Internet Engineering Task Force (IETF)
Request for Comments: 7229
Category: Informational
ISSN: 2070-1721

R. Housley
Vigil Security

May 2014

Object Identifiers for Test Certificate Policies

Abstract

This document provides several certificate policy identifiers for testing certificate handling software.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7229.

1. Introduction

This document provides several certificate policy identifiers for testing certificate handling software. These certificate policy identifiers are not intended for use in the public Internet.

The certificate policy identifiers provided in this document are consistent with the certificate profile specified in [RFC5280]. They are appropriate for testing the certificate policy processing, especially the handling of the certificate policy extension, the policy constraints extension, and the policy mapping extension.

2. Certificate Policy Identifiers for Testing

The following certificate policy identifiers are provided for testing certificate handling software. ASN.1 [ASN1-2008] object identifiers are used to name certificate policies.

```
id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
            dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-TEST OBJECT IDENTIFIER ::= { id-pkix 13 }

-- Object Identifiers used ONLY for TESTING
id-TEST-certPolicyOne       OBJECT IDENTIFIER ::= { id-TEST 1 }
id-TEST-certPolicyTwo       OBJECT IDENTIFIER ::= { id-TEST 2 }
id-TEST-certPolicyThree     OBJECT IDENTIFIER ::= { id-TEST 3 }
id-TEST-certPolicyFour      OBJECT IDENTIFIER ::= { id-TEST 4 }
id-TEST-certPolicyFive      OBJECT IDENTIFIER ::= { id-TEST 5 }
id-TEST-certPolicySix       OBJECT IDENTIFIER ::= { id-TEST 6 }
id-TEST-certPolicySeven     OBJECT IDENTIFIER ::= { id-TEST 7 }
id-TEST-certPolicyEight     OBJECT IDENTIFIER ::= { id-TEST 8 }
```

3. Security Considerations

This specification does not identify particular certificate policies for use in the Internet public key infrastructure. The actual policies used for production certificates can have a significant impact on the confidence that one can place in the certificate. No confidence should be placed in any certificate that makes use of these certificate policy identifiers, since they are intended only for testing.

4. IANA Considerations

The object identifiers used in this document are defined in an arc delegated by IANA to the PKIX Working Group. No further action by IANA is necessary for this document or any anticipated updates.

5. Normative References

[ASN1-2008] International Telecommunications Union, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, November 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

Appendix A. ASN.1 Module

This appendix provides the certificate policy identifiers (object identifiers) in an ASN.1 module. No fancy structures are needed, so this module is compatible with [ASN1-2008].

```
PKIXTestCertPolicies { iso(1) identified-organization(3) dod(6)
   internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
   id-mod-TEST-certPolicies(83) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --
-- IMPORTS NONE --

id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
            dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-TEST OBJECT IDENTIFIER ::= { id-pkix 13 }

-- Object Identifiers used ONLY for TESTING
id-TEST-certPolicyOne       OBJECT IDENTIFIER ::= { id-TEST 1 }
id-TEST-certPolicyTwo       OBJECT IDENTIFIER ::= { id-TEST 2 }
id-TEST-certPolicyThree     OBJECT IDENTIFIER ::= { id-TEST 3 }
id-TEST-certPolicyFour      OBJECT IDENTIFIER ::= { id-TEST 4 }
id-TEST-certPolicyFive      OBJECT IDENTIFIER ::= { id-TEST 5 }
id-TEST-certPolicySix       OBJECT IDENTIFIER ::= { id-TEST 6 }
id-TEST-certPolicySeven     OBJECT IDENTIFIER ::= { id-TEST 7 }
id-TEST-certPolicyEight     OBJECT IDENTIFIER ::= { id-TEST 8 }

END
```

Author’s Address

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com