

## TECHNICAL (PKI)

### **1. Are there standards by which PKI Shared Service Providers must comply regarding RA/CA communication and key escrow?**

PKI Shared Service Providers must comply with the Federal Common Policy Framework which details requirements for PKI operations.

(<http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf>)

### **2. What is the relationship of a Device CA to the PIV trust model?**

Device authentication is outside the scope of the Personal Identity Verification (PIV) program objectives. However, provisions have been made in the Federal Common Policy Framework for device certificates and agencies are encouraged to issue under this policy if interoperability with other Federal organizations is desired. (Ref: [X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework](#))

### **3. FIPS-201, Section 5.4.2 states: "All certificates issued to support PIV Card authentication shall be issued under the Common Policy". Does this statement refer to all PIV-defined keys and their corresponding certificates?**

Yes. The intent of this statement is that all certificates in the PIV data model shall be issued under the Common Policy.

### **4. Some of the specified ECC algorithms are patented by CertiCom and the Department of Defense has a licensing agreement for the use of patents in software development. What is the scope of this agreement for use implementing HSPD-12?**

NSA has licensed the rights to 26 patents held by CertiCom Inc. covering a variety of elliptic curve (EC) technology. Under the license, NSA has a right to sublicense vendors building equipment or components in support of US national security interests. The NSA will not grant sublicenses to vendors who intend to sell their equipment for use in other areas such as the entertainment industry or general corporate security. These are not considered national security applications and are not eligible for the sublicense. To determine if the use of patented EC technology qualifies for a sublicense as a U.S. national security interest, contact the Business Affairs Office of the NSA/CSS Commercial Solutions Center. (Ref: <http://www.nsa.gov/ia/industry/cep.cfm>. Vendors may also contact CertiCom directly to inquire about the NSA sublicense: <http://www.certicom.com>).

### **5. Both X.509v3 CRLs and OCSP are mandatory certificate status mechanisms. Under what circumstances would one status mechanism be preferred over the other or should both be used concurrently for all credential validation?**

It is mandatory for PKI Service Providers to make X.509v3 CRLs and OCSP responses available to relying parties. However, there is no scenario where a relying party is expected to check both the CRL and request status from an OCSP server. The relying party determines which status mechanism to use, based on the resources that are available in its environment. We might expect a physical access system for visitors to rely on OCSP responses, while an intra-agency application might function more efficiently using CRLs. Application developers may select the appropriate mechanism.

### **6. The FPKI Common Policy limits CA keys to a 6 year lifetime. Subscriber keys are limited to a maximum of half that (3 years). FIPS 201 allows credentials to be valid for up to 5 years. Given these facts, 5-year cards will require maintenance during their lifecycle (PIV certificate reissuance). Is this correct?**

This is correct. To use a PIV card for the maximum five years, new PKI credentials will need to be obtained at the three year point. This is a security feature, as well as mitigating the risk of large CRLs. There are currently no plans to modify either FIPS 201 or the Common Policy. Technically,

certificate renewal can be performed by the user from the desktop, or the agency may choose to re-issue smart cards every three years and align it with the PKI certificate issuance cycle.

**7. Since legacy PKIs will initially be issuing PIV certificates that do not assert the Common-Authentication policy object identifier (OID), do they need begin operating an On-line Certificate Status Protocol (OCSP) server as soon as they begin issuing PIV certificates, or can they wait until they begin issuing PIV certificates that include the Common-Authentication policy OID?**

A legacy PKI issuing PIV certificates needs to implement an OCSP server by January 1, 2008 or when the agency begins issuing certificates that assert the Common-Authentication policy OID, since these certificates must include the URL of the authoritative OCSP server.

**8. Is more than one certificate permitted to be bound to the same public key?**

No. Each public key in the PIV data model has only one certificate binding.