FPKIPA
Federal Public Key Infrastructure Policy Authority

MEMORANDUM FOR FEDERAL AGENCY LEGACY PKIs

SUBJECT: Implementing HSPD-12 using Legacy PKI certificates

Section 5.4.4 of FIPS 201 states: “Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)”

In order to facilitate Federal Legacy PKI compliance with this requirement, the Common Policy has been modified to include provisions that exclusively pertain to the Federal Legacy PKIs. By adding language pertaining to naming conventions and off-line root CAs, the main obstacles to compliance with the Common Policy by Federal Legacy PKI agencies have been removed. This should enable the Federal Legacy PKI agencies to express Common Policy OIDs in the PIV Authentication Certificates, as is required to meet the requirements of FIPS 201 (additional certificates for signing and key management can continue to only assert agency OIDs). However, those agencies planning to take advantage of this new language must ensure that they implement their certificates in a manner consistent with other provisions in the Common Policy. A Federal Legacy PKI will be deemed to be issuing PIV Authentication certificates in conformance with the Common Policy if it issues those certificates in accordance with the requirements of a certificate policy that has been mapped to the FBCA CP at the Medium Hardware or High assurance level and in accordance with the following additional provisions that affect certificate issuance:

- Identity proofing requirements (FIPS 201 Section 2)

- 18 hour CRL requirement (FIPS 201 Section 5.4.3) and the requirement to populate the nextUpdate field in CRLs as specified in the Common Policy, section 4.9.7.

- OCSP Requirement (FIPS 201 Sections 5.3 and 5.4)

- Requirement to issue the certificates in conformance with Worksheet 9 of the *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP)* Program [SSP-PROF] (FIPS 201 Section 5.4.2.1).

- Requirement not to post PIV Authentication certificates to a public directory. (FIPS 201 Section 5.4.5.1)

- Requirement to make directory information available via LDAP and HTTP. (FIPS 201 Section 5.4.5.1

Peter Alterman, Ph.D.
Chair