

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

Mr. John DiDuro called the TWG meeting to order at approximately 1:00 pm EST, and introduced those in person and via teleconference. Mr. Chris Loudon welcomed the TWG and mentioned that because of the TSCP Event, the TWG experienced lower than normal attendance.

Agenda Item 2
FPKI Technical Working Group Update
John DiDuro

Mr. DiDuro presented an overview of the past topic areas covered by the FPKI TWG and outlined future topics for TWG consideration. In addition, Mr. DiDuro presented a listing of documents produced by the TWG over the past year. The ensuing discussion sparked several areas for the TWG to address, including:

Name Constraints

Issue with name constraints – and subjectAltName and UUID – any nameConstraints appears to break Microsoft interpretation of the UUID as a valid SAN.

Mr. Santosh Chokhani said that Cygnacom may have uncovered some additional Microsoft issues very recently, and will be reporting their findings once formalized. The TWG requests details from Mr. Jeff Barry once they're known.

Microsoft Issues, in general

Mr. Loudon stated that the FPKIPA will be speaking with Microsoft again on this topic in an attempt to get a reaction to the U.S. Government's continued concern regarding their products.

Mr. Chokhani encouraged the FPKIPA to not ask Microsoft to make a judgment call, but to just correct their known issues.

The TWG community needs to identify additional tests for PDVAL testing to encourage Microsoft to enforce the standards to which others subscribe. In essence, Microsoft is violating several security issues by building paths beyond the root and causing excessive network traffic (at both the Certification Authority (CA) infrastructure's wide area network and at the end-user's local area network).

ACTIONS:

1. Mr. DiDuro to maintain the briefing that describes TWG events and deliverables.

Agenda Item 3
Authority Information Access (AIA) Crawler
Sandy Metzger Schoen

Ms. Sandy Metzger Schoen presented a briefing on the AIA crawler, which is a tool to discover and path-validate all CA certificates cross-certified with the Federal Common Policy (SHA-256) CA. The AIA crawler runs automatically on a weekly basis.

There were numerous discussions regarding the tool's use, future enhancements, and technical details of the tool's coding. Highlights of those discussions include:

- The tool does policy validation to all FPKI Object Identifiers (OIDs) and all FPKI Test OIDs including new EGTS OIDs.
- The tool summarizes various output files that are available and provides example Subordinates by agency or full paths.
- The tool does Online Certificate Status Protocol (OCSP) & Certificate Revocation List Distribution Point (CRLDP) validation checking – errors may include if the OCSP and CRLDP do not provide the same results and why.
- The tool uses custom code for the AIA chain and PKIX java library for general path, OID and path validation.

ACTIONS

2. Ms. Metzger Schoen to investigate future testing with the PKI Interoperability Test Tool (PITT) for path-validation.

Agenda Item 4
RSA Conference Recap
Giuseppe Cimmino

Mr. Giuseppe Cimmino, FPKIMA Platform Team lead, discussed his interaction with the BlueCoat federal team and a potential linkage with the FPKI TWG for future meetings.

ACTIONS

None

**Agenda Item 5
Acton and Next Steps
Wendy Brown**

Ms. Wendy Brown mentioned that the CAB Forum is developing network security guidelines that may be of interest to the FPKI TWG. In addition, Ms. Brown mentioned that the Four Bridges Forum is looking to develop audit requirements.

**Agenda Item 6
Adjourn Meeting
John DiDuro**

Mr. DiDuro adjourned the TWG meeting at approximately 3:00 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 |

FPKI TWG March 22, 2012 Meeting Minutes

| 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 ECU 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 |

FPKI TWG March 22, 2012 Meeting Minutes

| 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 | Closed |
| 39 | Create and maintain a TWG list of documents written to-date. | TWG (J.DiDuro) | 1/24/2012 | March 2012 | Ongoing |
| 40 | Ms. Metzger Schoen to investigate future testing with the PKI Interoperability Test Tool (PITT) for path-validation. | S. Metzger Schoen | 3/22/2012 | TBD | Open |

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

February 2012 TWG Highlights (in lieu of a meeting)

The February 2012 TWG meeting was cancelled due to scheduling conflicts with a number of key security-related activities, most notably ICAM Sharing Day and the RSA 2012 Conference. The following are several important updates.

Encryption Certificate Lookup Testing with CITE

Status: The TWG organized a test team meeting in mid-February 2012 to further explore encryption certificate lookup. The goals of the team are to test potential encryption certificate lookup models in support of encrypted email across the FPKI community, and make recommendations to the full TWG on viable models/requirements.

Next steps: The team is setting a realistic pace to establish requirements and test environments. Tasks were assigned to members from the Federal Public Key Infrastructure Management Authority (FPKIMA) as well as affiliates. Wendy Brown will report status to the TWG on a recurring basis until the team is ready to brief interim findings.

Introducing a new TWG Co-Chair

Jeff Voiner has joined Darlene Gore as a full-time member of the General Services Administration (GSA) Federal Acquisition Service (FAS) FPKIMA team, and will be co-chairing the TWG going forward. Jeff, while new to GSA, has been in federal service for seven years, and has been in an array of information technology positions for GSA and within private industry for PricewaterhouseCoopers and Mellon Financial. Jeff is anxious to use his considerable skills to help improve the PKI technical community.

Next TWG Meeting

The next TWG will be held on Tuesday, 20 March 2012.

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 |

FPKI TWG February 2012 Highlights

| 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 ECU 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 | Closed |
| 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 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 |

FPKI TWG February 2012 Highlights

| No. | Action Item | Point of Contact | Start Date | Target Date | Status |
|-----|---|---------------------|------------|---------------|--------|
| 36 | 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 | Closed |
| 39 | Create and publish a TWG list of documents written to-date. | TWG (J.DiDuro) | 1/24/2012 | February 2012 | Open |

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 |

FPKI TWG January 24, 2012 Meeting Minutes

Attendance List

| Organization | Name | T-Teleconference P-Present A-Absent |
|---|--------------------|--|
| NASA | Baldrige, 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 Loudon introduced Mr. DiDuro as the new TWG lead/coordinator, and noted that there would be no changes in direction or support. Mr. Loudon 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 Baldrige noted this is a move towards the best commercial practice of removing LDAP URIs out of cross-certificates. Mr. Baldrige 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. Baldrige 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. Baldrige 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 production 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 |

FPKI TWG January 24, 2012 Meeting Minutes

| 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 ECU 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 |

FPKI TWG January 24, 2012 Meeting Minutes

| 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 |



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

FPKI TWG December 20, 2011 Meeting Minutes

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 Loudon

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.

CBCA to Lockheed Martin



| CertiPath OIDs | LMCO OIDs |
|-------------------------|--------------------------|
| [...24019.1.1.1.17 msw] | [...103.100.1.1.3.2 msw] |
| [...24019.1.1.1.18 mhw] | [...103.100.1.1.3.1 mhw] |

Policy Mappings:

[1] Issuer Domain=...24019.1.1.1.17
Subject Domain=...103.100.1.1.3.2

[2] Issuer Domain=...24019.1.1.1.17
Subject Domain=...103.100.1.1.3.1


[3] Issuer Domain=...24019.1.1.1.18
Subject Domain=...103.100.1.1.3.1

Mapping [3] is 'lost'
because it's Subject
Domain has already
been encountered in
Mapping [2]

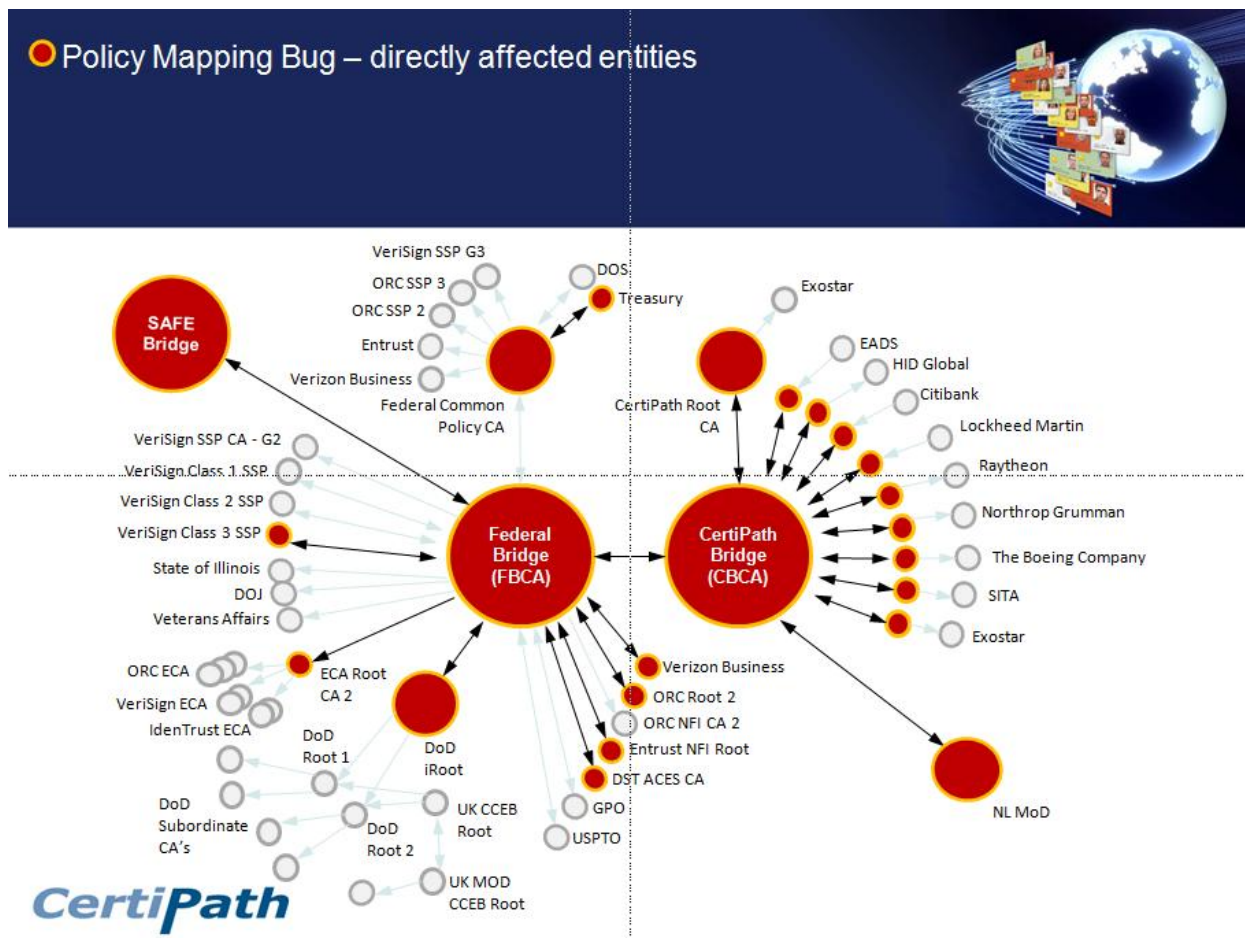
✓

✓

X



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 ECU 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 ECU 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 |

FPKI TWG December 20, 2011 Meeting Minutes

| 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 ECU 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 |

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

October 25, 2011

9:00 a.m. – 12:00 p.m.

| | | |
|-------|---|--------------|
| 9:00 | Welcome & Opening Remarks Introductions | Matt Kotraba |
| 9:05 | Microsoft Timestamp Authority Position Paper Update | Wendy Brown |
| 9:15 | Plans for Encryption Certificate Lookup & Retrieval Testing | Wendy Brown |
| 9:20 | Microsoft Path Building Anomalies Design Change Request Update | Matt Kotraba |
| 9:30 | Trust Store Management Guidance | Matt Kotraba |
| | <ul style="list-style-type: none">• Logistics for developing guidance | |
| 9:40 | <ul style="list-style-type: none">• Review and discuss research findings<ul style="list-style-type: none">○ ICAM Roadmap Guidance○ USGCB / FDCC Settings○ DoD PKE Guidance | |
| 10:30 | <ul style="list-style-type: none">• Recommendations Paper Outline & Writing Assignments<ul style="list-style-type: none">○ Problem Statement○ Current Status of Federal Guidance○ Recommendations | |
| 12:00 | Adjourn Meeting | Matt Kotraba |

FPKI TWG October 25, 2011 Meeting Minutes

Attendance List

| Organization Supported | Name | Email | P-Present/ T- Teleconference |
|---------------------------------------|------------------|--|------------------------------------|
| CertiPath | Jeff Barry | jeff.barry@certipath.com | P |
| 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 |
| DHS | Larry Shomo | Lawrence.Shomo@associates.dhs.gov | P |
| DHS | Neal Fuerst | Neal.Fuerst@ASSOCIATES.HQ.DHS. GOV | T |
| DHS | David Fisher | David.Fisher@ASSOCIATES.HQ.DHS .GOV | T |
| DigiCert | Scott Rea | Scott.Rea@DIGICERT.COM | 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 | T |
| eValid8 | Jim Schminky | james.schminky@evalid8.com | P |
| GSA | Darlene Gore | darlene.gore@gsa.gov | T |
| GSA | Jeff Voiner | jeffrey.voiner@gsa.gov | T |
| GSA | Albert Ingram | albert.ingram@gsa.gov | T |
| GSA (Contractor) | Brant Petrick | Brant.Petrick@gsa.gov | P |
| GSA (Contractor) | Chris Loudon | chris.loudon@pgs.protiviti.com | P |
| GSA (Contractor) | Dave Shepherd | DSHEPHERD@lmi.org | T |
| 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 |
| HHS | Toby Slusher | tus8@CDC.GOV | P |
| NRC | David Sulser | david.sulser@nrc.gov | P |
| PTO | Amit Jan | Amit.Jain@USPTO.GOV | T |
| Safe-Biopharma | Gary Wilson | gwilson@SAFE-BIOPHARMA.ORG | T |
| Treasury | Dan Wood | Daniel.Wood@treasury.gov | P |

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

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
Microsoft Timestamp Authority Position Paper Update
Wendy Brown

Wendy Brown informed the TWG that Microsoft responded to the FPKI TWG Timestamp Server Authority (TSA) Position Paper and Microsoft is still moving forward with the TSA requirement to maintain the codeSigning Extended Key Usage (EKU) property in the Windows Root Certificate Program. The FPKI Policy Authority (FPKIPA) Chair submitted a 180-day extension request to Microsoft to obtain additional time for the FPKIPA to address the TSA requirement.

Matt Kotraba shared the results of the survey sent to the FPKIPA on the usage of code signing certificates. The survey revealed several findings:

- The Department of Defense (DoD) does issue code-signing certificates for use on code shared externally (however DoD is not directly under Common Policy CA) and that DoD uses a Verisign TSA.
- The United States Postal Service uses commercial code-signing certificates
- The Department of Treasury shares externally with financial institutions along with distributing the Treasury Root.

The TWG agreed that more information on agency use of code-signing certificates is necessary to gauge the full impact of dropping the codeSigning EKU from Common Policy.

Use of the FPKI Community Interoperability Test Environment (CITE) to test the effects of dropping the codeSigning EKU from the Windows Trust Store was discussed. However, there is not enough known to effectively model and simulate the FPKI usage of code signing, and therefore the results of the test may not give an accurate depiction of what will occur in production environments.

ACTIONS

1. Matt Kotraba will inform Deb Gallagher that there are FPKI members who currently have a TSA as one solution to this issue..

Agenda Item 3
Plans for Encryption Certificate Lookup & Retrieval Testing
Wendy Brown

Wendy Brown informed the TWG that testing of the Transglobal Secure Collaboration Program (TSCP) Secure Email (SE) solution for public encryption certificate lookup and retrieval (*discussed at the September 2011 TWG*) will take place after the TWG completes the *Trust Store Management Guidance* document. Certipath, NRC, and NASA have already volunteered to participate in the test. TWG is actively seeking additional volunteers who are willing to assist with this effort.

ACTIONS

- None.

Agenda Item 4
Microsoft Path Building Anomalies Design Change Request Update
Matt Kotraba

Matt Kotraba provided an updated status of the NASA and NRC open tickets with Microsoft regarding “Microsoft Cryptographic Application Programmer Interface (CAPI) Path Building Anomalies” (*discussed at the September 2011 FPKI TWG*). NASA needs assistance in building their business case with Microsoft. The DoD has also experienced similar path building issues where Microsoft selects an inappropriate chain. NASA is looking for impact statements which specify the impact to the affected organizations, the number of users this issue affects, and specific examples to include screen shots or logs that capture examples of incorrect paths being selected.

Santosh Chokhani informed the TWG of a DoD VIP session with Microsoft involving a 4-star General. This issue is on the list of top DoD issues with Microsoft products. Dan Jeffers indicated the DISA DoD PKE group does not have its own Premier support agreement with Microsoft and instead must rely on the Services and Agencies within the DoD to submit tickets to Microsoft. .

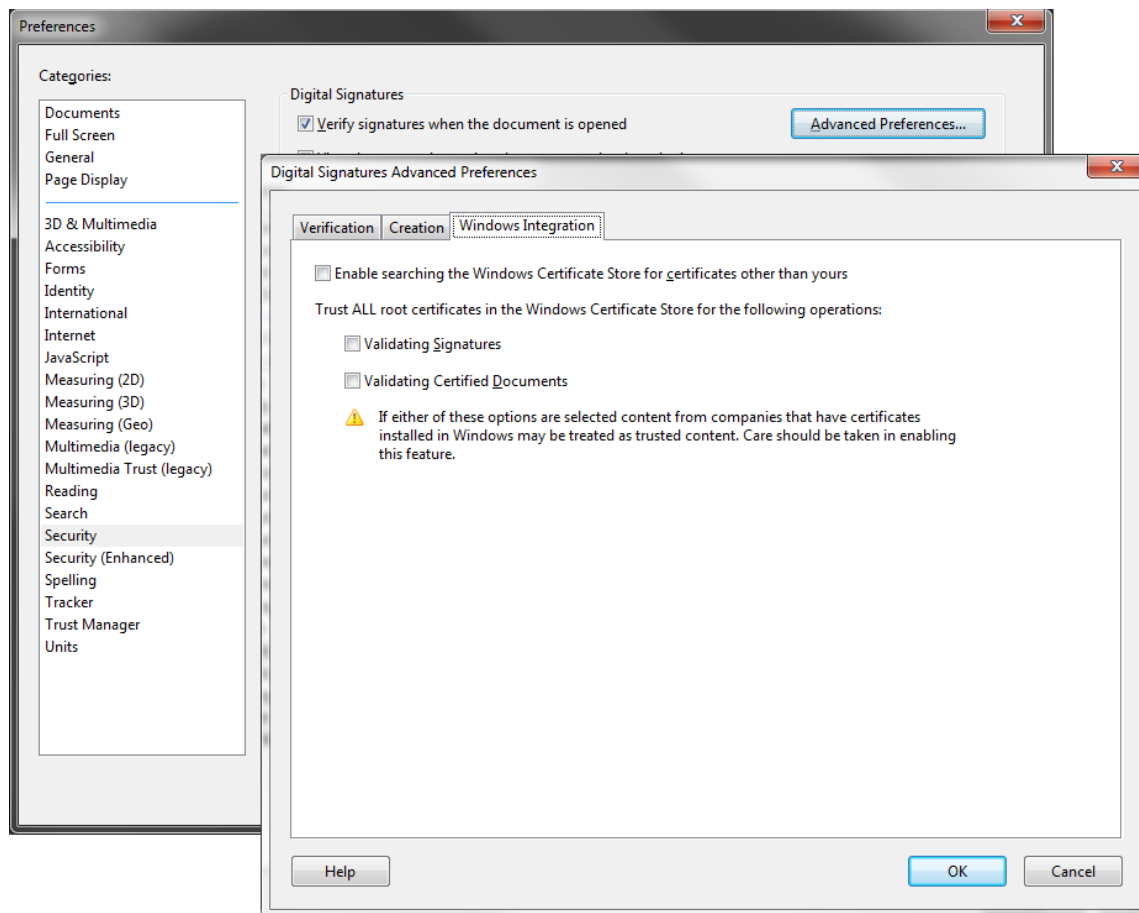
ACTIONS

1. Dan Wood will submit a request to Treasury to see if Treasury has experienced similar path building issues with Microsoft.
2. Santosh Chokhani will check if the DoD VIP session with Microsoft included this path building issue and determine what if any action is being taken by Microsoft. Santosh will include the information about the NASA and NRC tickets that have been opened to assist DoD in associating their issue with a wider impact across the entire federal community.

Agenda Item 5
Trust Store Management Guidance Working Session
Matt Kotraba

Matt Kotraba led a review of the Trust Store Management research findings, which included ICAM Roadmap guidance, NIST U.S. Government Configuration Baseline (USGCB) and Federal Desktop Core Configuration (FDCC) settings, and DOD PKE guidance presented at the April 2011 Identity Protection and Management (IdPM) Conference.

- The draft ICAM Roadmap Guidance version 2 (*not yet published*) includes definitions of Trust Anchors and the Trust Anchor Management Protocol (TAMP), but does not provide system owner / administrator level guidance for configuring current vendor products.
- USGCB and FDCC provide Trust Store settings for Windows systems, but do not provide settings for non-Windows systems or supplemental guidance on how a system owner should manage their Trust Stores manually if they choose to do so.
- An Adobe setting to leverage Microsoft CAPI was discussed. To access the setting in Adobe Reader 9, click Edit, Preferences (or Ctrl-K), click the security category on the left menu, then click on Advanced Preferences, then the Windows Integration tab. See screen shot below for available settings in Adobe Reader 9.



Details on these Adobe settings are discussed on <http://learn.adobe.com/wiki/pages/viewpage.action?pageId=67076127>.

Two Adobe posts are particularly relevant.

- “There are several checkboxes in the Security->Advanced preferences relating to Windows Integration. How do these affect Acrobat and Reader's interaction with the Microsoft Certificate Store and CAPI?

During chain-building of the signature process, Acrobat and Reader search all over for the needed certificates; the Acrobat Address Book (AAB), the Windows Cert Store, the CertCache folder, P12/PFX files, smart cards and tokens, and maybe even the internet if bFollowURLsFromAIA (a registry option) is turned on. Other than the last item, Acrobat doesn't care one iota what reg key or preference setting is selected. It builds the chain, top to bottom, as best it can.

Now comes time to establish trust. Here's is where the "use Windows trust anchor" option comes into play. Either it's off (the default setting) and the only place Acrobat can use to establish trust is the AAB, or it's on and Acrobat will use both the AAB and Windows. They are not mutually exclusive.”

- “Is there a way to force Acrobat/Reader to use CAPI for OCSP checking? If so - what's the regkey? Also, what are the implications?

The order in which revocation checkers are invoked is fixed. It is always OCSP->CRL->CAPI discriminated against the content of cRevocationChecker array in the registry. If cRevocationChecker is not defined all three are used in the listed order. If cRevocationChecker is defined then only those that are defined in cRevocationChecker are used but in the same order sans those that are not in cRevocationChecker array. For instance if cRevocationChecker array contains MSCAPI_RevocationChecker and Adobe_OCSPRevChecker (in this order) then only these two will be used but Adobe_OCSPRevChecker first and MSCAPI_RevocationChecker second, not in the order they are listed in cRevocationChecker array.

LTV has embedded OCSP/CRL. Those are always checked with Acrobat's code, not CAPI. However, if only MSCAPI revocation checking is enabled then embedded LTV info will NOT be used, eliminating the benefit of this long-term validation information.”

- An important lesson learned was gained from the DoD effort to use automated tools to remove unnecessary Trust Anchors from application Trust Stores. The automated tools often removed Trust Anchors that were necessary for system operations. System owners and administrators must be involved in the Trust Anchor assessment in order to properly identify the necessary Trust Anchors and avoid system performance issues.
- DHS found challenges identifying the Trust Anchors necessary for drivers and access to external websites. Dan Wood recommended contacting the DHS Trusted Internet Connections (TIC) Access Provider group to find out more on what external sites are accessed.

The second half of this session focused on developing a white paper for the FPKIPA and ICAMSC audience detailing the challenges associated with managing the current vendor Trust Stores, the current state of Federal guidance, and recommendations to enhance Federal guidance on Trust Store Management.

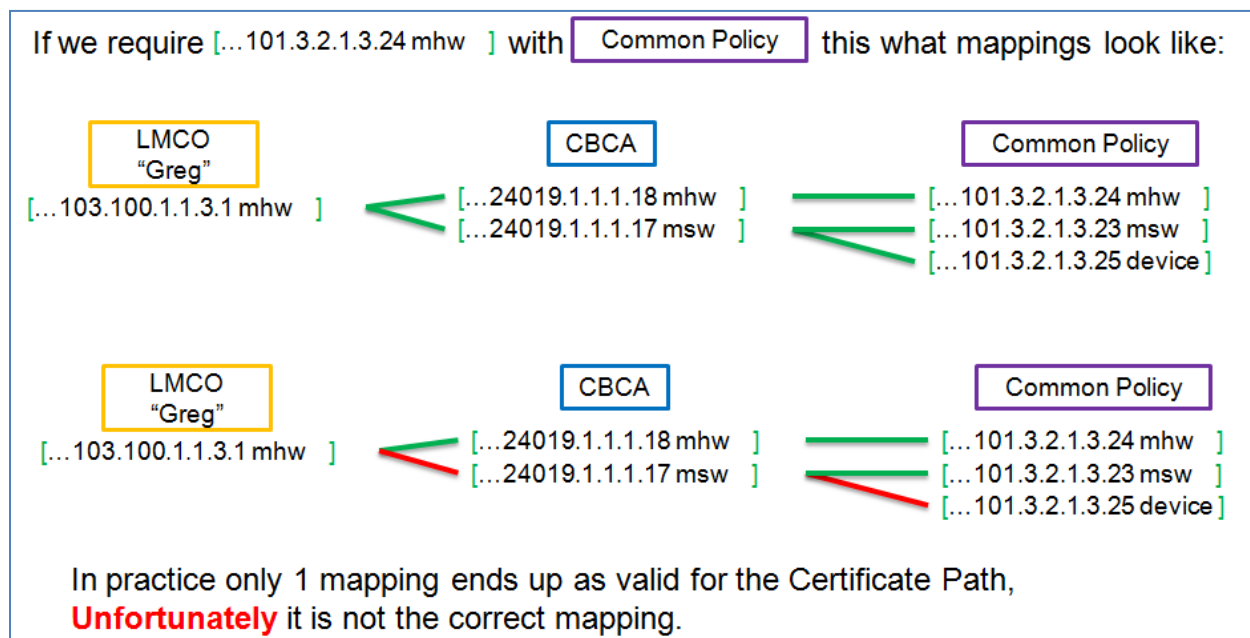
- Matt Kotraba led the review of a proposed outline for this white paper and comments were captured during the meeting.
- To facilitate additional community participation in the development of the white paper the full TWG review of the draft paper was pushed back until the December 2011 TWG.

ACTIONS

1. Once finalized, Matt Kotraba will send the TWG a copy of the ICAM Roadmap version 2.
2. Matt Kotraba will coordinate with the DoD PKE group to find out more on the process used by DoD to identify which Trust Anchors were required in their environment.
3. Dan Wood to provide TWG a copy of the Treasury's Participation in the Federal PKI ECO-System white paper. (completed)

Open Discussion Microsoft CAPI Policy Mapping Anomalies Santosh Chokhani and Jeff Barry

Santosh Chokhani and Jeff Barry introduced an issue with Microsoft CAPI policy mapping during the path building process. When Microsoft CAPI runs into multiple policy mappings from the issuer domain mapped to the same policy in the subject domain, CAPI only selects the first mapping in the list. The illustration below helps to visualize the error.



Within the Certipath community, this issue is causing significant user authentication issues with applications that leverage policy mappings during the authentication process. There was significant interest from the TWG to put this issue on the November 15, 2011 TWG meeting agenda.

ACTIONS

1. Follow-up action for Jeff Barry and Santosh Chokhani to prepare a full session on this topic at the November 15, 2011 TWG meeting.

**Agenda Item 6
Adjourn Meeting
Matt Kotraba**

The next FPKI TWG meeting is scheduled for Tuesday, November 15, 2011 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.

Matt Kotraba adjourned the FPKI TWG meeting at 12:00 p.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 |
| 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 | Closed |
| 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 |
| 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 | Closed |
| 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 | Closed |
| 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 | Closed |
| 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 |

FPKI TWG October 25, 2011 Meeting Minutes

| No. | Action Item | Point of Contact | Start Date | Target Date | Status |
|-----|--|---------------------------|------------|----------------------------------|--------|
| 19 | Contact the FPKI TWG to identify members for the Trust Management Guidance tiger team. | FPKIMA (Matt Kotraba) | 9/15/2011 | 10/15/2011 | Closed |
| 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 | 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 | Open |
| 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 | Open |
| 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 | Open |
| 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 | Open |
| 27 | Provide TWG a copy of the Treasury's Participation in the Federal PKI ECO-System white paper. | Treasury (Dan Wood) | 10/25/2011 | 10/25/2011 | Closed |
| 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 | Open |
| 29 | Prepare a TWG session for the Microsoft CAPI Policy Mapping Anomalies issue | Certipath (Jeff Barry) | 10/25/2011 | 11/15/2011 | Open |

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 Loudon |
| 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 3 rd 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 Loudon |

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 Loudon | chris.loudon@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@bpd.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 Loudon

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 Loudon 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 ECU 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 Baldrige 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 Baldrige
- 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 Loudon

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 Loudon 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 |

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 Loudon |
| 10:00 | FPKI Community Interoperability Test Environment (CITE) Comment Review | Wendy Brown / Jeff Jarboe |
| 11:15 | PKI Repository Requirements Evolution | Wendy Brown / Chris Loudon |
| 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 Loudon |

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 Loudon | chris.loudon@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 Baldrige | tim.baldrige@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 Loudon

Chris Loudon 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 Loudon

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 Loudon

Chris Loudon 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 Loudon 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 |

Federal Public Key Infrastructure Technical Working Group Meeting Minutes

Prepared for the General Services Administration
By Protiviti Government Services

**Wednesday
June 11, 2014**

1:00 p.m. – 2:30 p.m.

General Services Administration 1800 F Street Northwest Washington, DC

| | | |
|------|---------------------------------|------------------|
| 1:00 | Welcome & Opening Remarks | Chris Loudon |
| 1:05 | Ozone Server PDVAL Report | Kenneth Myers |
| 1:15 | FPKI CDN Project | Giuseppe Cimmino |
| 2:25 | Wrap-up and Adjourn the Meeting | Chris Loudon |

FPKI TWG June 11, 2014 Meeting Minutes

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or not identified their organization.

| Name | Organization |
|--------------------|------------------|
| Ambs, Matthew | DHS |
| Baldrige, Tim | DoD |
| Ball, Mike | Electrosoft |
| Barry, Jeff | Certipath |
| Blanchard, Deborah | Verizon Business |
| Bolin, Neil | Certipath |
| Boss, Daniel | USDA |
| Brown, Wendy | FPKIMA |
| Burke, James | DoJ |
| Camat, Aldrich | DHS |
| Carson, Mike | Telos |
| Chokhani, Santosh | DoD |
| Cimmino, Giuseppe | FPKIMA |
| Cunningham, Robert | VA |
| Davies, Jim | DHS |
| Diduro, John | FPKIMA |
| Disiena, Ridley | NASA |
| Erickson, Shari | USDA |
| Evans, Paul | DoE |
| Gerhard, Andrew | Verizon Business |
| Gray, Michael | Education |
| Hai Ja, Curtis | Transportation |
| Hannan, John | GPO |
| Head, Derrek | State |
| Jackson, Angela | USPS |
| Jeffers, Daniel | DoD |
| Jarboe, Jeff | State |
| Johnson, Todd | Treasury |
| Kandela, Savith | FPKIMA |
| Kluegel, Lynn | DoE |
| LeVan, LeChell | DHS |
| Louden, Chris | FPKIMA |

FPKI TWG June 11, 2014 Meeting Minutes

| | |
|-----------------------|------------------|
| McBride, Terry | Treasury |
| McCloud, Dennis | HHS |
| Morrison, Scott | DoJ |
| Myers, Kenneth | FPKIMA |
| Page, Ryan | PM-ISE |
| Race, Steve | TSCP |
| Salgado, John | DoD |
| Sambit, Dash | Symantec |
| Shorter, Scott | Electrosoft |
| Skordinski, Steve | TSCP |
| Slusher, Toby | HHS |
| Smith, Thomas | John Hopkins APL |
| Spainhour, Ben | DoD |
| Spence, Willie | Treasury, IRS |
| Stone, Wayne | NASA |
| Talley, Janet | FAA |
| Thakkar, Jay | DoD |
| Thomas, Michele | USDA |
| Townsend, Paul | Mount Airey |
| Walker, Dave | DHS |
| Wallace, Carl | DHS |
| Ward, Keith | TSCP |
| Wasserman, Jamie | SSA |
| Weiser, Russ | Verizon Business |
| Woods, Dan | Treasury |
| Woodford, Christopher | Treasury |
| Wyatt, Terry | NASA |
| Zeimat, Adam | USDA |

Agenda Item 1 - Welcome and Opening remarks (Chris Loudon)

The FPKI TWG met at GSA, 1800 F Street Northwest, Washington, DC. Mr. Chris Loudon (Supporting FPKIMA) opened the meeting by thanking everyone for attending and stated that Ms. Darlene Gore would not be able to attend due to a sudden conflict. He reviewed the agenda and then introduced Mr. Kenneth Myers (Supporting FPKIMA) to present the Ozone Server PDVAL report.

Agenda Item 2 - Mount Airey Ozone Server PDVAL Report (Kenneth Myers)

Mr. Myers opened the topic by introducing the report and then introduced Mr. Paul Townsend from Mount Airey. Mr. Townsend started with a functional description of the Ozone Server. It operates by acting as a verification plug-in to an application. It makes a verification decision based on the certificate asserted from the user against a set of proofs created from an authoritative source designated by the Server. The proof can be either static or dynamic and is delivered to the Ozone Server which makes a verification decision. The decision is asserted to the application to allow access based on the presented credential. One unidentified caller asked if the Ozone Server will be deployed as publicly accessible. Chris Loudon responded no, the FPKIMA tests commercial product capabilities against NIST PKITS guidelines to create a list of approved products to be used in the FPKI. It is up to the individual agencies to contact the company and obtain a service contract for use. Mr. Myers concluded the topic with the test results. The Ozone Server passed all required and optional tests except for one issue in the optional name constraints tests. In these tests, an error message created stated the error was with the subject alternative name even when the subject alternative name wasn't what violated the name constraints. The optional test criteria only test for the appropriate result and not the error message. In all tests, the Ozone Server successfully returned the appropriate response. No comments or concerns were raised by those in attendance. The next step is to forward the report and validation report to the FPKIPA Chair and then add the product to the PDVAL Product List.

Mr. Myers introduced Mr. Giuseppe Cimmino (Supporting FPKIMA) to present a brief and discussion on the FPKI Content Delivery Network Project

ACTIONS:

1. An FPKIPA approval letter will be drafted and sent to the FPKIPA Chair, Deborah Gallagher, for signature and acceptance into the FPKI PDVAL Product List.

Agenda Item 3 – FPKI CDN Project (Giuseppe Cimmino)

Mr. Cimmino opened the topic with a brief introduction of general CDN operations. He explained the concept of origin and edge servers and also the general performance and security enhancements possible with a CDN. He then moved onto the detailed technical brief of the FPKI CDN Project. Currently, the FPKI CRLs are hosted from an HTTP

repository with two static IP addresses. The project proposes to transition the HTTP capability of the FPKIMA repository to a CDN for performance and security enhancements. Mr. Cimmino outlined the three options that are currently being considered being (1) a full move to CDN, (2) a limited CDN option with a block of IPs for those Entities with tight egress controls and (3) a hybrid option combining both a CDN option and retaining the current HTTP repository for those Entities that cannot support the dynamic nature of a CDN.

An unidentified caller asked if there was a plan for stale content on CDN. Mr. Cimmino responded the CRLs are published twice a day and the FPKIMA is looking at future enhancements to the HTTP cache headers to guarantee a system that cached the content could determine if the data is up to date based on the content of the CRL. CDNs are used today for CRL and OCSP delivery by both government and commercial PKIs. If an emergency CRL is needed, the FPKIMA can push it to the CDN which can flush the outdated content on their network in a magnitude of minutes. Cache flushing is a well-known requirement and well supported by commercial CDN vendors.

There was a question if the CDN would service HTTPS. The FPKIMA does not serve over HTTPS today because the content is already digitally signed.

Todd Johnson (Treasury) asked how many edge servers would be located outside the US because there might be the potential for traffic analysis. If a CONUS based users hits an OCONUS server someone could analyze what traffic is hitting which server for authentication methods and use it for advanced targeting. Mr. Cimmino responded CDNs have different "maps" and we can choose which ones we want. The issue there is two-sided. Traffic analysis could be done on OCONUS origin servers as well. Whether CONUS traffic would ever be sent OCONUS in the case of all US servers being unavailable is an interesting edge condition and we can ask the vendor if this has come up and if we can require a geo-based map to the same region i.e. CONUS to CONUS.

In response to a question whether the CDN would support DNSSEC, we would support DNSSEC from the root though .gov to fpki.gov, but we didn't find CDN vendors who did dynamic signing. We would support DNSSEC up to the return of the CName to the CDN. The follow-up question was whether this would be a violation of the requirement to support DNSSEC for government systems. There are a number of government systems using CDNs today, the White House being one of them, but this is something the FPKIMA will investigate further.

Matt Ambs (DHS) asked if the hybrid approach is used would the dual existing HTTP servers exist indefinitely. Mr. Cimmino responded they would exist as long as they are needed. The FPKIMA would continue to support the current setup because regardless of the CDN option, the FPKI's HTTP server would always be needed to be the origin server for the CDN.

There was a contracting question about the decision to use Akamai. This isn't a contracting discussion; this is a technical discussion on Entities ability to configure their systems to use a CDN.

There was a question how to support an agency that is using DNS resolution provided through another provider, like openDNS or a commercial vendor. If that agency also has strict egress controls, the limited map option is the only option. The limited option, meaning a limited set of IPs is used in the CDN. This is a specific issue with the Federal Reserve Board (FRB), but may apply to other entities with strict egress and outbound traffic firewall policies. Todd Johnson (Treasury) asked the FRB representative to get with him offline as it might be a Treasury only issue. Giuseppe remarked that the FRB currently uses a limited map configuration of the Akamai CDN through their current vendor, Symantec.

Jim Davies (DHS OneNet) asked if there is any advice on configuring non-proxy aware devices. A non-proxy aware device is a service where the application doesn't know there is a proxy http service. The Proxy service usually provides a many to one relationship, the CDN would create many-to-many relationships. This might be solved with a rule that bypasses the proxy service for given content such as p7c files and CRLs. Could do rules based on content for CRLs. Would the proxy allow access to the edge server from the domain resolvers? Mr. Cimmino responded adding a CDN shouldn't impact whether you're using a proxy or not. Mr. Cimmino said he would set up a separate call with DHS to fully understand and resolve this question.

Dave Walker asked if there is a technical document we can take a look at it for our network engineers? Mr. Cimmino responded there is the presentation that was sent out in the meeting announcement and the intro presentation that was also presented to the FPKIPA. Mr. Cimmino will send both presentations to the participants if they send their emails. Once the CDN options are approved, details will be distributed to the community. Agreements will be sent to those with egress controls to properly set up access to ensure operational continuity. The FPKIMA will also send out implementation time lines after approval, but there isn't a firm date of when an option will be decided.

ACTIONS:

1. Follow-up with Akamai on geo-based traffic analysis for advanced targeting.
2. Research DNSSEC support on CDNs.
3. Set-up call with DHS to discuss non-proxy aware devices and CDNs.
4. Send any additional questions/concerns to giuseppe.cimmino@protiviti.com
5. Distribute presentations to participants who send their contact information.
6. Distribute technical documents and option descriptions to participants after FPKIPA approval is complete.

Agenda Item 4 - Wrap-up and Adjourn Meeting (Chris Loudon)

Mr. Loudon thanked everyone for attending and adjourned the TWG meeting at approximately 2:00 PM EST.



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 Loudon |
| 9:50 | FPKI Affiliate Test Environment | Wendy Brown |
| 11:00 | High-level Strategies for Transition Planning | Chris Loudon |
| 12:00 | Lunch | All |
| 1:00 | Time Stamping with Code Signing Signature | Matt Kotraba/ Wendy Brown |
| 2:30 | Open Discussion of New Issues | Chris Loudon |
| 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 Loudon | chris.loudon@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 Loudon 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 Loudon

Chris Loudon 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 Loudon

Chris Loudon 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 Loudon

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

- a. **FPKI Issues Tracking**: Chris Loudon 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 ECU for Claim Signers**: Chris Loudon introduced a proposal for a new ECU 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 ECUs. The issuance of Personal Identity Verification (PIV) and PIV-Interoperable (PIV-I) certificates introduced the need for a certificate ECU to assert a signer of PIV and PIV-I attributes. Individual single purpose ECUs, PIV Signer and PIV-I Signer were established to meet this requirement rather than establishing a single ECU to cover any claim signer. FICAM initiatives are introducing attribute signers that will require an ECU to assert attribute claims about entities. The Claim Signer ECU could be used for these attribute signers. The FPKI TWG members agreed with this proposal and believe it will help provide a universal ECU for all future claim signers.

Adjourn Meeting
Chris Loudon

Chris Loudon 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 |