Federal Public Key Infrastructure Policy Authority
10401 Fernwood Road, Rm. 3F16
Bethesda, MD 20892

TO: Federal PKI Policy Authority Cross-Certified Federal Agencies

FROM: Dr. Peter Alterman, Chair

SUBJECT: Medium Hardware Policy

DATE: September 12, 2006

Issue:
Updating Federal Agency certificate policies to permit differentiation of subscriber certificates deployed on hardware tokens and conforming to Federal Bridge Medium Assurance certificate policy so that they conform to the Federal Bridge Medium Assurance Hardware certificate policy.

Background
The Federal Bridge Certificate Policy was reformatted to comply with RFC3647 and accepted by the Policy Authority on September 13, 2005. In addition to reformatting the Certificate Policy, several specific changes were included to better align the policy with other government-wide initiatives, most notably E-Authentication and HSPD12. Specifically, a new policy level and corresponding OID was added to the four previously existing policies. This new policy OID allows differentiation between medium assurance credentials deployed in software and medium assurance credentials deployed on hardware tokens. This distinction is required to differentiate between medium assurance credentials as they apply to E-Authentication Assurance Levels 3 and 4.

In addition, HSPD-12 requires the use of hardware tokens and digital credentials that meet the Federal Common Policy Framework. OMB-05-24 stipulates that agency deployed credentials cross certified with the Federal Bridge Certification Authority (FBCA) at Medium Assurance or higher meet this requirement. The challenge for these credentials is that they identify themselves as Hardware-based. Certificates conforming to Federal Bridge High Assurance are hardware-based by definition, whereas those conforming to Medium Assurance require a unique policy OID to make the distinction between software- and hardware-based credentials; this new policy OID should comply with Federal Bridge Medium Hardware.

Recommendation:
1. Federal agencies cross-certified with the FBCA take immediate steps to revise their certificate polices to add a policy OID for credentials conforming to FBCA Medium Assurance that will be

deployed in hardware (e.g. FIPS 201-compliant smart cards). The agency certificate policy requirements for this new OID must conform to Federal Bridge Medium Hardware.

The following policy mapping requirements pertain specifically to Medium Hardware but not Medium Assurance:

- FBCA Section 6.1.1.2 Subscriber key generation must be performed using a hardware cryptographic module.

- FBCA Section 6.2.1 The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA	Subscriber	RA
Medium Hardware	Level 2 hardware	Level 2 hardware	Level 2 hardware

- FBCA Section 6.2.4.2 Subscriber private signature keys may not be backed up or copied

The following pertains to Medium Assurance but NOT to Medium Hardware:

- Section 6.1.7 Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP.

2. Submit revised policy, with changes highlighted, to the FPKIPA for review and approval.

3. FBCA and Agency officials reissue cross certificates to include the new policy mappings.

4. Federal agencies should complete this update no later than October 27, 2007.

Action:
Federal Agencies cross certified with the FBCA respond to the Chair, Federal PKI Policy Authority concerning plans to add a policy OID for hardware-based certificates conforming to FBCA Medium Hardware and the timeframes for completion.