

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 9, 2017

J. Abley  
Dyn, Inc.  
J. Schlyter  
Kirei AB  
G. Bailey  
Independent  
P. Hoffman  
ICANN  
July 8, 2016

**DNSSEC Trust Anchor Publication for the Root Zone  
draft-jabley-dnssec-trust-anchor-15**

**Abstract**

The root zone of the Domain Name System (DNS) has been 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 has used to distribute the DNSSEC trust anchors.

**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 January 9, 2017.

**Copyright Notice**

Copyright (c) 2016 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.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">2</a>
<a href="#">1.1.</a>	<a href="#">Definitions</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">IANA DNSSEC Root Zone Trust Anchor Formats and Semantics</a>	<a href="#">4</a>
<a href="#">2.1.</a>	<a href="#">Hashes in XML</a>	<a href="#">4</a>
<a href="#">2.1.1.</a>	<a href="#">XML Syntax</a>	<a href="#">4</a>
<a href="#">2.1.2.</a>	<a href="#">XML Semantics</a>	<a href="#">5</a>
<a href="#">2.1.3.</a>	<a href="#">Converting from XML to DS Records</a>	<a href="#">6</a>
<a href="#">2.1.4.</a>	<a href="#">XML Example</a>	<a href="#">7</a>
<a href="#">2.2.</a>	<a href="#">Certificates</a>	<a href="#">8</a>
<a href="#">2.3.</a>	<a href="#">Certificate Signing Requests</a>	<a href="#">9</a>
<a href="#">3.</a>	<a href="#">Root Zone Trust Anchor Retrieval</a>	<a href="#">9</a>
<a href="#">3.1.</a>	<a href="#">Retrieving Trust Anchors with HTTPS and HTTP</a>	<a href="#">9</a>
<a href="#">4.</a>	<a href="#">Accepting DNSSEC Trust Anchors</a>	<a href="#">10</a>
<a href="#">5.</a>	<a href="#">IANA Considerations</a>	<a href="#">11</a>
<a href="#">6.</a>	<a href="#">Security Considerations</a>	<a href="#">11</a>
<a href="#">7.</a>	<a href="#">Acknowledgements</a>	<a href="#">11</a>
<a href="#">8.</a>	<a href="#">References</a>	<a href="#">11</a>
<a href="#">8.1.</a>	<a href="#">Normative References</a>	<a href="#">11</a>
<a href="#">8.2.</a>	<a href="#">Informative References</a>	<a href="#">13</a>
<a href="#">Appendix A.</a>	<a href="#">Historical Note</a>	<a href="#">13</a>
<a href="#">Appendix B.</a>	<a href="#">About this Document</a>	<a href="#">13</a>
<a href="#">B.1.</a>	<a href="#">Discussion</a>	<a href="#">13</a>
	<a href="#">Authors' Addresses</a>	<a href="#">14</a>

## [1. Introduction](#)

The Domain Name System (DNS) is described in [[RFC1034](#)] and [[RFC1035](#)]. Security extensions to the DNS (DNSSEC) are described in [[RFC4033](#)], [[RFC4034](#)], [[RFC4035](#)], [[RFC4509](#)], [[RFC5155](#)] and [[RFC5702](#)].

A discussion of operational practices relating to DNSSEC can be found in [[RFC6781](#)].

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. A detailed description of corresponding key management practices can be found in [DPS], which can be retrieved from the IANA Repository at <<https://www.iana.org/dnssec/>>.

This document describes the formats and distribution methods of DNSSEC trust anchors that have been used by IANA for the root zone of the DNS since 2010. 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.

IMPORTANT NOTE: at the time of this writing, IANA intends to change the formats and distribution methods in the future. If such a change happens, IANA will publish the changes on its web site at <<https://www.iana.org/dnssec/files>>.

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 [RFC5011].

## **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 the basic idea, that trust is assumed and not derived, is common to all the common uses of the term "trust anchor".

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 DS RR can do so.



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 [[RFC2119](#)].

## **[2.](#) IANA DNSSEC Root Zone Trust Anchor Formats and Semantics**

IANA publishes trust anchors for the root zone in three formats:

- o an XML document that contains the hashes of the DNSKEY records
- o certificates in PKIX format [[RFC5280](#)] that contain DS records and the full public key of DNSKEY records
- o certificate signing requests (CSRs) in PKCS#10 format [[RFC2986](#)] that contain DS records and the full public key of DNSKEY records

These formats and the semantics associated with each are described in the rest of this section.

### **[2.1.](#) Hashes in XML**

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 Delegation Signer (DS) resource records from [[RFC4034](#)].

#### **[2.1.1.](#) XML Syntax**

A Relax NG Compact Schema for the documents used to publish trust anchors is given in Figure 1.



```
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 }
}
```

Figure 1

#### **2.1.2. 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 element in the TrustAnchor element is different than the id element 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 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 DNSKEY record in the zone defined in the Zone element.

The id attribute in the KeyDigest element is an opaque string that identifies the hash. Its value is used in the file names and URI of the other trust anchor formats. This is described in [Section 3.1](#). For example, if the value of the id attribute in the KeyDigest element is "Kjqmt7v", the URI for the CSR that is associated with this hash will be [<https://data.iana.org/root-anchors/Kjqmt7v.csr>](https://data.iana.org/root-anchors/Kjqmt7v.csr). Note that the id element in the KeyDigest element is different than the id element 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. Note that the KeyDigest element is optional; if it is not given, the trust anchor can be used until a KeyDigest element covering the same DNSKEY record but having a validUntil attribute is trusted by the relying party. Relying parties SHOULD NOT use a KeyDigest outside of the time range given in the validFrom and validUntil attributes.

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 signing algorithm identifier for the DNSKEY record represented in this KeyDigest.

The DigestType element in the KeyDigest element contains the 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.

### **[2.1.3](#). Converting from XML to DS Records**

The display format for the DS record that is the equivalent of a KeyDigest element can be constructed by marshaling the KeyTag, Algorithm, DigestType, and Digest elements. For example, assume that the TrustAnchor element contains:



```
<?xml version="1.0" encoding="UTF-8"?>
<TrustAnchor
  id="AD42165F-3B1A-4778-8F42-D34A1D41FD93"
  source="http://data.iana.org/root-anchors/root-anchors.xml">
<Zone>.</Zone>
<KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00">
<KeyTag>19036</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>
49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
</Digest>
</KeyDigest>
</TrustAnchor>
```

The DS record would be:

```
. IN DS 19036 8 2
    49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
```

#### [2.1.4.](#) XML Example

Figure 2 describes two fictitious trust anchors for the root zone.



```
<?xml version="1.0" encoding="UTF-8"?>

<TrustAnchor
  id="AD42165F-B099-4778-8F42-D34A1D41FD93"
  source="http://data.iana.org/root-anchors/root-anchors.xml">
  <Zone>.</Zone>
  <KeyDigest id="42"
    validFrom="2010-07-01T00:00:00-00:00"
    validUntil="2010-08-01T00:00:00-00:00">
    <KeyTag>34291</KeyTag>
    <Algorithm>5</Algorithm>
    <DigestType>1</DigestType>
    <Digest>c8cb3d7fe518835490af8029c23efbce6b6ef3e2</Digest>
  </KeyDigest>
  <KeyDigest id="53"
    validFrom="2010-08-01T00:00:00-00:00">
    <KeyTag>12345</KeyTag>
    <Algorithm>5</Algorithm>
    <DigestType>1</DigestType>
    <Digest>a3cf809dbdbc835716ba22bdc370d2efa50f21c7</Digest>
  </KeyDigest>
</TrustAnchor>
```

Figure 2

## 2.2. Certificates

Each public key that can be used as a trust anchor is represented as a certificate in PKIX format. Each certificate is signed by the ICANN certificate authority. The SubjectPublicKeyInfo in the certificate represents the public key of the KSK. The Subject field has the following attributes:

O: the string "ICANN".

OU: the string "IANA".

CN: the string "Root Zone KSK" followed by the time and date of key generation in the format specified in [RFC3339]. For example, a CN might be "Root Zone KSK 2010-06-16T21:19:24+00:00".

resourceRecord: a string in the presentation format of the Delegation Signer (DS) [RFC4034] resource record for the DNSSEC public key.

The "resourceRecord" attribute in the Subject is defined as follows:



```
ResourceRecord
{ iso(1) identified-organization(3) dod(6) internet(1) security(5)
  mechanisms(5) pkix(7) id-mod(0) id-mod-dns-resource-record(70) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

IMPORTS

caseIgnoreMatch FROM SelectedAttributeTypes
  { joint-iso-itu-t ds(5) module(1) selectedAttributeTypes(5) 4 }

;

iana OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
  dod(6) internet(1) private(4) enterprise(1) 1000 }

iana-dns OBJECT IDENTIFIER ::= { iana 53 }

resourceRecord ATTRIBUTE ::= {
  WITH SYNTAX IA5String
  EQUALITY MATCHING RULE caseIgnoreIA5Match
  ID iana-dns
}

END
```

### **2.3. Certificate Signing Requests**

Each public key that can be used as a trust anchor is represented as a certificate signing request (CSR) in PKCS#10 format. The SubjectPublicKeyInfo and Subject field are the same as for certificates (see [Section 2.2](#) above).

## **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 described in [Section 2.1](#) is [<https://data.iana.org/root-anchors/root-anchors.xml>](https://data.iana.org/root-anchors/root-anchors.xml).

The URL for retrieving the PKIX certificate described in [Section 2.2](#) is [<https://data.iana.org/root-anchors/KEYDIGEST-ID.crt>](https://data.iana.org/root-anchors/KEYDIGEST-ID.crt), with the string "KEYDIGEST-ID" replaced the "id" attribute from the KeyDigest element from the XML file, as described in [Section 2.1.2](#).

The URL for retrieving the CSR described in [Section 2.3](#) is [<https://data.iana.org/root-anchors/KEYDIGEST-ID.csr>](https://data.iana.org/root-anchors/KEYDIGEST-ID.csr), with the string "KEYDIGEST-ID" replaced the "id" attribute from the KeyDigest element from the XML file, as described in [Section 2.1.2](#).

#### **4. 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 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. It is also important to note that the ICANN CA cannot be used to verify the origin of the trust anchor in the CSR format.

The content and origin of the XML file can be verified using a digital signature on the file. IANA provides a detached CMS [[RFC5652](#)] signature that chains to the ICANN CA with the XML file. The URL for a detached CMS signature for the XML file is [<https://data.iana.org/root-anchors/root-anchors.p7s>](https://data.iana.org/root-anchors/root-anchors.p7s).

(IANA also provided a detached OpenPGP [[RFC4880](#)] signature as a second parallel verification mechanism for the first trust anchor publication, but has indicated that it will not use this parallel mechanism in the future.)

Another method IANA uses to help validator operators verify the content and origin of trust anchors they receive is to use the 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 Certificate Authority. 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.



## **5. IANA Considerations**

This document defines id-mod-dns-resource-record, value 70 (see [Section 2.2](#)), in the SMI Security for PKIX Module Identifier registry.

Beyond the IANA registry action above, this document makes no other requests and places no further restrictions on IANA.

## **6. 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, as an aid to the formats and retrieval methods described here being integrated usefully into user environments.

## **7. 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.

This document incorporates suggestions made by Alfred Hoenes, whose contributions are appreciated.

## **8. References**

### **8.1. Normative References**

- [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), DOI 10.17487/RFC1034, November 1987, <<http://www.rfc-editor.org/info/rfc1034>>.
- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<http://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, <<http://www.rfc-editor.org/info/rfc2119>>.



- [RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", [RFC 2986](#), DOI 10.17487/RFC2986, November 2000, <<http://www.rfc-editor.org/info/rfc2986>>.
- [RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", [RFC 3339](#), DOI 10.17487/RFC3339, July 2002, <<http://www.rfc-editor.org/info/rfc3339>>.
- [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, <<http://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, <<http://www.rfc-editor.org/info/rfc4034>>.
- [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", [RFC 4035](#), DOI 10.17487/RFC4035, March 2005, <<http://www.rfc-editor.org/info/rfc4035>>.
- [RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", [RFC 4509](#), DOI 10.17487/RFC4509, May 2006, <<http://www.rfc-editor.org/info/rfc4509>>.
- [RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, [RFC 5011](#), DOI 10.17487/RFC5011, September 2007, <<http://www.rfc-editor.org/info/rfc5011>>.
- [RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", [RFC 5155](#), DOI 10.17487/RFC5155, March 2008, <<http://www.rfc-editor.org/info/rfc5155>>.
- [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](#), DOI 10.17487/RFC5280, May 2008, <<http://www.rfc-editor.org/info/rfc5280>>.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, [RFC 5652](#), DOI 10.17487/RFC5652, September 2009, <<http://www.rfc-editor.org/info/rfc5652>>.



- [RFC5702] Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC", [RFC 5702](#), DOI 10.17487/RFC5702, October 2009, <<http://www.rfc-editor.org/info/rfc5702>>.
- [RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", [RFC 6781](#), DOI 10.17487/RFC6781, December 2012, <<http://www.rfc-editor.org/info/rfc6781>>.

## **[8.2. Informative References](#)**

- [DPS] Ljunggren, F., Okubo, T., Lamb, R., and J. Schlyter, "DNSSEC Practice Statement for the Root Zone KSK Operator", October 2010, <<https://www.iana.org/dnssec/icann-dps.txt>>.
- [RFC4880] Callas, J., Donnerhackle, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", [RFC 4880](#), DOI 10.17487/RFC4880, November 2007, <<http://www.rfc-editor.org/info/rfc4880>>.

## **[Appendix A. Historical Note](#)**

The first KSK for use in the root zone of the DNS was generated at a key ceremony at an 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.

## **[Appendix B. About this Document](#)**

[RFC Editor: please remove this section, including all subsections, prior to publication.]

### **[B.1. Discussion](#)**

This document is not the product of any IETF working group. However, communities interested in similar technical work can be found at the IETF in the DNSOP and DNSEXT working groups.

The team responsible for deployment of DNSSEC in the root zone can be reached at [rootsign@icann.org](mailto:rootsign@icann.org).

The authors also welcome feedback sent to them directly.





Authors' Addresses

Joe Abley  
Dyn, Inc.  
470 Moore Street  
London, ON N6C 2C2  
Canada

Phone: +1 519 670 9327  
Email: [jabley@dyn.com](mailto:jabley@dyn.com)

Jakob Schlyter  
Kirei AB

Email: [jakob@kirei.se](mailto:jakob@kirei.se)

Guillaume Bailey  
Independent

Email: [GuillaumeBailey@outlook.com](mailto:GuillaumeBailey@outlook.com)

Paul Hoffman  
ICANN

Email: [paul.hoffman@icann.org](mailto:paul.hoffman@icann.org)

