

SIDR
Internet-Draft
Intended status: Informational
Expires: November 17, 2010

G. Huston
APNIC
May 16, 2010

A Profile for Algorithms and Key Sizes for use in the Resource Public
Key Infrastructure
draft-ietf-sidr-rpki-algs-01.txt

Abstract

This document defines a profile for the algorithm and key size to be used for signatures applied to certificates, Certificate Revocation Lists, and signed objects in the context of the Resource Public Key Infrastructure.

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 17, 2010.

Copyright Notice

Copyright (c) 2010 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 defines a profile for the algorithm and key size to be used for signatures applied to certificates, Certificate Revocation Lists (CRLs), and signed objects in the context of the Resource Public Key Infrastructure (RPKI) [[I-D.ietf-sidr-arch](#)].

This section of the profile is specified in a distinct profile document, referenced by the RPKI Certificate Policy (CP) [[I-D.ietf-sidr-cp](#)] and the RPKI Certificate Profile [[I-D.ietf-sidr-res-certs](#)], in order to allow for a degree of algorithm and key agility in the RPKI, while permitting some longer term stability in the CP and Certificate Profile specifications.

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](#).

2. Algorithm and Key Size

This profile specifies the use of RSASSA-PKCS1-v1_5 [[RFC3447](#)] with the SHA-256 hash algorithm to compute the signature of certificates, CRLs, and signed objects in the context of the RPKI. Accordingly, the OID value in the RPKI for such signatures MUST be 1.2.840.113549.1.1.11 (sha256WithRSAEncryption). The RSA key pairs used to compute the signatures MUST have a 2048-bit modulus and a public exponent (e) of 65,537.

In order to facilitate a potential need to transition to stronger cryptographic algorithms in the future, Certification Authorities (CAs) and Relying Parties (RPs) SHOULD be able to generate and verify RSASSA-PKCS1-v1_5 signatures using the SHA-512 hash algorithm and RSA key sizes of 3072 and 4096 bits.

3. Future Upates

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 updated 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 accomodate 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.

Note: This document specifies the current algorithm requirements for the RPKI. The document acknowledges a requirement for algorithm agility, both in terms of larger key sizes in conjunction with the current algorithms, and transition to other algorithms. It is noted that the SDR architecture is one where each CA is required to generate signed material that may be validated by the entire collection of Relying Parties. This architectural requirement precludes the use of any negotiation between a CA and a RP as to the algorithm to use for signed products in the RPKI. This constraint implies that any transition of key size or algorithm will require a phased approach with the concurrent support of both old and new algorithms until such time as it is deemed that all RPs can support the new algorithm. Given that there is no accommodation for multiple signature algorithms in the current collection of RPKI specifications, either the collection of RPKI specifications will require subsequent revision to support the use of multiple signature algorithms within the specifications of signed objects in the RPKI, which itself poses a transition issue, or all such form of algorithm transition will require the construction and operation of a parallel RPKI structure that is entirely distinct from the "current" RPKI structure by virtue of its exclusive use of a "new" algorithm for signature generation. The latter option, that of the concurrent operation of parallel RPKI structures, poses some complex issues in terms of synchronisation of actions across the set of RPKI CAs, as well as issues of consistency and coherency in the operation of multiple parallel RPKI frameworks, as well as the uncertainties associated with a global determination of when any such transition can be considered "complete". The alternate approach, of allowing multiple signature algorithms in the RPKI certificate profile, and in the specification of CMS signatures as used in manifests, ROAS, other signed objects, and in the provisioning protocol, allows for

algorithm transition to occur within a single RPKI framework, and allows for individual CAs to commence use of multiple algorithms in a piecemeal fashion without reliance on the algorithm transition of the immediate superior CA and without a forced synchronisation of algorithm transition with subordinate CAs. In the light of this consideration, this document recommends the comprehensive revision of the existing RPKI specification and architecture documents to include provision for multiple signatures with multiple algorithms in order to support an orderly transition to longer key sizes and to other signature algorithms in the RPKI.

[4.](#) Security Considerations

The Security Considerations of [[RFC3779](#)], [[RFC5280](#)], and [[RFC4055](#)] apply to signatures as defined by this profile, and their use.

Algorithm transition poses some particular security issues, relating to potential vulnerabilities in the parallel operation of an RPKI framework where a potentially compromised algorithm remains in use beyond a reasonable time for retirement. These issues should be considered in detail in a future version of this document.

[5.](#) IANA Considerations

[There are no IANA considerations in this document.]

[6.](#) 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.

7. Normative References

- [I-D.ietf-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", [draft-ietf-sidr-arch](#) (work in progress), July 2009.
- [I-D.ietf-sidr-cp]
Seo, K., Watro, R., Kong, D., and S. Kent, "Certificate Policy (CP) for the Resource PKI (RPKI)", [draft-ietf-sidr-cp](#) (work in progress), July 2009.
- [I-D.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), February 2008.
- [RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography

Huston

Expires November 17, 2010

[Page 4]

Internet-Draft

RPKI Algorithm Profile

May 2010

Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", [RFC 3447](#), February 2003.

- [RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", [RFC 3779](#), June 2004.
- [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.
- [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.

Author's Address

Geoff Huston
Asia Pacific Network Information Centre

Email: gih@apnic.net

Huston

Expires November 17, 2010

[Page 5]