**FPKIPA
Federal Public Key Infrastructure Policy Authority
**

**X.509 Certificate Policy**

**For The**

**U.S. Federal PKI**

**Common Policy Framework**

Version 3647 - 1.17

December 13, 2011

**Signature Page**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chair, Federal Public Key Infrastructure Policy Authority DATE

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Document Version** | **Document Date** | **Revision Details** |
| 1.0 | May 7, 2007 | Revised Common Policy (RFC 3647 format) |
| 1.1 | July 17, 2007 | Alignment of Cryptographic Algorithm Requirements with SP 800-78-1 |

Table of Contents

[1. Introduction 1](#_Toc154126086)

[1.1 Overview 2](#_Toc154126087)

[1.1.1. Certificate Policy (CP) 2](#_Toc154126088)

[2. Publication and Repository Responsibilities 2](#_Toc154126089)

[2.1. Repositories 2](#_Toc154126090)

[2.2. Publication of Certification Information 2](#_Toc154126091)

[2.2.1. Publication of Certificates and Certificate Status 2](#_Toc154126092)

# Introduction

This certificate policy (CP) includes seven distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a high assurance user policy, a user authentication policy, and a card authentication policy. In this document, the term “device” means a non-person entity, i.e., a hardware device or software application. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all seven policies.

The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. However, there are some applications in use within the federal government that cannot process certificates or certificate revocation information signed using SHA-256. Therefore this CP also includes five additional distinct certificate policies which indicate the use of the deprecated SHA-1 after December 31, 2010. These id-fpki-sha1 policies adhere to all the requirements of the associated id-common policy with the exception that the certificate is generated with a SHA-1 signature and the issuing CA may use SHA-1 for generation of PKI objects such as CRLs and OCSP responses until December 31, 2013. It should be noted that certificates issued on or after January 1, 2011 are not FIPS 201 compliant, and therefore do not meet the requirements of HSPD-12. CAs that issue SHA-1 certificates after December 31, 2010 may not also issue FIPS 201 compliant certificates.

The user policies apply to certificates issued to Federal employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support access to Federal systems that have not been designated national security systems.

A PKI that uses this CP will provide the following security management services:

* Key generation/storage
* Certificate generation, modification, re-key, and distribution
* Certificate revocation list (CRL) generation and distribution
* Directory management of certificate related items
* This is a sub-bullet in a list
* Certificate token initialization/programming/management
* System management functions (e.g., security audit, configuration management, archive.)

The user policies require Federal employees, contractors, and other affiliated personnel to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. The device policy also requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

This policy does not presume any particular PKI architecture. The policy may be implemented through a hierarchical PKI, mesh PKI, or a single certification authority (CA). Any CA that asserts this policy in certificates must obtain prior approval from the Federal PKI Policy Authority. CAs that issue certificates under this policy may operate simultaneously under other policies. Such CAs must not assert the OIDs in this policy in certificates unless they are issued in accordance with all the requirements of this policy.

This policy establishes requirements for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that chose to distribute self-signed certificates, such as a hierarchical PKI’s root CA.

This CP is consistent with request for comments (RFC) 3647, the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

## 1.1 Overview

### Certificate Policy (CP)

Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. This CP applies only to CAs owned by or operated on behalf of the Federal government that issue certificates according to this policy.

# Publication and Repository Responsibilities

## Repositories

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. Specific requirements are found in *Shared Service Provider Repository Service Requirements* [SSP REP]. CAs may optionally post subscriber certificates in this repository in accordance with agency policy, except as noted in section 9.4.3. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other parties (e.g., Federal agencies).

## Publication of Certification Information

### Publication of Certificates and Certificate Status

The publicly accessible repository system shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually. Where applicable, the certificate status server (CSS) shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.