Network Working Group	J. Abley	
Internet-Draft	ICANN	
Intended status: Informational	J. Schlyter	
Expires: April 2, 2011	Kirei	
	September 29, 2010	

TOC

DNSSEC Trust Anchor Publication for the Root Zone
draft-jabley-dnssec-trust-anchor-00

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 how such trust anchors are published.

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 April 2, 2011.

Copyright Notice

Table of Contents

1. Introduction
2. Root Zone Trust Anchor Publication
    2.1. XML
    2.2. Certificate Signing Request (PKCS#10)
3. Root Zone Trust Anchor Retrieval
    3.1. HTTP
    3.2. HTTP Over TLS
    3.3. Signature Verification
4. IANA Considerations
5. Security Considerations
6. Acknowledgements
7. References
    7.1. Normative References
    7.2. Informative References

Appendix A. Trust Anchor Publication Document Schema
Appendix B. Example Signed Trust Anchor Set
Appendix C. ASN.1 for Delegation Signer Extension
Appendix D. Historical Note
Appendix E. About this Document
    E.1. Discussion
    E.2. Document History
        E.2.1. draft-jabley-dnssec-trust-anchor-00

§ Authors' Addresses

1. Introduction

TOC

The Domain Name System (DNS) is described in [RFC1034] (Mockapetris, P., “Domain names - concepts and facilities,” November 1987.) and [RFC1035] (Mockapetris, P., “Domain names - implementation and specification,” November 1987.). Security extensions to the DNS (DNSSEC) are described in [RFC4033] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.), [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” March 2005.) and [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” March 2005.).
A discussion of operational practices relating to DNSSEC can be found in [RFC4641] (Kolkman, O. and R. Gieben, “DNSSEC Operational Practices,” September 2006.).

In DNSSEC a secure response to a query is one which is cryptographically signed and validated. An individual signature is validated by following a chain of signatures to a key which is trusted for some extra-protocol reason.
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] (Ljunggren, F., Okubo, T., Lamb, R., and J. Schlyter, “DNSSEC Practice Statement for the Root Zone KSK Operator,” May 2010.), which can be retrieved from the IANA Repository located at https://www.iana.org/dnssec/.
This document describes the distribution of DNSSEC trust anchors. Whilst the data formats and the publication and retrieval methods described in this document might well be adapted for other uses, this document's focus is more specific and is concerned only with the distribution of trust anchors for the root zone.

---

2. Root Zone Trust Anchor Publication

TOC

Trust anchors for the root zone are published in two formats:

- as the hash of the corresponding DNSKEYs consistent with the defined presentation format of Delegation Signer (DS) resource records [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” March 2005.), contained within an XML document, as described in Section 2.1 (XML), and

- as Certificate Signing Requests (CSRs) in PKCS#10 format [RFC2986] (Nystrom, M. and B. Kaliski, “PKCS #10: Certification Request Syntax Specification Version 1.7,” November 2000.) for further processing by Certification Authorities and validation of proof of possession of the corresponding private keys, as described in Section 2.2 (Certificate Signing Request (PKCS#10)).

Both formats are described in this document.

2.1. XML

TOC

Trust anchors are published in an XML document whose schema is described in Appendix A (Trust Anchor Publication Document Schema). The document contains a complete set of trust anchors for the root zone, including anchors suitable for immediate use and also historical data.

Examples of trust anchors packaged and signed for publication can be found in Appendix B (Example Signed Trust Anchor Set).

2.2. Certificate Signing Request (PKCS#10)

TOC

To facilitate signing the trust anchor by a public key infrastructure, trust anchors are also published as Certificate Signing Requests (CSRs) in PKCS#10 format (Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7," November 2000.) [RFC2986]. Each CSR will have a Subject with 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] (Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps," July 2002.), e.g. "Root Zone KSK 2010-06-16T21:19:24+00:00".
>
> **resourceRecord:** the hash of the public key consistent with the presentation format of the Delegation Signer (DS) [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions," March 2005.) resource record (see Appendix C (ASN.1 for Delegation Signer Extension) for attribute definition).

---

3. Root Zone Trust Anchor Retrieval

TOC

3.1. HTTP

TOC

Trust anchors are available for retrieval using HTTP [RFC2616] (Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.).
The URL for retrieving the CSR is <http://data.iana.org/root-anchors/key-label.csr>, with "key-label" replaced by the key label of the corresponding KSK.

The URL for retrieving the IANA-signed Certificate is <http://data.iana.org/root-anchors/key-label.crt>, with "key-label" again replaced as described above.
The URL for retrieving the complete trust anchor set is http://data.iana.org/root-anchors/root-anchors.xml.
The URL for a detached S/MIME signature for the current trust anchor set is http://data.iana.org/root-anchors/root-anchors.p7s.
The URL for a detached OpenPGP [RFC4880] (Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format," November 2007.) signature for the current trust anchor set is http://data.iana.org/root-anchors/root-anchors.asc.

3.2. HTTP Over TLS

TOC

Trust anchors are available for retrieval using HTTP over TLS [RFC2818] (Rescorla, E., "HTTP Over TLS," May 2000.).
The URLs specified in Section 3.1 (HTTP) are also available using HTTPS. That is:
The URL for retrieving the CSR is <https://data.iana.org/root-anchors/key-label.csr>, with "key-label" replaced by the key label of the corresponding KSK.
The URL for retrieving the IANA-signed Certificate is <https://data.iana.org/root-anchors/key-label.crt>, with "key-label" again replaced as described above.
The URL for retrieving the complete trust anchor set is https://data.iana.org/root-anchors/root-anchors.xml.
The URL for a detached S/MIME signature for the complete trust anchor set is https://data.iana.org/root-anchors/root-anchors.p7s.
The URL for a detached OpenPGP [RFC4880] (Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format," November 2007.) signature for the current trust anchor set is https://data.iana.org/root-anchors/root-anchors.asc.

3.3. Signature Verification

TOC

The OpenPGP [RFC4880] (Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format," November 2007.) keys used to sign trust anchor documents carry signatures from personal keys of staff who are able to personally attest to their validity. Those staff members will continue to make their personal keys freely available for examination by third parties, e.g. by way of PGP key parties at operator and IETF meetings. In this fashion a diverse set of paths through the PGP web of trust will be maintained to the trust anchor PGP keys.

An OpenPGP keyring containing public keys pertinent to signature verification is published at http://data.iana.org/root-anchors/icann.pgp. The public keys on that keyring will also be distributed widely, e.g. to public PGP key servers.
Certificates used to create S/MIME signatures will be signed by a Certificate Authority (CA) administered by ICANN as the IANA functions operator and also optionally by well-known (e.g. WebTrust-certified) CAs to facilitate signature validation with widely-available X.509 trust anchors.

---

4. IANA Considerations

TOC

Key Signing Key (KSK) management for the root zone is an IANA function. This document describes an initial set of publication mechanisms for trust anchors related to that management. In the future, additional publication schemes may be also be made available, in which case they will be described in a new document which updates this one.
Existing mechanisms will not be deprecated without very strong technical justification.
This document contains information about an existing service, and has no IANA actions.

---

5. Security Considerations

TOC

This document describes how DNSSEC trust anchors for the root zone of the DNS are published. It is to be expected that many DNSSEC clients will only configure a single trust anchor to perform validation, and that the trust anchor they use will be that of the root zone. 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.

---

6. Acknowledgements

TOC

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.

---

7. References

TOC

7.1. Normative References

TOC

[RFC1034]	Mockapetris, P., “Domain names - concepts and facilities,” STD 13, RFC 1034, November 1987 (TXT).
[RFC1035]	Mockapetris, P., “Domain names - implementation and specification,” STD 13, RFC 1035, November 1987 (TXT).
[RFC2616]	Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1,” RFC 2616, June 1999 (TXT, PS, PDF, HTML, XML).
[RFC2818]	Rescorla, E., “HTTP Over TLS,” RFC 2818, May 2000 (TXT).
[RFC2986]	Nystrom, M. and B. Kaliski, “PKCS #10: Certification Request Syntax Specification Version 1.7,” RFC 2986, November 2000 (TXT).
[RFC3339]	Klyne, G., Ed. and C. Newman, “Date and Time on the Internet: Timestamps,” RFC 3339, July 2002 (TXT, HTML, XML).
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” RFC 4033, March 2005 (TXT).
[RFC4034]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” RFC 4034, March 2005 (TXT).
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” RFC 4035, March 2005 (TXT).
[RFC4641]	Kolkman, O. and R. Gieben, “DNSSEC Operational Practices,” RFC 4641, September 2006 (TXT).
[RFC4880]	Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, “OpenPGP Message Format,” RFC 4880, November 2007 (TXT).

7.2. Informative References

TOC

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

TOC

Appendix A. Trust Anchor Publication Document Schema

A Relax NG Compact Schema for the documents used to publish trust anchors can be found 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

Appendix B. Example Signed Trust Anchor Set

TOC

Figure 2 describes two trust anchors for the root zone such as might be retrieved using the URL https://data.iana.org/root-anchors/root-anchors.xml.

```
<?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

TOC

Appendix C. ASN.1 for Delegation Signer Extension

```
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
}
```

Appendix D. Historical Note

TOC

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 E. About this Document

TOC

[RFC Editor: please remove this section, including all subsections, prior to publication.]
This document, once published in the RFC series, is intended to provide a stable reference for DNS implementors and future document authors, and a clear specification that will aid effective and secure dissemination of DNSSEC trust anchors to the operators of DNSSEC validators.

TOC

E.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.
The authors also welcome feedback sent to them directly.

E.2. Document History

TOC

E.2.1. draft-jabley-dnssec-trust-anchor-00

TOC

This document is based on earlier documentation used within and published by the team responsible for DNSSEC deployment in the root zone. This is the first revision circulated with the intention of publication in the RFC series.

Authors' Addresses

TOC

	Joe Abley
	ICANN
	4676 Admiralty Way, Suite 330
	Marina del Rey, CA 90292
	US
Phone:	+1 519 670 9327
Email:	joe.abley@icann.org
	Jakob Schlyter
	Kirei AB
	P.O. Box 53204
	Goteborg SE-400 16
	Sweden
Email:	jakob@kirei.se