Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 2, 2015

L. Vegoda
T. Manderson
ICANN
September 29, 2014

RPKI Key Management Issues
draft-vegoda-manderson-sidr-key-management-00

Abstract

Strong key management is central to the security of any hierarchy of cryptographic certificates. Well-defined architectural objectives will be important guides to the detailed design work needed to support the deployment of a Global Trust Anchor for the RPKI. This document identifies some of the questions that need to be addressed in the architectural guidelines for key management.

Table of Contents

1. Introduction 2
2. Terminology 2
3. Definitions 2
4. Algorithm support 3
4.1. Algorithm based on jurisdiction 3
4.2. Algorithm vulnerability 3
5. Key Length 3
6. Key rollover support 4
6.1. Protocol support for key rollover events not requiring a change in cryptographic algorithm 4
7. Communication from validators to objects signers regarding validation status 4
8. IANA Considerations 4
9. Security Considerations 5
10. References 5
Appendix A. Acknowledgements 6
Authors' Addresses 6

1. Introduction

Strong key management is central to the security of any hierarchy of cryptographic certificates [NISTKEYMANAGEMENT]. The deployment of a Global Trust Anchor for the RPKI requires a set of well-defined architectural objectives to guide the detailed design work. This document identifies some of the questions that need to be addressed in the architectural guidelines for key management.

2. Terminology

It is assumed that the reader is familiar with the terms and concepts described in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280], "A Profile for X.509 PKIX Resource Certificates" [RFC6487], and "X.509 Extensions for IP Addresses and AS Identifiers" [RFC3779].

3. Definitions

The Global Trust Anchor (GTA) is the root of the Internet's RPKI hierarchy and is responsible for issuing subordinate certificates for resources within 0/0 (IPv4), 0::/0 (IPv6), and Autonomous System Numbers 0-4294967295.

4. Algorithm support

4.1. Algorithm based on jurisdiction

[RFC6485] requires that RPKI signatures use a SHA-256 hashing algorithm and 2048-bit RSA keys. Some jurisdictions have legal impediments to implementing this requirement [RFC5830] [RFC5832], resulting in a need to use other cryptographic algorithms. To support RPKI CAs in all jurisdictions, there is therefore a need to allow the use of algorithms other than RSA and SHA-256, and so validators will need to support these algorithms if they are going to successfully validate objects signed with a certificate using a signature algorithm other than RSA with a SHA-256 hash.

Advice is sought on how jurisdictional requirements can be addressed in the set of supported algorithms.

4.2. Algorithm vulnerability

Published cryptographic algorithms are constantly tested [NISTALGORITHMTESTING]. There is a potential that the RSA algorithm will be found vulnerable to one or more attacks during the lifetime of an RPKI GTA that uses the algorithm. In order to mitigate this risk it is necessary to require support for additional public-key cryptographic algorithms in the RPKI so that the operator can roll the GTA to one using a different algorithm.

Advice is sought on how a production GTA can roll the algorithms it uses in the event of an effective attack on the RSA algorithm becoming available during the production lifetime of the GTA.

5. Key Length

The US National Institute of Standards and Technology recommends [NISTKEYMANAGEMENT] that 2048-bit RSA keys, as required in [RFC6485], should not be used after 2030. It is common for an X.509 trust anchor to have a 15 year or longer lifetime [COMODO] [DIGICERT] [ENTRUST] [SYMANTEC]. If an RPKI GTA uses a standard lifetime it needs to use a key that is longer than 2048 bits. Alternatively, the key needs to be rolled prior to 2030 and the protocol must be updated to support keys that are judged to be safe to use after that date. If the key rollover and protocol update is selected, the lead time needs to be sufficient to make sure that the entire deployed base is upgraded to support the new algorithm of key length.

Advice is sought on whether the GTA should use a shorter lifetime than is typical in X.509 TAs or use a keylength that is considered safe beyond 2030.

6. Key rollover support

6.1. Protocol support for key rollover events not requiring a change in cryptographic algorithm

Key rollover events must be communicated to subordinate CAs so that they know to reissue certificates and entities holding certificates, so that they know to re-sign objects. Key rollover events must also be communicated to validators so that they know to validate against a new certificate.

No mechanism has yet been defined for communicating key rollovers. This could either be performed with in-protocol signaling or via an out-of-band mechanism using domain specific businesses processes. Whichever option is selected needs to be sufficiently robust to allow for all involved parties to reissue certificates, or re-sign objects, or just configure a new key, expeditiously.

Advice is sought on whether in-protocol signaling should be developed or an out-of-band set of domain specific business processes should be used.

7. Communication from validators to objects signers regarding validation status

No mechanism has yet been defined to allow validators to tell a certificate issuer or object signer that a certificate it issued or object it signed has failed validation. In an inter-domain routing context this means that validation failure might only be communicated via a routing failure when local policy is configured to drop a route if validation fails.

This lack of validation status signaling could have catastrophic consequences if a problem occurs in a certificate or object near the top of the hierarchy. Such a failure in validation could impact a significant percentage of the Internet's routing capability without providing adequate tools for diagnosis and remediation.

Advice is sought on whether it is important for validators to be able to signal validation failures to certificate issuers and signers.

8. IANA Considerations

This document does not define any IANA actions. This section may be removed by the RFC Editor prior to publication.

9. Security Considerations

The RPKI needs to support better security in inter-domain routing. The security improvements should be partnered with improvements to the overall robustness and resilience of the inter-domain routing system. Until the issues described in this document are addressed the fragility of the system means that it is not safe to deploy in production environments and must remain merely of academic interest.

10. References

[COMODO] Comodo CA, Ltd., "Comodo Certification Practices Statement, Section 2.1.1, v.4.0", July 2012, <https://www.comodo.com/repository/Comodo_CA_CPS_4.0.pdf>.

[DIGICERT] DigiCert Inc., "DigiCert Certification Practices Statement, Section 6.3.2, v.4.0.6", May 2014, <https://www.digicert.com/docs/cps/DigiCert_CPS_v406-May-14-2014.pdf>.

[ENTRUST] Entrust Limited, "Entrust Certificate Services Certification Practice Statement, Appendix A, v.2.11", March 2014, <http://www.entrust.net/CPS/pdf/SSL-CPS-English-20140304-Version-2-11.pdf>.

[NISTALGORITHMTESTING] National Institute of Standards and Technology, "Cryptographic Algorithm Validation Program", September 2014, <http://www.nist.gov/itl/csd/stvm/cavp.cfm>.

[NISTKEYMANAGEMENT] Barker, E., "NIST Special Publication 800-57, Recommendation for Key Management - Part 1: General (Revision 3)", July 2014, <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf>.

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

[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.

[RFC5830] Dolmatov, V., "GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms", RFC 5830, March 2010.

[RFC5832] Dolmatov, V., "GOST R 34.10-2001: Digital Signature Algorithm", RFC 5832, March 2010.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)", RFC 6485, February 2012.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

[SYMANTEC] Symantec Corporation, "Symantec Trust Network (STN) Certification Practice Statement v.3.8.1.6, Section 6.3.2", July 2014, <http://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf>.

Appendix A. Acknowledgements

Geoff Huston, George Michaelson, Andrew de la Haye, and Tim Bruijnzeels, Richard Barnes, and Alia Atlas helped clarify some of the questions in this document. Thanks to Kim Davies, Tomofumi Okubo, and Elise Gerich for early reviews of this document.

Authors' Addresses

Leo Vegoda
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

Phone: +1 310 301 5800
Email: leo.vegoda@icann.org
URI: http://www.icann.org/

Terry Manderson
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

Phone: +1 310 301 5800
Email: terry.manderson@icann.org
URI: http://www.icann.org/