Internet Engineering Task Force (IETF)
Request for Comments: 7318
Updates: 6487
Category: Standards Track
ISSN: 2070-1721

A. Newton
ARIN
G. Huston
APNIC

July 2014

Policy Qualifiers in Resource Public Key Infrastructure (RPKI) Certificates

Abstract

This document updates RFC 6487 by clarifying the inclusion of policy qualifiers in the certificate policies extension of Resource Public Key Infrastructure (RPKI) resource certificates.

Status of This Memo

This is an Internet Standards Track document.

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). Further information on Internet Standards is available in 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/rfc7318.

Table of Contents

1. Introduction

This document introduces policy qualifiers in the certificate policies extension of the RPKI resource certificates. This document updates [RFC6487].

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 Section 4 also states: "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."

Because there is a need for some RPKI Certificate Authorities to include policy qualifiers in their certificates, this document updates Section 4.8.9 of [RFC6487] as follows:

OLD:

> This extension MUST be present and MUST be marked critical. It MUST include exactly one policy, as specified in the RPKI Certificate Policy (CP) [RFC6484].

NEW:

> This extension MUST be present and MUST be marked critical. It MUST include exactly one policy, as specified in the RPKI CP [RFC6484]. Exactly one policy qualifier MAY be included. If a policy qualifier is included, the policyQualifierId MUST be the Certification Practice Statement (CPS) pointer qualifier type (id-qt-cps).

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 qualifier that MAY be present in a resource certificate MUST NOT change the definition of the RPKI CP [RFC6484].

3. Security Considerations

The Security Considerations of [RFC6487] apply to this document.

This document updates the RPKI certificate profile to specify that the certificate policies extension can include a policy qualifier, which is a URI. While dereferencing the URI is not required for certificate validation, doing so could provide a denial-of-service (DoS) vector, where the target host may be subjected to bogus work dereferencing the URI. However, this specification, like [RFC5280], places no processing requirements on the URI included in the qualifier.

As an update to [RFC6487], this document broadens the class of certificates that conform to the RPKI profile by explicitly including within the profile those certificates that contain a policy qualifier as described here. A relying party that performs a strict validation based on [RFC6487] and fails to support the updates described in this document would incorrectly invalidate RPKI objects that include the changes in Section 2.

4. Acknowledgments

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

Sean Turner provided significant text to this document regarding the processing of the CPS URI and limiting the scope of the allowable content of the policy qualifier.

5. 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
USA

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