Individual Submission
Internet-Draft
Intended status: Informational
Expires: January 31, 2010

G. Huston
APNIC

July 30, 2009

A Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure
draft-huston-sidr-rpki-algs-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 31, 2010.

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.

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 the RSA algorithm [RFC3447] to compute the signature of certificates, CRLs and signed objects in the context of the RPKI. This profile specifies a default of SHA-256 with RSA (sha256WithRSAEncryption), and allows for the use of SHA-384 (sha384WithRSAEncryption) or SHA-512 (sha384WithRSAEncryption). Accordingly, The OID values used in the RPKI for such signatures MUST be one of { pkcs-1 11 }, { pkcs-1 12 } or { pkcs-1 13 } [RFC4055].

The required RSA key size MUST be 2048 bits.

The public exponent (e) of the RSA algorithm is F4 (65,537).

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.

Certification Authorities (CAs) and Relying Parties (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.

4. Security Considerations

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

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 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