Test Certificate Policy to Support PKI Pilots and Testing

1 Introduction

This Certificate Policy (CP) defines certificate policies to facilitate testing of public key cryptography and public key infrastructures.

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

The United States Government disclaims any liability that may arise from the use of this CP.

1.1 Overview

This policy pertains to certificates issued for testing and evaluation ONLY.

1.2 Document name and identification

This policy is associated with the following 256 object identifiers:

- - test policy arc

```
csor-test-policies OBJECT IDENTIFIER ::= { 2 16 840 1 101 3 2 1 48 }
```

- - test policy OIDs

```
test1   OBJECT IDENTIFIER ::= { csor-test-policies 1   }
test2   OBJECT IDENTIFIER ::= { csor-test-policies 2   }
test3   OBJECT IDENTIFIER ::= { csor-test-policies 3   }
test4   OBJECT IDENTIFIER ::= { csor-test-policies 4   }
test5   OBJECT IDENTIFIER ::= { csor-test-policies 5   }
test6   OBJECT IDENTIFIER ::= { csor-test-policies 6   }
test7   OBJECT IDENTIFIER ::= { csor-test-policies 7   }
test8   OBJECT IDENTIFIER ::= { csor-test-policies 8   }
test9   OBJECT IDENTIFIER ::= { csor-test-policies 9   }
test10  OBJECT IDENTIFIER ::= { csor-test-policies 10  }
...
test256 OBJECT IDENTIFIER ::= { csor-test-policies 256 }
```

A CA may assert any of the 256 OIDs above in the certificate policies extension of a public key certificate. When present in the certificate policies extension, each of these OIDs indicates that the stipulations contained in this policy were enforced in the issuance of that certificate, and will continue to be enforced in the maintenance of certificate status information.

1.3 PKI participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this policy should be used for testing purposes ONLY.

1.4.2 Prohibited certificate uses

This CP does not guarantee any particular level of assurance. These certificates should not be used to implement security for real-world applications.

1.5 Policy administration

1.5.1 Organization administering the document

The NIST CSOR registrar is responsible for all aspects of this CP.

1.5.2 Contact person

Questions regarding this CP shall be directed to the NIST CSOR registrar via electronic mail at <csor@nist.gov>.

1.5.3 Person determining CPS suitability for the policy

This CP may be used without a CPS.

1.5.4 CPS approval procedures

No stipulation.

2 Publication and repository responsibilities

No stipulation.

3 Identification and authentication

No stipulation.

4 Certificate life-cycle operational requirements

No stipulation.

5 Facility, management, and operational controls

No stipulation.

6 Technical security controls

No stipulation.

7 Certificate, CRL, and OCSP profiles

No stipulation.

8 Compliance audit and other assessments

No stipulation.

9 Other business and legal matters

No stipulation.

9.1 Fees

No stipulation.

9.2 Financial responsibility

No stipulation.

9.3 Confidentiality of business information

No stipulation.

9.4 Privacy of personal information

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

The United States Government disclaims any liability that may arise from use of any certificate issued by any CA that asserts this policy through the OIDs specified in Section 1.2.

9.9 Indemnities

No stipulation.

9.10 Term and termination

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.17 Other provisions

No stipulation.

References

[RFC 3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet X.509 public key infrastructure certificate policy and certification practices framework, November 2003.