Network Working Group
Internet-Draft
Updates: 6487 (if approved)
Intended status: Standards Track
Expires: June 8, 2013

A. Newton
ARIN
G. Huston
APNIC

December 5, 2012

Policy Qualifiers in RPKI Certificates
draft-newton-sidr-policy-qualifiers-00

Abstract

This document updates RFC 6487 by clarifying the inclusion of policy qualifiers in the certificate policies extension of RPKI resource certificates.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 8, 2013.

Copyright Notice

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Update to RFC 6487

[RFC6487] profiles certificates, certificate revocation lists, and certificate signing requests specified in [RFC5280] for use in routing public key infrastructure.

[RFC5280] defines an extension to certificates for the listing of policy information (See section 4.2.1.4). [RFC6487] states in Section 4.8.9: "This extension MUST be present and MUST be marked critical. It MUST include exactly one policy, as specified in the RPKI CP [RFC6484]". This references the CertPolicyId of the sequence allowed in PolicyInformation as defined by [RFC5280].

[RFC5280] also specifies that PolicyInformation may optionally have a sequence of PolicyQualifierInfo objects. [RFC6487] does not specifically allow or disallow these PolicyQualifierInfo objects although it also states in section 4: "Unless specifically noted as being OPTIONAL, all the fields listed here MUST be present, and any other fields MUST NOT appear in a conforming resource certificate."

This document updates [RFC6487], Section 4.8.9, to explicitly allow optional PolicyQualifierInfo objects in the PolicyInformation specified by [RFC6487].

As noted in [RFC5280], section 4.2.1.4: "Optional qualifiers, which MAY be present, are not expected to change the definition of the policy." In this case any optional policy qualifiers that MAY be present in a resource certificate MUST NOT change the definition of the RPKI CP [RFC6484].

3. Acknowledgements

Frank Hill and Adam Guyot helped define the scope of this issue and identified and worked with RPKI validator implementers to clarify the use of policy qualifiers in resource certificates.

4. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, February 2012.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for

X.509 PKIX Resource Certificates", RFC 6487,
February 2012.

Authors' Addresses

Andrew Lee Newton
American Registry for Internet Numbers
3635 Concorde Parkway
Chantilly, VA 20151
US

Email: andy@arin.net
URI: http://www.arin.net

Geoff Huston
Asia Pacific Network Information Center
6 Cordelia Street
South Brisbane QLD 4101
Australia

Email: gih@apnic.net
URI: http://www.apnic.net