



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.