Network Working Group
Internet-Draft
Intended status: BCP
Expires: August 4, 2011

J. Abley
D. Knight
ICANN

January 31, 2011

Establishing an Appropriate Root Zone DNSSEC Trust Anchor at Startup
draft-jabley-dnsop-validator-bootstrap-00

Abstract

Domain Name System Security Extensions (DNSSEC) allow cryptographic signatures to be used to validate responses received from the Domain Name System (DNS). A DNS client which validates such signatures is known as a validator.

The choice of appropriate root zone trust anchor for a validator is expected to vary over time as the corresponding cryptographic keys used in DNSSEC are changed.

This document provides guidance on how validators might determine an appropriate trust anchor for the root zone to use at start-up, or when other mechanisms intended to allow key rollover to be tolerated gracefully are not available.

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 August 4, 2011.

Table of Contents

1. Definitions

The terms Key Signing Key (KSK) and Trust Anchor are used as defined in [RFC4033].

The term Validator is used in this document to mean a Validating Security-Aware Stub Resolver, as defined in [RFC4033].

2. Introduction

The Domain Name System (DNS) is described in [RFC1034] and [RFC1035]. DNS Security Extensions (DNSSEC) are described in [RFC4033], [RFC4034] and [RFC4035].

The root zone of the DNS was signed using DNSSEC in July 2011, and many top-level domain registries have since signed their zones, installing secure delegations for them in the root zone. A single trust anchor for the root zone is hence increasingly sufficient for validators.

Validators are deployed in a variety of environments, and there is variation in the amount of system administration that might reasonably be expected to be available. For example, embedded devices might never be administered by a human operator, whereas validators deployed on general-purpose operating systems in enterprise networks might have technical staff available to assist with their configuration.

This document includes descriptions of mechanisms for validator bootstrapping, intended to be sufficient for embedded devices. The implementation of those mechanisms might be automatic in the case of unattended devices, or manual, carried out by a systems administrator, depending on local circumstances.

The choice of appropriate trust anchor for a DNSSEC Validator is expected to vary over time as the corresponding KSK used in the root zone is changed. The DNSSEC Policy and Practice Statement (DPS) for the root zone KSK maintainer [KSK-DPS] specifies that scheduled KSK rollover will be undertaken according to the semantics specified in [RFC5011]. Validators which are able to recognise and accommodate those semantics should need no additional support to be able to maintain an appropriate trust anchor over a root zone KSK rollover event.

The possibility remains, however, that [RFC5011] signalling will not be available to a validator: e.g. certain classes of emergency KSK rollover may require a compromised KSK to be discarded more quickly than [RFC5011] specifies, or a validator might be off-line over the whole key-roll event.

This document provides guidance on how DNSSEC Validators might determine an appropriate set of trust anchors to use at start-up, or when other mechanisms intended to allow key rollover to be tolerated gracefully are not available.

The bootstrapping procedures described in this document are also

expected to be useful for a deployed, running validator which is not able to accommodate a KSK roll using [RFC5011] signalling.

3. Summary of Approach

A validator that has no valid trust anchor initialises itself as follows.

3.1. Initial State

A validator in its initial state is capable of sending and receiving DNS queries and responses, but is not capable of validating signatures received in responses.

A validator must confirm that its local clock is sufficiently accurate before trust anchors can be established, and before processing of DNSSEC signatures can proceed. Discussion of timing considerations can be found in Section 4.

3.2. Trust Anchor Retrieval

Once the local clock has been synchronised, a validator may proceed to gather candidate trust anchors for consideration. Discussion of trust anchor retrieval can be found in Section 5.

3.3. Trust Anchor Selection

Once a set of candidate trust anchors has been obtained, a validator attempts to find one trust anchor in the set which is appropriate for use. This process involves verification of cryptographic signatures, and is discussed in Section 6.

3.4. Full Operation

The validator now has an accurate trust anchor for the root zone, and is capable of validating signatures on responses from the DNS.

4. Timing Considerations

DNSSEC signatures are valid for particular periods of time, as specified by the administrator of the zone containing the signatures. It follows that any validator must maintain an accurate local clock in order to verify that signatures are accurate.

Trust anchors correspond to KSKs in particular zones. Zone administrators may choose to replace KSKs from time to time, e.g. due to a key compromise or local key management policy, and the corresponding appropriate choice in trust anchor will change as KSKs are replaced.

Trust anchors for the root zone in particular are published with intended validity periods, as discussed in Section 5. A validator making use of such trust anchors also requires an accurate local clock in order to avoid configuring a local trust anchor which corresponds to an old key.

Validators should take appropriate steps to ensure that their local clocks are set with sufficient accuracy, and in the case where local clocks are set with reference to external time sources over a network [RFC5905] that the time information received from those sources is authentic.

5. Retrieval of Candidate Trust Anchors

Candidate trust anchors may be retrieved using several mechanisms. The process of gaining trust in particular candidate trust anchors before using them is discussed in Section 6.

5.1. Retrieval of Trust Anchors from Local Sources

A trust anchor which is packaged with validator software can never be trusted, since the corresponding root zone KSK may have rolled since the software was packaged, and the trust anchor may be derived from a root zone KSK that was retired due to compromise.

Validators should never use local trust anchors for bootstrapping.

5.2. Retrieval of Trust Anchors from the DNS

The current root zone trust anchor is a hash (in DS RDATA format) of a member of the root zone apex DNSKEY RRSet that has the SEP bit set. Such a trust anchor could be derived from a response to the query ". IN DNSKEY?", but there is no mechanism available to trust the result: without an existing, accurate trust anchor the validator has no means to gauge the authenticity of the response.

Validators should never derive trust anchors from DNSKEY RRSets obtained from the DNS.

5.3. Retrieval of Trust Anchors from the Root Zone KSK Manager

The Root Zone KSK Manager publishes trust anchors corresponding to the root zone KSK as described in [I-D.jabley-dnssec-trust-anchor].

A full history of previously-published trust anchors, including the trust anchor recommended for immediate use, is made available in an XML document at the following stable URLs:

- <http://data.iana.org/root-anchors/root-anchors.xml>
- <https://data.iana.org/root-anchors/root-anchors.xml>

Validity periods for each trust anchor packaged in the root-anchors.xml document are provided as XML attributes, allowing an appropriate trust anchor for immediate use to be identified (but see Section 4).

Individual trust anchors are also packaged as X.509 identity certificates, signed by various Certificate Authorities (CAs). URLs to allow those certificates to be retrieved are included as optional

elements in the XML document.

For automatic bootstrapping, the recommended approach is as follows.

1. Retrieve <http://data.iana.org/root-anchors/root-anchors.xml>

2. Identify the trust anchors which are valid for current use, with reference to the current time and date.

3. Retrieve the corresponding X.509 identity certificates for the key identified in the previous step, for use in establishing trust in the retrieved trust anchor (see Section 6).

6. Establishing Trust in Candidate Trust Anchors

Once a candidate trust anchor has been retrieved, the validator must establish that it is authentic before it can be used. This document recommends that this be carried out by checking the signatures on each of the X.509 identity certificates retrieved in the previous step until a certificate is found which matches a CA trust anchor.

This verification phase requires that validators ship with a useful set of CA trust anchors, and that corresponding identity certificates are published by the root zone KSK manager. In some cases validator implementors may decide to use commercial CA services, perhaps a subset of the "browser list" that is commonly distributed with web browsers; alternatively a vendor may instantiate its own CA and make arrangements with the root zone KSK manager to have the corresponding identity certificate locations published in root-anchors.xml.

The CA trust anchors packaged with validators should have an expected lifetime in excess of the anticipated life of the validator. As a protection against CA failure, validators are recommended to ship with more than one CA trust anchor.

7. Failure to Locate a Valid Trust Anchor

A validator that has failed to locate a valid trust anchor may re-try the retrieval and trust establishment phases indefinitely, but must not perform validation on DNS responses until a valid trust anchor has been identified.

8. IANA Considerations

This document has no IANA actions.

9. Security Considerations

This document discusses an approach for automatic configuration of trust anchors in a DNSSEC validator.

10. Normative References

[I-D.jabley-dnssec-trust-anchor]
Abley, J. and J. Schlyter, "DNSSEC Trust Anchor Publication for the Root Zone", draft-jabley-dnssec-trust-anchor-01 (work in progress), October 2010.

[KSK-DPS] Ljunggren, F., Okubo, T., Lamb, R., and J. Schlyter, "DNSSEC Practice Statement for the Root Zone KSK Operator", May 2010.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", RFC 5011, September 2007.

[RFC5905] Mills, D., Martin, J., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

Appendix A. Acknowledgements

This document contains material first discussed at VeriSign and ICANN during the deployment of DNSSEC in the root zone, and also draws upon subsequent technical discussion from public mailing lists. The contributions of all those who voiced opinions are acknowledged.

Appendix B. Editorial Notes

This section (and sub-sections) to be removed prior to publication.

B.1. Discussion

This is not a working group document. However, the topics discussed in this document are consistent with the general subject area of the DNSOP working group, and discussion of this document could reasonably take place on the corresponding mailing list.

B.2. Change History

00 Initial draft.

Authors' Addresses

Joe Abley
ICANN
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292
USA

Phone: +1 519 670 9327
Email: joe.abley@icann.org

Dave Knight
ICANN
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292
USA

Phone: +1 310 913 4512
Email: dave.knight@icann.org