Internet Engineering Task Force (IETF)
Request for Comments: 9718
Obsoletes: 7958
Category: Informational
ISSN: 2070-1721

J. Abley
Cloudflare
J. Schlyter
Kirei AB
G. Bailey
Independent
P. Hoffman
ICANN

January 2025

DNSSEC Trust Anchor Publication for the Root Zone

Abstract

The root zone of the global Domain Name System (DNS) is cryptographically signed using DNS Security Extensions (DNSSEC).

In order to obtain secure answers from the root zone of the DNS using DNSSEC, a client must configure a suitable trust anchor. This document describes the format and publication mechanisms IANA uses to distribute the DNSSEC trust anchors.

This document obsoletes RFC 7958.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9718.

Table of Contents

1. Introduction

The global Domain Name System (DNS) is described in [RFC1034] and [RFC1035]. DNS Security Extensions (DNSSEC) are described in [RFC9364].

In the DNSSEC protocol, Resource Record Sets (RRsets) are signed cryptographically. This means that a response to a query contains signatures that allow the integrity and authenticity of the RRset to be verified. DNSSEC signatures are validated by following a chain of signatures to a "trust anchor". The reason for trusting a trust anchor is outside the DNSSEC protocol, but having one or more trust anchors is required for the DNSSEC protocol to work.

The publication of trust anchors for the root zone of the DNS is an IANA function performed by ICANN, through its affiliate Public Technical Identifiers (PTI). A detailed description of corresponding key management practices can be found in [DPS].

This document describes the formats and distribution methods of DNSSEC trust anchors that are used by IANA for the root zone of the DNS. Other organizations might have different formats and mechanisms for distributing DNSSEC trust anchors for the root zone; however, most operators and software vendors have chosen to rely on the IANA trust anchors.

The formats and distribution methods described in this document are a complement to, not a substitute for, the automated DNSSEC trust anchor update protocol described in [RFC5011]. That protocol allows for secure in-band succession of trust anchors when trust has already been established. This document describes one way to establish an initial trust anchor that can be used by the mechanism defined in [RFC5011].

This document obsoletes [RFC7958].

1.1. Definitions

The term "trust anchor" is used in many different contexts in the security community. Many of the common definitions conflict because they are specific to a specific system, such as just for DNSSEC or just for S/MIME messages.

In cryptographic systems with hierarchical structure, a trust anchor is an authoritative entity for which trust is assumed and not derived. The format of the entity differs in different systems, but

all common uses of the term "trust anchor" share the basic idea that the decision to trust this entity is made outside of the system that relies on it.

The root zone trust anchor formats published by IANA are defined in Section 2. [RFC4033] defines a trust anchor as a "configured DNSKEY RR or DS RR hash of a DNSKEY RR". Note that the formats defined here do not match the definition of "trust anchor" from [RFC4033]; however, a system that wants to convert the trusted material from IANA into a Delegation Signer (DS) RR can do so.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. IANA DNSSEC Root Zone Trust Anchor Format and Semantics

IANA publishes trust anchors for the root zone as an XML [W3C.REC-xml11-20060816] document that contains the hashes of the DNSKEY records and optionally the keys from the DNSKEY records.

This format and the associated semantics are described in the rest of this section.

Note that the XML document can have XML comments. For example, IANA might use these comments to add pointers to important information on the IANA website. XML comments are only used as human-readable commentary, not extensions to the grammar.

The XML document contains a set of hashes for the DNSKEY records that can be used to validate the root zone. The hashes are consistent with the defined presentation format of a DS resource.

The XML document can also contain the keys and flags from the DNSKEY records. The keys and flags are consistent with the defined presentation format of a DNSKEY resource.

Note that the hashes are mandatory in the syntax, but the keys are optional.

2.1. XML Syntax

Below is the RELAX NG Compact Schema [RELAX-NG] for the documents used to publish trust anchors:

```
datatypes xsd = "http://www.w3.org/2001/XMLSchema-datatypes"

start = element TrustAnchor {
  attribute id { xsd:string },
  attribute source { xsd:string },
  element Zone { xsd:string },
  keydigest+
}

keydigest = element KeyDigest {
  attribute id { xsd:string },
  attribute validFrom { xsd:dateTime },
  attribute validUntil { xsd:dateTime }?,

  element KeyTag {
      xsd:nonNegativeInteger { maxInclusive = "65535" } },
  element Algorithm {
      xsd:nonNegativeInteger { maxInclusive = "255" } },
  element DigestType {
```

```
        xsd:nonNegativeInteger { maxInclusive = "255" } },
    element Digest { xsd:hexBinary },
    publickeyinfo?
  }

  publickeyinfo =
    element PublicKey { xsd:base64Binary },
    element Flags {
       xsd:nonNegativeInteger { maxInclusive = "65535" } }
```

2.2. XML Semantics

The TrustAnchor element is the container for all of the trust anchors in the file.

The id attribute in the TrustAnchor element is an opaque string that identifies the set of trust anchors. Its value has no particular semantics. Note that the id attribute in the TrustAnchor element is different than the id attribute in the KeyDigest element described below.

The source attribute in the TrustAnchor element gives information about where to obtain the TrustAnchor container. It is likely to be a URL and is advisory only.

The Zone element in the TrustAnchor element states to which DNS zone this container applies. The Zone element is in presentation format as specified in [RFC1035], including the trailing dot. The root zone is indicated by a single period (.) character without any quotation marks.

The TrustAnchor element contains one or more KeyDigest elements. Each KeyDigest element represents the digest of a past, current, or potential future DNSKEY record of the zone defined in the Zone element. The values for the elements in the KeyDigest element are defined in [RFC4034]. The IANA registries for DNSSEC-related values are described in [RFC9157].

The id attribute in the KeyDigest element is an opaque string that identifies the hash. Note that the id attribute in the KeyDigest element is different than the id attribute in the TrustAnchor element described above.

The validFrom and validUntil attributes in the KeyDigest element specify the range of times that the KeyDigest element can be used as a trust anchor.

The KeyTag element in the KeyDigest element contains the key tag for the DNSKEY record represented in this KeyDigest.

The Algorithm element in the KeyDigest element contains the DNSSEC signing algorithm identifier for the DNSKEY record represented in this KeyDigest.

The DigestType element in the KeyDigest element contains the DNSSEC digest algorithm identifier for the DNSKEY record represented in this KeyDigest.

The Digest element in the KeyDigest element contains the hexadecimal representation of the hash for the DNSKEY record represented in this KeyDigest.

The publickeyinfo named pattern in the KeyDigest element contains two mandatory elements: the base64 representation of the public key for the DNSKEY record represented in this KeyDigest and the flags of the DNSKEY record represented in this KeyDigest. The publickeyinfo named

pattern is optional and is new in this specification. It can be useful when IANA has a trust anchor that has not yet been published in the DNS root and for calculating a comparison to the Digest element.

2.3. XML Example

The following is an example of what the trust anchor file might look like. The full public key is only given for a trust anchor that does not have a validFrom time in the past.

```
<?xml version="1.0" encoding="UTF-8"?>
<TrustAnchor id="E9724F53-1851-4F86-85E5-F1392102940B"
  source="http://data.iana.org/root-anchors/root-anchors.xml">
  <Zone>.</Zone>
  <KeyDigest id="Kjqmt7v"
      validFrom="2010-07-15T00:00:00+00:00"
      validUntil="2019-01-11T00:00:00+00:00">  <!-- This key
      is no longer valid, since validUntil is in the past -->
    <KeyTag>19036</KeyTag>
    <Algorithm>8</Algorithm>
    <DigestType>2</DigestType>
    <Digest>
49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
    </Digest>
  </KeyDigest>
  <KeyDigest id="Klajeyz" validFrom="2017-02-02T00:00:00+00:00">
    <KeyTag>20326</KeyTag>
    <Algorithm>8</Algorithm>
    <DigestType>2</DigestType>
    <Digest>
E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
    </Digest>
    <PublicKey>
      AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4Rg
      WOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQ
      uCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj
      /EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Ap
      xz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXG
      Xws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
    </PublicKey>
    <Flags>257</Flags>
  </KeyDigest>
  <!-- The following is called "KSK-2024" as a shorthand name -->
  <KeyDigest id="Kmyv6jo" validFrom="2024-07-18T00:00:00+00:00">
    <KeyTag>38696</KeyTag>
    <Algorithm>8</Algorithm>
    <DigestType>2</DigestType>
    <Digest>
683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16
    </Digest>
  </KeyDigest>
</TrustAnchor>
```

The DS RRset derived from this example is:

```
. IN DS 20326 8 2
   E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
. IN DS 38696 8 2
   683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16
```

Note that this DS record set only has two records. A potential third record, one that includes the key tag 19036, is already invalid based on the validUntil attribute’s value and is thus not part of the trust anchor set.

The DNSKEY RRset derived from this example is:

```
. IN DNSKEY 257 3 8
  AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
  +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
  ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
  0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
  oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
  RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
  R1AkUTV74bU=
```

Note that this DNSKEY record set only has one record. A potential second record, one based on the key tag 19036, is already invalid based on the validUntil attribute's value and is thus not part of the trust anchor set. Another potential second record, one based on the key tag 38696, does not contain the optional publickeyinfo named pattern; therefore, the DNSKEY record for it cannot be calculated.

3. Root Zone Trust Anchor Retrieval

3.1. Retrieving Trust Anchors with HTTPS and HTTP

Trust anchors are available for retrieval using HTTPS and HTTP.

In this section, all URLs are given using the "https:" scheme. If HTTPS cannot be used, replace the "https:" scheme with "http:".

The URL for retrieving the set of hashes in the XML document described in Section 2 is <https://data.iana.org/root-anchors/root-anchors.xml>.

3.2. Accepting DNSSEC Trust Anchors

A validator operator can choose whether or not to accept the trust anchors described in this document using whatever policy they want. In order to help validator operators verify the content and origin of trust anchors they receive, IANA uses digital signatures that chain to an ICANN-controlled Certificate Authority (CA) over the trust anchor data.

It is important to note that the ICANN CA is not a DNSSEC trust anchor. Instead, it is an optional mechanism for verifying the content and origin of the XML and certificate trust anchors.

The content and origin of the XML document can be verified using a digital signature on the file. IANA provides a detached Cryptographic Message Syntax (CMS) [RFC5652] signature that chains to the ICANN CA with the XML document. This can be useful for validator operators who have received a copy of the ICANN CA's public key in a trusted out-of-band fashion. The URL for a detached CMS signature for the XML document is <https://data.iana.org/root-anchors/root-anchors.p7s>.

Another method IANA uses to help validator operators verify the content and origin of trust anchors they receive is to use the Transport Layer Security (TLS) protocol for distributing the trust anchors. Currently, the CA used for "data.iana.org" is well known, that is, one that is a WebTrust-accredited CA. If a system retrieving the trust anchors trusts the CA that IANA uses for the "data.iana.org" web server, HTTPS SHOULD be used instead of HTTP in order to have assurance of data origin.

3.3. Changes in the Trust Model for Distribution

IANA used to distribute trust anchors as a self-signed Pretty Good Privacy (PGP) message and as a self-issued certificate signing

request; this was described in [RFC7958]. This document removes those methods because they rely on a trust model that mixes out-of-band trust of authentication keys with out-of-band trust of the DNSSEC root keys. Note, however, that cryptographic assurance for the contents of the trust anchor now comes from the Web PKI or the ICANN CA as described in Section 3.2. This cryptographic assurance is bolstered by informal comparisons made by users of the trust anchors, such as software vendors comparing the trust anchor files they are using.

4. Security Considerations

This document describes how DNSSEC trust anchors for the root zone of the DNS are published. Many DNSSEC clients will only configure IANA-issued trust anchors for the DNS root to perform validation. As a consequence, reliable publication of trust anchors is important.

This document aims to specify carefully the means by which such trust anchors are published, with the goal of making it easier for those trust anchors to be integrated into user environments. Some of the methods described (such as accessing over the Web with or without verifying the signature on the file) have different security properties; users of the trust anchor file need to consider these when choosing whether to load the set of trust anchors.

4.1. Security Considerations for Relying Parties

The body of this document does not specify any particular behavior for relying parties. Specifically, it does not say how a relying party should treat the trust anchor file as a whole. However, some of the contents of the trust anchor file require particular attention for relying parties.

4.1.1. validUntil

Note that the validUntil attribute of the KeyDigest element is optional. If the relying party is using a trust anchor that has a KeyDigest element that does not have a validUntil attribute, it can change to a trust anchor with a KeyDigest element that does have a validUntil attribute, as long as that trust anchor’s validUntil attribute is in the future and the KeyTag, Algorithm, DigestType, and Digest elements of the KeyDigest are the same as those in the previous trust anchor.

Relying parties SHOULD NOT use a KeyDigest outside of the time range given in the validFrom and validUntil attributes.

4.1.2. Comparison of Digest and publickeyinfo

A KeyDigest element can contain both a Digest and a publickeyinfo named pattern. If the Digest element would not be a proper DS record for a DNSKEY record represented by the publickeyinfo named pattern, relying parties MUST NOT use that KeyDigest as a trust anchor. A relying party that wants to make such a comparison needs to marshal the elements of the DNSKEY record that became the DS record using the algorithm specified in Section 5.1.4 of [RFC4034].

Relying parties need to implement trust anchor matching carefully. A single trust anchor represented by a KeyDigest element can potentially change its Digest and KeyTag values between two versions of the trust anchor file, for example, when the key is revoked or the flag value changes for some other reason. Relying parties that fail to take this property into account are at risk of using an incorrect set of trust anchors.

4.1.3. Different Outputs from Processing the Trust Anchor File

Relying parties that require the optional publickeyinfo named pattern to create trust anchors will store fewer trust anchors than those that only require a Digest element. Thus, two systems processing the same trust anchor file can end up with a different set of trust anchors.

5. IANA Considerations

Each time IANA produces a new trust anchor, it MUST publish that trust anchor using the format described in this document.

IANA MAY delay the publication of a new trust anchor for operational reasons, such as having a newly created key in multiple facilities.

When a trust anchor that was previously published is no longer suitable for use, IANA MUST update the trust anchor file accordingly by setting a validUntil date for that trust anchor. The validUntil attribute that is added MAY be a date in the past or in the future, depending on IANA's operational choices.

More information about IANA's policies and procedures for how the cryptographic keys for the DNS root zone are managed (also known as "DNSSEC Practice Statements" or "DPSs") can be found at <https://www.iana.org/dnssec/procedures>.

[RFC7958] defined id-mod-dns-resource-record, value 70, which was added to the "SMI Security for PKIX Module Identifier" registry. This document does not use that identifier.

6. References

6.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, <https://www.rfc-editor.org/info/rfc5011>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC7958] Abley, J., Schlyter, J., Bailey, G., and P. Hoffman,

"DNSSEC Trust Anchor Publication for the Root Zone", RFC 7958, DOI 10.17487/RFC7958, August 2016, <https://www.rfc-editor.org/info/rfc7958>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9157] Hoffman, P., "Revised IANA Considerations for DNSSEC", RFC 9157, DOI 10.17487/RFC9157, December 2021, <https://www.rfc-editor.org/info/rfc9157>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[W3C.REC-xml11-20060816] Bray, T., Paoli, J., Sperberg-McQueen, M., Maler, E., Yergeau, F., and J. Cowan, "Extensible Markup Language (XML) 1.1 (Second Edition)", W3C Recommendation REC-xml11-20060816, 16 August 2006, <https://www.w3.org/TR/2006/REC-xml11-20060816>.

6.2. Informative References

[DPS] Root Zone KSK Operator Policy Management Authority, "DNSSEC Practice Statement for the Root Zone KSK Operator", <https://www.iana.org/dnssec/procedures>.

[RELAX-NG] Clark, J., "RELAX NG Compact Syntax", OASIS Committee Specification, November 2002, <https://www.oasis-open.org/committees/relax-ng/compact-20021121.html>.

Appendix A. Changes from RFC 7958

This document includes the following changes:

* Made a significant technical change per Erratum ID 5932 <https://www.rfc-editor.org/errata/eid5932>. This change is in the seventh paragraph of Section 2.2.

* Added the optional publickeyinfo named pattern with two mandatory elements, PublicKey and Flags.

* Removed the certificates and certificate signing mechanisms.

* Removed the detached OpenPGP signature mechanism.

* Updated the reference to the DNSSEC Practice Statement [DPS].

* Stated explicitly that the XML documents might have XML comments in them.

* Clarified the use of the detached CMS signature.

* Updated the IANA Considerations section to indicate requirements on IANA.

* Simplified the description of using the validFrom and validUntil attributes.

* Added new security considerations.

* Made some editorial changes.

Appendix B. Historical Note

The first Key Signing Key (KSK) for use in the root zone of the DNS was generated at a key ceremony at the ICANN Key Management Facility (KMF) in Culpeper, Virginia, USA on 2010-06-16. This key entered production during a second key ceremony held at an ICANN KMF in El Segundo, California, USA on 2010-07-12. The resulting trust anchor was first published on 2010-07-15.

The second KSK for use in the root zone of the DNS was generated at key ceremony #27 at the ICANN KMF in Culpeper, Virginia, USA on 2016-10-27. This key entered production during key ceremony #28 held at the ICANN KMF in El Segundo, California, USA on 2017-02-02. The resulting trust anchor was first published on 2018-11-11.

More information about the key ceremonies, including full records of previous ceremonies and plans for future ceremonies, can be found at <https://www.iana.org/dnssec/ceremonies>.

Acknowledgements

Many pioneers paved the way for the deployment of DNSSEC in the root zone of the DNS, and the authors hereby acknowledge their substantial collective contribution.

RFC 7958 incorporated suggestions made by Alfred Hoenes and Russ Housley, whose contributions are appreciated.

Authors' Addresses

Joe Abley
Cloudflare
Amsterdam
Netherlands
Email: jabley@cloudflare.com

Jakob Schlyter
Kirei AB
Email: jakob@kirei.se

Guillaume Bailey
Independent
Email: guillaumebailey@outlook.com

Paul Hoffman
ICANN
Email: paul.hoffman@icann.org