Internet Engineering Task Force
Internet-Draft
Updates: 6485 (if approved)
Intended status: Standards Track
Expires: July 5, 2014

G. Michaelson, Ed.
G. Huston
APNIC

January 2014

Clarifying RPKI use of CMS SignerInfo" draft-michaelson-signerinfo-01

Abstract

RFC6485 section 2 mandated a single CMS OID sha256withRSAEncryption from RFC4055 for use in the CMS SignerInfo field. This draft updates RFC6485 and extends it to permit the correct CMS use which includes an option of rsaEncryption for the SignerInfo field.

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 July 5, 2014.

Table of Contents

1. Introduction

RFC 6485 [RFC6485] defines The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI). In that document, Section 2 specifies a single signature algorithm (SHA-256) and a single CMS OID, sha256withRSAEncryption, to be used for the SignerInfo field of the CMS object.

A closer reading of the relevant RFCs RFC 4055 [RFC4055] and RFC 5754 [RFC5754] identified that the CMS SignerInfo field must support use of the rsaEncryption OID for full conformance with the CMS specifications, and the normative references in RFC 6485 inherit the requirement.

To ensure full conformance with the CMS specifications, RFC 6485 is updated by this draft. All of RFC 6485 applies except for a change to the SignerInfo field.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Revised CMS SignerInfo

In RFC 6485 Section 2 the following sentence:

> The Object Identifier (OID) sha256withRSAEncryption from [RFC4055] MUST be used.

Is replaced by:

> One of the Object Identifiers (OID) rsaEncryption or sha256WithRSAEncryption from [RFC4055] MUST be used. RPKI implementations MUST support rsaEncryption for the signatureAlgorithm field and SHOULD support sha256WithRSAEncryption.

3. Current Systems Behaviour

All known RPKI CA implementations already do what this draft recommends.

4. Acknowledgements

Andrew Chi and David Mandelberg discovered this problem.

Russ Housley documented the RFC chain back to 2630.

This draft reflects a discussion between Rob Austein and Matt Lepinski on the SIDR Working group mailing list and a private communication between Rob Austein and Geoff Huston.

5. IANA Considerations

This memo includes no request to IANA.

6. Security Considerations

By conforming more closely to the CMS specifications, RPKI CMS objects are less likely to be rejected as non-conformant with the standards. No change is made to the cryptographic status of the CMS objects produced.

7. References

7.1. Normative References

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

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

[RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", RFC 5754, January 2010.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)", RFC 6485, February 2012.

7.2. Informative References

[AUSTEIN] Austein, SR., "RFC 6485 is inconsistent with base CMS specifications", 2012, <http://www.ietf.org/mail-archive/web/sidr/current/msg04813.html>.

Authors' Addresses

George Michaelson (editor)
APNIC
6 Cordelia St, South Brisbane
Brisbane, Queensland 4101
AU

Phone: +61 7 3858 3150
Email: ggm@apnic.net

Geoff Huston
APNIC

Email: gih@apnic.net