

SIDR  
Internet-Draft  
Intended status: Standards Track  
Expires: October 15, 2011

G. Huston  
APNIC  
April 13, 2011

The Profile for Algorithms and Key Sizes for use in the Resource Public  
Key Infrastructure  
[draft-ietf-sidr-rpki-algs-05.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 (RPs) 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 October 15, 2011.

## Copyright Notice

Copyright (c) 2011 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

Internet-Draft

RPKI Algorithm Profile

April 2011

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 [[ID.ietf-sidr-arch](#)].

This document is referenced by other RPKI profiles and specifications, including the RPKI Certificate Policy (CP) [[ID.ietf-sidr-cp](#)], the RPKI Certificate Profile [[ID.ietf-sidr-res-certs](#)], the SDR architecture [[ID.ietf-sidr-arch](#)], and the signed object template for the RPKI [[ID.ietf-sidr-signed-object](#)]. 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](#)]. Hash algorithms are not identified by themselves in certificates and CRLs instead 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 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 CAs generate authority and subject key identifiers [[ID.ietf-sidr-res-certs](#)].

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 signatureAlgorithm 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.

Huston

Expires October 15, 2011

[Page 3]

---

Internet-Draft

RPKI Algorithm Profile

April 2011

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 [\[RFC3370\]](#).

## [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 relaxed 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 [[ID.ietf-sidr-res-certs](#)] 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

[There are no IANA considerations in this document.]

Huston

Expires October 15, 2011

[Page 4]

---

Internet-Draft

RPKI Algorithm Profile

April 2011

## 8. Acknowledgments

The author acknowledges 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.

## 9. Normative References

[ID.ietf-sidr-arch]

Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", [draft-ietf-sidr-arch](#) (work in progress), September 2010.

[ID.ietf-sidr-cp]

Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate

Policy (CP) for the Resource PKI (RPKI)",  
[draft-ietf-sidr-cp](#) (work in progress), September 2010.

[ID.ietf-sidr-res-certs]

Husotn, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates",  
[draft-ietf-sidr-res-certs](#) (work in progress), May 2008.

[ID.ietf-sidr-signed-object]

Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure",  
[draft-ietf-sidr-signed-object-01.txt](#) (work in progress), October 2010.

[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.

Huston

Expires October 15, 2011

[Page 5]

---

Internet-Draft

RPKI Algorithm Profile

April 2011

[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.

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

Author's Address

Geoff Huston  
APNIC

Email: [gih@apnic.net](mailto:gih@apnic.net)