Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 19, 2015

J. Abley
Dyn, Inc.
J. Schlyter
Kirei
G. Bailey
Microsoft

October 16, 2014

DNSSEC Trust Anchor Publication for the Root Zone
draft-jabley-dnssec-trust-anchor-10

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 19, 2015.

Copyright Notice

Copyright (c) 2014 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

1. Introduction 2
2. Root Zone Trust Anchor Publication 3
2.1. XML 3
2.2. Certificate Signing Request (PKCS#10) 4
3. Root Zone Trust Anchor Retrieval 4
3.1. HTTP 4
3.2. HTTP Over TLS 5
3.3. Signature Verification 5
4. Implementation Considerations 6
4.1. HTTP Over TLS Transport 6
4.2. XML Validation 6
4.3. Trust Anchor Validation 7
5. IANA Considerations 7
6. Security Considerations 7
7. Acknowledgements 8
8. References 8
8.1. Normative References 8
8.2. Informative References 9
Appendix A. Trust Anchor Publication Document Schema 10
Appendix B. Example Signed Trust Anchor Set 11
Appendix C. ASN.1 Module for DNS Resource Record 12
Appendix D. Historical Note 12
Appendix E. About this Document 13
E.1. Discussion 13
E.2. Document History 13
E.2.1. draft-jabley-dnssec-trust-anchor-00 13
E.2.2. draft-jabley-dnssec-trust-anchor-01 13
E.2.3. draft-jabley-dnssec-trust-anchor-02 13
E.2.4. draft-jabley-dnssec-trust-anchor-04 13
E.2.5. draft-jabley-dnssec-trust-anchor-05 13
E.2.6. draft-jabley-dnssec-trust-anchor-06 14
E.2.7. draft-jabley-dnssec-trust-anchor-07 14
E.2.8. draft-jabley-dnssec-trust-anchor-10 14
Authors' Addresses 14

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. Signatures are validated by following a chain of signatures to a key called a "trust anchor". The reason for trusting such a key 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 [IANA-DNSSEC-INFO].

This document describes the distribution of the DNSSEC trust anchors from IANA. This document is concerned only with the distribution of trust anchors for the root zone, although the data formats and the publication and retrieval methods described here can be adapted for other uses.

The protocol described in this document is 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. The protocol described in this document allows a trust anchor to initially be established out-of-band, possibly relying on trusted out-of-band authorities. Thus, this document and [RFC5011] are complimentary protocols.

2. Root Zone Trust Anchor Publication

Trust anchors for the root zone are published in two formats, each of which is described in this document:

- as the hashes of the corresponding DNSKEY records, consistent with the defined presentation format of Delegation Signer (DS) resource records [RFC4034], contained within an XML document, as described in Section 2.1, and

- as Certificate Signing Requests (CSRs) in PKCS#10 format [RFC2986] for further processing by other entities such as Certification Authorities and validation of proof of possession of the corresponding private keys, as described in Section 2.2.

2.1. XML

Trust anchors are published in an XML document whose schema is described in Appendix A. The document contains a complete set of trust anchors for the root zone, including anchors suitable for immediate use and also historical data. Each trust anchor optionally includes one or more Certificate elements, with Uniform Resource Locators (URLs) for retrieving corresponding X.509 certificates.

Examples of trust anchors packaged and signed for publication can be found in Appendix B.

2.2. Certificate Signing Request (PKCS#10)

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 [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], 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] resource record (see Appendix C for attribute definition).

3. Root Zone Trust Anchor Retrieval

3.1. HTTP

Trust anchors are available for retrieval using HTTP [RFC2616].

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 a signed X.509 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 available from [TA-HTTP-XML].

The URL for a detached S/MIME [RFC5751] signature for the current trust anchor set, in XML format, is available from [TA-HTTP-SMIME].

The URL for a detached OpenPGP [RFC4880] signature for the current trust anchor set, in XML format, is available from [TA-HTTP-PGP].

3.2. HTTP Over TLS

Trust anchors are available for retrieval using HTTP over TLS [RFC2818].

The URLs specified in Section 3.1 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 a signed X.509 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 available from [TA-HTTPS-XML].

The URL for a detached S/MIME [RFC5751] signature for the current trust anchor set is available from [TA-HTTPS-SMIME].

The URL for a detached OpenPGP [RFC4880] signature for the current trust anchor set is available from [TA-HTTPS-PGP].

TLS sessions are authenticated with certificates presented from the server. No client certificate verification is performed. The certificate presented by the server is chosen such that it can be trusted using an X.509 trust anchor that is believed to be well-known, e.g. one that corresponds to a WebTrust-accredited Certificate Authority. Other TLS authentication mechanisms may be considered in the future.

3.3. Signature Verification

The OpenPGP [RFC4880] 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 [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 [RFC5751] signatures for the current trust anchor set, in XML format, are 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. Implementation Considerations

Note: This non-normative section gives suggestions for implementing root zone trust anchor retrieval.

Root trust anchor retrieval by the HTTP or HTTP over TLS transports has several implementation considerations to ensure robustness, usability and secure operation.

4.1. HTTP Over TLS Transport

The HTTP over TLS transport [RFC2818] is suggested instead of using the unencrypted HTTP transport [RFC2616] for implementations that use the XML-format root trust anchors, since the latter transport does not provide authentication. It is not suggested that implementations restrict certification path validation of the HTTP over TLS transport session to the current or historical certificate authorities used by the root trust anchor server, since doing so would reduce robustness of the implementation. It is suggested that the implementation configure the HTTP over TLS transport library to: validate the certification path against certificate revocation lists [RFC5280], and/or with the online certificate status protocol [RFC6960]; and reject self-signed certificates and certification paths that do not terminate in a trusted certificate authority.

Implementations can allow configuration of the URL used to retrieve the root trust anchor resources, but it is suggested that the default configuration use the URLs specified in Section 3.2.

4.2. XML Validation

Implementations may perform strict validation of the retrieved XML document against the XML schema; however, such an implementation would not be robust against future changes in the XML schema. It is suggested that the implementation perform "loose" validation, where unknown attributes and elements are ignored. This suggestion allows

for future additions to the XML schema without affecting existing implementations.

4.3. Trust Anchor Validation

The implementation can ignore trust anchors for which the Algorithm or DigestType elements refer to an unknown, or unsupported algorithm. Additionally, trust anchors for which the Algorithm or DigestType elements refer to a deprecated algorithm can be ignored, provided that this suggestion does not cause all trust anchors to be ignored. Further, note that these suggestions may not apply where an implementation shares trust anchors between many DNS validating resolvers, since the set of supported algorithms may vary between resolvers, and could possibly be disjoint.

The implementation can also ignore a trust anchor when the validUntil time, if present, is in the past. If the implementation also supports automated updates of trust anchors [RFC5011], it can ignore trust anchors where the current time subtracted from the validFrom time, if present, is greater than the add-hold down time [RFC5011] for the trust point.

The implementation can reject any trust anchor for a trust point other than the root zone.

5. IANA Considerations

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 also be made available, in which case they will be described in a new document that updates this one.

Existing mechanisms will not be deprecated without very strong technical justification.

This document serves as the reference for id-mod-dns-resource-record, value 70, in the SMI Security for PKIX Module Identifier registry.

6. Security Considerations

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 IANA-issued trust anchors to perform validation, and that the trust anchors they use will be those 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.

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 Paul Hoffman and Alfred Hoenes, whose contributions are appreciated.

8. References

8.1. Normative References

[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.

[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.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, November 2000.

[RFC3339] Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.

[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.

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, September 2007.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

[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.

[RFC5702] Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5702, October 2009.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, December 2012.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, June 2013.

8.2. Informative References

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

[IANA-DNSSEC-INFO] , "IANA DNSSEC Information", , <https://www.iana.org/dnssec/>.

[ICANN-PGP] , "ICANN PGP Keys", , <http://data.iana.org/root-anchors/icann.pgp>.

[TA-HTTP-PGP]
, "Root DNSSEC Trust Anchors (OpenPGP)", ,
<http://data.iana.org/root-anchors/root-anchors.asc>.

[TA-HTTP-SMIME]
, "Root DNSSEC Trust Anchors (S/MIME)", ,
<http://data.iana.org/root-anchors/root-anchors.p7s>.

[TA-HTTP-XML]
, "Root DNSSEC Trust Anchors (XML)", ,
<http://data.iana.org/root-anchors/root-anchors.xml>.

[TA-HTTPS-PGP]
, "Root DNSSEC Trust Anchors (OpenPGP)", , <https://
data.iana.org/root-anchors/root-anchors.asc>.

[TA-HTTPS-SMIME]
, "Root DNSSEC Trust Anchors (S/MIME)", , <https://
data.iana.org/root-anchors/root-anchors.p7s>.

[TA-HTTPS-XML]
, "Root DNSSEC Trust Anchors (XML)", , <https://
data.iana.org/root-anchors/root-anchors.xml>.

[root-anchors]
, "DNSSEC Trust Anchors", , <https://data.iana.org/root-
anchors/root-anchors.xml>.

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 },

        element Certificate {
                attribute source { xsd:string },
                empty
        }+
    }
```

Figure 1

Appendix B. Example Signed Trust Anchor Set

Figure 2 describes two trust anchors for the root zone such as might be retrieved from [root-anchors].

```
<?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>
        <Certificate
          source="http://data.iana.org/root-anchors/Kexample1.crt"/>
```

```
          <Certificate
            source="http://data.iana.org/root-anchors/Kexample2.crt"/>
      </KeyDigest>

   </TrustAnchor>
```

Figure 2

Appendix C. ASN.1 Module for DNS Resource Record

```
   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
```

Appendix D. 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 E. About this Document

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

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

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

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.

E.2.2. draft-jabley-dnssec-trust-anchor-01

Incorporated initial community suggestions. Editorial improvements. Allocate OID and clean up syntax of ASN.1 module.

E.2.3. draft-jabley-dnssec-trust-anchor-02

Draft expired.

E.2.4. draft-jabley-dnssec-trust-anchor-04

Added the optional <Certificate> element to the XML schema to provide a mechanism for locating external X.509 certificates relating to a particular key.

E.2.5. draft-jabley-dnssec-trust-anchor-05

Update author address.

E.2.6. draft-jabley-dnssec-trust-anchor-06

Update references.

E.2.7. draft-jabley-dnssec-trust-anchor-07

Minor changes based on review by Paul Hoffman.

E.2.8. draft-jabley-dnssec-trust-anchor-10

Incorporate additional suggestions by Paul Hoffman. Add consideration for OCSP to Implementation Considerations.

Authors' Addresses

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

Phone: +1 519 670 9327
Email: jabley@dyn.com

Jakob Schlyter
Kirei AB

Email: jakob@kirei.se

Guillaume Bailey
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Phone: +1 425 538 6153 x86153
Email: gubailey@microsoft.com