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

G. Huston
APNIC

February 2012

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

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, and signed objects as well as for the relying parties (RPs) that verify these digital signatures.

Status of This Memo

Copyright Notice

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 the algorithms defined in this document to 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 [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, 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]. The hashing algorithm is not identified by itself when used in certificates and CRLs, as they are combined with the digital signature algorithm (see below).

  When used in the Cryptographic Message Syntax (CMS) SignedData, the hash algorithm (in this case, the hash algorithm is sometimes called a message digest algorithm) is identified by itself. For CMS SignedData, the object identifier and parameters for SHA-256 (as defined in [RFC5754]) MUST be used when populating the digestAlgorithms and digestAlgorithm fields.

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

When used to generate and verify digital signatures the hash and digital signature algorithms are referred 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.

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 signatureAlgoithm field [RFC3370] using the OID from above; 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.

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 CMS SignedData's signature field is as specified in [RFC3370].

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.

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 certificates and CRLs. The Security Considerations of [RFC5754] apply to signed objects. No new security threats are introduced as a result of this specification.

7. Acknowledgments

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

9. 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.

[RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, August 2002.

[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.

[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] Husotn, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, February 2012.

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

Author's Address

Geoff Huston
APNIC

EMail: gih@apnic.net