

SIDR
Internet-Draft
Obsoletes: [6485](#) (if approved)
Intended status: Standards Track
Expires: November 16, 2015

G. Huston
G. Michaelson, Ed.
APNIC
May 15, 2015

The Profile for Algorithms and Key Sizes for use in the Resource Public
Key Infrastructure
[draft-ietf-sidr-rfc6485bis-02.txt](#)

Abstract

This document specifies the algorithms, algorithms' parameters, asymmetric key formats, asymmetric key size and signature format for the Resource Public Key Infrastructure subscribers that generate digital signatures on certificates, Certificate Revocation Lists, and signed objects as well as for the Relying Parties that verify these digital signatures.

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 November 16, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

This document specifies:

- * the digital signature algorithm and parameters;
- * the hash algorithm and parameters;
- * the public and private key formats; and,
- * the signature format

used by Resource Public Key Infrastructure (RPKI) subscribers when they apply digital signatures to certificates, Certificate Revocation Lists (CRLs), and signed objects (e.g., Route Origin Authorizations (ROAs) and manifests). Relying Parties (RPs) also use this document when verify RPKI subscribers' digital signatures [[RFC6480](#)].

This document is referenced by other RPKI profiles and specifications, including the RPKI Certificate Policy (CP) [[RFC6484](#)], the RPKI Certificate Profile [[RFC6487](#)], the SIDR Architecture [[RFC6480](#)], and the Signed Object Template for the RPKI [[RFC2119](#)]. Familiarity with these documents is assumed.

1.1. 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. Algorithms

Two cryptographic algorithms are used in the RPKI:

- * The signature algorithm used in certificates, CRLs, and signed objects is RSA Public-Key Cryptography Standards (PKCS) #1 Version 1.5 (sometimes referred to as "RSASSA-PKCS1-v1_5") from [Section 5 of \[RFC4055\]](#).
- * The hashing algorithm used in certificates, CRLs, and signed objects is SHA-256 [[SHS](#)] (see note below). Hashing algorithms

are not identified individually in certificates and CRLs, as the identity of the hashing algorithm is combined with the identity of the digital signature algorithm.

When used in the context of the Cryptographic Message Syntax

(CMS) SignedData, the hashing algorithm is identified individually (in this case the hashing algorithm is sometimes called a message digest algorithm).

NOTE: The exception to the above hashing algorithm use is the use of SHA-1 [[SHS](#)] when CAs generate authority and subject key identifiers [[RFC6487](#)].

For generating and verifying certificates and CRLs the hashing and digital signature algorithms are referred to together, i.e., "RSA PKCS#1 v1.5 with SHA-256" or more simply "RSA with SHA-256". The Object Identifier (OID) sha256WithRSAEncryption from [[RFC4055](#)] MUST be used in this case.

For CMS SignedData, the object identifier and parameters for SHA-256 in [[RFC5754](#)] MUST be used for the SignedData digestAlgorithms field and the SignerInfo digestAlgorithm field when generating and verifying CMS SignedData objects. The object identifier and parameters for rsaEncryption MUST be used for the SignerInfo signatureAlgorithm field when generating CMS SignedData objects. RPKI implementations MUST accept CMS SignedData objects that use the object identifier and parameters for either rsaEncryption or sha256WithRSAEncryption for the SignerInfo signatureAlgorithm field when verifying CMS SignedData objects.

Locations for this OID are as follows:

In the certificate, the OID appears in the signature and signatureAlgorithm fields [[RFC4055](#)];

In the CRL, the OID appears in the signatureAlgorithm field [[RFC4055](#)];

In CMS SignedData, the OID appears in each SignerInfo signatureAlgorithm field, the SignerInfo digestAlgorithm field,

and in the SignedData digestAlgorithms [[RFC5652](#)]; and,

In a certification request, the OID appears in the PKCS #10 signatureAlgorithm field [[RFC2986](#)], or in the Certificate Request Message Format (CRMF) POPOSigningKey signature field [[RFC4211](#)].

[3.](#) Asymmetric Key Pair Formats

The RSA key pairs used to compute the signatures MUST have a 2048-bit modulus and a public exponent (e) of 65,537.

Huston & Michaelson Expires November 16, 2015 [Page 3]

Internet-Draft RPKI Algorithm Profile May 2015

[3.1.](#) Public Key Format

The Subject's public key is included in subjectPublicKeyInfo [[RFC5280](#)]. It has two sub-fields: algorithm and subjectPublicKey. The values for the structures and their sub-structures follow:

algorithm (which is an AlgorithmIdentifier type):

The object identifier for RSA PKCS#1 v1.5 with SHA-256 MUST be used in the algorithm field, as specified in [Section 5 of \[RFC4055\]](#). The value for the associated parameters from that clause MUST also be used for the parameters field.

subjectPublicKey:

RSAPublicKey MUST be used to encode the certificate's subjectPublicKey field, as specified in [[RFC4055](#)].

[3.2.](#) Private Key Format

Local Policy determines private key format.

[4.](#) Signature Format

The structure for the certificate's signature field is as specified in [Section 1.2 of \[RFC4055\]](#). The structure for the Cryptographic Message Syntax (CMS) SignedData's signature field is as specified in [[RFC5652](#)].

5. Additional Requirements

It is anticipated that the RPKI will require the adoption of updated key sizes and a different set of signature and hash algorithms over time, in order to maintain an acceptable level of cryptographic security to protect the integrity of signed products in the RPKI. This profile should be relaxed to specify such future requirements, as and when appropriate.

Certification Authorities (CAs) and RPs SHOULD be capable of supporting a transition to allow for the phased introduction of additional encryption algorithms and key specifications, and also accommodate the orderly deprecation of previously specified algorithms and keys. Accordingly, CAs and RPs SHOULD be capable of supporting multiple RPKI algorithm and key profiles simultaneously within the scope of such anticipated transitions. The recommended procedures to implement such a transition of key sizes and algorithms is not specified in this document.

6. Security Considerations

The Security Considerations of [[RFC4055](#)], [[RFC5280](#)], and [[RFC6487](#)] apply to certificate and CRLs. The Security Considerations of [[RFC5754](#)] apply to signed objects. No new security are introduced as a result of this specification.

7. IANA Considerations

[Remove before publication. There are no IANA considerations in this document.]

8. Changes Aplied to [RFC6485](#)

This document represents a slight technical change to [[RFC6485](#)] that is considered to be outside the limited scope of an erratum.

[Section 2 of \[RFC6485\]](#) specified 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

[RFC4055] and [RFC5754] has 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 [RFC6485] inherited this requirement.

This document changes [Section 2 of \[RFC6485\]](#). By conforming to the CMS specifications as per [RFC4055] and [RFC5754], RPKI CMS objects are less likely to be rejected as non-conformant with the CMS standards. No change is made to the cryptographic status of the CMS objects produced. This change reflects the behaviour of deployed interoperating code. No other changes have been made to the specification as described in [RFC6485].

[9.](#) Acknowledgments

The authors acknowledge the re-use in this draft of material originally contained in working drafts the RPKI Certificate Policy and Resource Certificate profile documents. The co-authors of these two documents, namely Stephen Kent, Derrick Kong, Karen Seo, Ronald Watro, George Michaelson and Robert Loomans, are acknowledged, with thanks. The constraint on key size noted in this profile is the outcome of comments from Stephen Kent and review comments from David Cooper. Sean Turner has provided additional review input to this document.

Huston & Michaelson	Expires November 16, 2015	[Page 5]
---------------------	---------------------------	----------

Internet-Draft	RPKI Algorithm Profile	May 2015
----------------	------------------------	----------

Andrew Chi and David Mandelberg discovered the issue addressed in this update to [RFC6485], and the changes in this updated specification reflect the outcome of a discussion between Rob Austein and Matt Lepinski on the SIDR Working group mailing list. George Michaelson edited the update to this document.

[10.](#) References

[10.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification

Request Syntax Specification Version 1.7", [RFC 2986](#), November 2000.

- [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.
- [RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", [RFC 4211](#), September 2005.
- [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.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", [RFC 5652](#), September 2009.
- [RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", [RFC 5754](#), January 2010.
- [RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", [RFC 6480](#), February 2012.
- [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.

- [SHS] National Institute of Standards and Technology (NIST), "FIPS Publication 180-3: Secure Hash Standard", FIPS Publication 180-3, October 2008.

[10.2.](#) Informative References

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

Authors' Addresses

Geoff Huston
APNIC

Email: gih@apnic.net

George Michaelson (editor)
APNIC

Email: ggm@apnic.net