Internet Engineering Task Force (IETF)
Request for Comments: 7935
Obsoletes: 6485
Category: Standards Track
ISSN: 2070-1721

G. Huston
G. Michaelson, Ed.
APNIC

August 2016

The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure

Abstract

This document specifies the algorithms, algorithms’ parameters, asymmetric key formats, asymmetric key size, and signature format for the Resource Public Key Infrastructure (RPKI) subscribers that generate digital signatures on certificates, Certificate Revocation Lists (CRLs), Cryptographic Message Syntax (CMS) signed objects and certification requests as well as for the relying parties (RPs) that verify these digital signatures.

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 7841.

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/rfc7935.

Copyright Notice

Table of Contents

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) [RFC6480] subscribers when they apply digital signatures to certificates and Certificate Revocation Lists (CRLs) [RFC5280], Cryptographic Message Syntax (CMS) signed objects [RFC5652] (e.g., Route Origin Authorizations (ROAs) [RFC6482] and manifests [RFC6486]), and certification requests [RFC2986] [RFC4211]. Relying parties (RPs) also use the algorithms defined in this document to verify RPKI subscribers’ digital signatures [RFC6480].

The RPKI profiles and specification documents that reference RFC 6485 now refer to this document; these documents include the RPKI Certificate Policy (CP) [RFC6484], the RPKI Certificate Profile [RFC6487], the RPKI Architecture [RFC6480], and the Signed Object Template for the RPKI [RFC6488]. 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, CMS signed objects, and certification requests is RSA Public-Key Cryptography Standards (PKCS) #1 Version 1.5 (sometimes referred to as "RSASSA-PKCS1-v1_5") from Section 8.2 of [RFC3447].

- The hashing algorithm used in certificates, CRLs, CMS signed objects and certification requests is SHA-256 [SHS] (see note below).

  NOTE: The exception is the use of SHA-1 [SHS] when CAs generate authority and subject key identifiers [RFC6487].

In certificates, CRLs, and certification requests the hashing and digital signature algorithms are identified 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 these products.

The OID is in the following locations:

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

In CMS SignedData, the hashing (message digest) and digital signature algorithms are identified separately. The object identifier and parameters for SHA-256 (as defined in [RFC5754]) MUST be used for the SignedData digestAlgorithms field and the SignerInfo digestAlgorithm field. The object identifier and parameters for rsaEncryption [RFC3370] MUST be used for the SignerInfo signatureAlgorithm field when generating CMS SignedData objects. RPKI implementations MUST accept either rsaEncryption or sha256WithRSAEncryption for the SignerInfo signatureAlgorithm field when verifying CMS SignedData objects (for compatibility with objects produced by implementations conforming to [RFC6485]).

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.

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 the 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 signature field in the CMS SignedData’s SignerInfos 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 replaced to specify such future requirements, as and when appropriate.

The procedures to implement such a transition of key sizes and algorithms are specified in [RFC6916].

6. Security Considerations

The Security Considerations of [RFC4055], [RFC5280], and [RFC6487] apply to certificates and CRLs. The Security Considerations of [RFC2986], [RFC4211], and [RFC6487] apply to certification requests. The Security Considerations of [RFC5754] apply to CMS signed objects. No new security threats are introduced as a result of this specification.

7. Changes Applied to RFC 6485

This update includes a slight technical change to [RFC6485] that is considered to be outside the limited scope of an erratum. The document update process has included other errata and also corrected a number of nits.

Section 2 of [RFC6485] specified sha256WithRSAEncryption as the OID to use for the SignerInfo signatureAlgorithm field in CMS SignedObjects. However, existing implementations use the rsaEncryption OID for this field. (Support for rsaEncryption in third-party cryptographic libraries is better than sha256WithRSAEncryption, perhaps because [RFC3370] says that support for rsaEncryption is required, while support for OIDs that specify both RSA and a digest algorithm is optional.)

Rather than force existing implementations to switch to sha256WithRSAEncryption, this document was changed to follow existing practice. This does not represent a cryptographic algorithm change, just an identifier change. (Unlike certificates, CRLs, and certification requests, CMS signed objects have a separate algorithm identifier field for the hash (digest) algorithm, and that field is already required to contain the id-sha256 OID per Section 2.)

To avoid compatibility problems, RPs are still required to accept sha256WithRSAEncryption if encountered.

Other changes include:

* Minor wording and typo fixes.

* Corrections to references ([RFC5652] instead of [RFC3370], [RFC3447] instead of [RFC4055]).

* Additional citations included in the Introduction.

* Correction to the CRMF POPOSigningKey field that is mentioned in Section 2 (algorithmIdentifier instead of signature).

* Inclusion of certification requests in mentions of certificates, CRLs, and CMS signed objects.

* Replacement of text in Section 5 with a pointer to the procedures specified in [RFC6916] (algorithm agility).

* Replacement of "signed object" with "CMS signed object" everywhere.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <http://www.rfc-editor.org/info/rfc2986>.

[RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, DOI 10.17487/RFC3370, August 2002, <http://www.rfc-editor.org/info/rfc3370>.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, DOI 10.17487/RFC3447, February 2003, <http://www.rfc-editor.org/info/rfc3447>.

[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, DOI 10.17487/RFC4055, June 2005, <http://www.rfc-editor.org/info/rfc4055>.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, DOI 10.17487/RFC4211, September 2005, <http://www.rfc-editor.org/info/rfc4211>.

[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, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <http://www.rfc-editor.org/info/rfc5652>.

[RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", RFC 5754, DOI 10.17487/RFC5754, January 2010, <http://www.rfc-editor.org/info/rfc5754>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <http://www.rfc-editor.org/info/rfc6480>.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, DOI 10.17487/RFC6484, February 2012, <http://www.rfc-editor.org/info/rfc6484>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <http://www.rfc-editor.org/info/rfc6487>.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, DOI 10.17487/RFC6488, February 2012, <http://www.rfc-editor.org/info/rfc6488>.

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

8.2. Informative References

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <http://www.rfc-editor.org/info/rfc6482>.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)", RFC 6485, DOI 10.17487/RFC6485, February 2012, <http://www.rfc-editor.org/info/rfc6485>.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, DOI 10.17487/RFC6486, February 2012, <http://www.rfc-editor.org/info/rfc6486>.

[RFC6916] Gagliano, R., Kent, S., and S. Turner, "Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI)", BCP 182, RFC 6916, DOI 10.17487/RFC6916, April 2013, <http://www.rfc-editor.org/info/rfc6916>.

Acknowledgments

The authors acknowledge the reuse in this document of material originally contained in working drafts of the RPKI Certificate Policy [RFC6484] and resource certificate profile [RFC6487] documents. The coauthors 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.

Andrew Chi and David Mandelberg discovered the issue addressed in this replacement of [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. Richard Hansen contributed a significant number of suggestions that have been incorporated into this document.

Authors’ Addresses

Geoff Huston
APNIC

Email: gih@apnic.net

George Michaelson (editor)
APNIC

Email: ggm@apnic.net