Storing Certificates in the Domain Name System (DNS)
------- ----------- -- --- ------ ---- ------ -----

Donald E. Eastlake 3rd, Olafur Gudmundsson

Status of This Document

This draft, file name draft-ietf-dnssec-certs-04.txt, is intended to
become a Proposed Standard RFC. Distribution of this document is
unlimited. Comments should be sent to the DNSSEC mailing list <dns-
security@tis.com> or to the authors.

This document is an Internet-Draft. Internet-Drafts are working
documents of the Internet Engineering Task Force (IETF), its areas,
and its working groups. Note that other groups may also distribute
working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six
months. Internet-Drafts may be updated, replaced, or obsoleted by
other documents at any time. It is not appropriate to use Internet-
Drafts as reference material or to cite them other than as a
``working draft'' or ``work in progress.''

To view the entire list of current Internet-Drafts, please check the
"1id-abstracts.txt" listing contained in the Internet-Drafts Shadow
Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern
Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific
Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

[changes from draft 2 to 3: update author info, add RFC 2119
reference, change dates, add IANA Considerations] [[changes from
draft 3 to 4: update author info, change dates, tweak IANA
Considerations including adding reference to RFC 2434, update URL
references [RFC 1738] to absolute URI references [RFC 2396], update
PGP references to new RFC 2440]]

Abstract

Cryptographic public key are frequently published and their
authenticity demonstrated by certificates. A CERT resource record
(RR) is defined so that such certificates and related certificate
revocation lists can be stored in the Domain Name System (DNS).

Table of Contents

1. **Introduction**

   Public keys are frequently published in the form of a certificate and
   their authenticity is commonly demonstrated by certificates and
   related certificate revocation lists (CRLs). A certificate is a
   binding, through a cryptographic digital signature, of a public key,
   a validity interval and/or conditions, and identity, authorization,
   or other information. A certificate revocation list is a list of
   certificates that are revoked, and incidental information, all signed
   by the signer (issuer) of the revoked certificates. Examples are
   X.509 certificates/CRLs in the X.500 directory system or PGP
   certificates/revocations used by PGP software.

   Section 2 below specifies a CERT resource record (RR) for the storage
   of certificates in the Domain Name System.

   Section 3 discusses appropriate owner names for CERT RRs.

   Sections 4, 5, and 6 below cover performance, IANA, and security
   considerations, respectively.

   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. **The CERT Resource Record**

   The CERT resource record (RR) has the structure given below. Its RR
   type code is 37.

```
                        1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |             type              |              key tag          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   algorithm   |                                               /
   +---------------+            certificate or CRL                 /
   /                                                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
```

   The type field is the certificate type as define in section 2.1
   below.

   The algorithm field has the same meaning as the algorithm field in
   KEY and SIG RRs [draft-ietf-dnssec-secext2-*.txt] except that a zero
   algorithm field indicates the algorithm is unknown to a secure DNS,
   which may simply be the result of the algorithm not having been

standardized for secure DNS.

D. Eastlake, O. Gudmundsson   [Page 3]

The key tag field is the 16 bit value computed for the key embedded in the certificate as specified in the DNSSEC Standard [draft-ietf-dnssec-secext2-*.txt]. This field is used as an efficiency measure to pick which CERT RRs may be applicable to a particular key. The key tag can be calculated for the key in question and then only CERT RRs with the same key tag need be examined. However, the key must always be transformed to the format it would have as the public key portion of a KEY RR before the key tag is computed. This is only possible if the key is applicable to an algorithm (and limits such as key size limits) defined for DNS security. If it is not, the algorithm field MUST BE zero and the tag field is meaningless and SHOULD BE zero.

2.1 Certificate Type Values

The following values are defined or reserved:

```
Value   Mnemonic   Certificate Type
-----   --------   ----------- ----
    0              reserved
    1    PKIX      X.509 as per PKIX
    2    SPKI      SPKI cert
    3    PGP       PGP cert
 4-252             available for IANA assignment
  253    URI       URI private
  254    OID       OID private
255-65534          available for IANA assignment
65535             reserved
```

The PKIX type is reserved to indicate an X.509 certificate conforming to the profile being defined by the IETF PKIX working group. The certificate section will start with a one byte unsigned OID length and then an X.500 OID indicating the nature of the remainder of the certificate section (see 2.3 below). (NOTE: X.509 certificates do not include their X.500 directory type designating OID as a prefix.)

The SPKI type is reserved to indicate a certificate formated as to be specified by the IETF SPKI working group.

The PGP type indicates a Pretty Good Privacy certificate as described in RFC 2440 and its extensions and successors.

The URI private type indicates a certificate format defined by an absolute URI. The certificate portion of the CERT RR MUST begin with a null terminated URI [RFC 2396] and the data after the null is the private format certificate itself. The URI SHOULD be such that a retrieval from it will lead to documentation on the format of the

certificate. Recognition of private certificate types need not be

based on URI equality but can use various forms of pattern matching
so that, for example, subtype or version information can also be
encoded into the URI.

The OID private type indicates a private format certificate specified
by a an ISO OID prefix. The certificate section will start with a
one byte unsigned OID length and then a BER encoded OID indicating
the nature of the remainder of the certificate section. This can be
an X.509 certificate format or some other format. X.509 certificates
that conform to the IETF PKIX profile SHOULD be indicated by the PKIX
type, not the OID private type. Recognition of private certificate
types need not be based on OID equality but can use various forms of
pattern matching such as OID prefix.

2.2 Text Representation of CERT RRs

The RDATA portion of a CERT RR has the type field as an unsigned
integer or as a mnemonic symbol as listed in section 2.1 above.

The key tag field is represented as an unsigned integer.

The algorithm field is represented as an unsigned integer or a
mnemonic symbol as listed in [draft-ietf-dnssec-secext2-*.txt].

The certificate / CRL portion is represented in base 64 and may be
divided up into any number of white space separated substrings, down
to single base 64 digits, which are concatenated to obtain the full
signature. These substrings can span lines using the standard
parenthesis.

Note that the certificate / CRL portion may have internal sub-fields
but these do not appear in the master file representation. For
example, with type 254, there will be an OID size, an OID, and then
the certificate / CRL proper. But only a single logical base 64
string will appear in the text representation.

2.3 X.509 OIDs

OIDs have been defined in connection with the X.500 directory for
user certificates, certification authority certificates, revocations
of certification authority, and revocations of user certificates.
The following table lists the OIDs, their BER encoding, and their
length prefixed hex format for use in CERT RRs:

```
        id-at-userCertificate
            = { joint-iso-ccitt(2) ds(5) at(4) 36 }
                == 0x 03 55 04 24
        id-at-cACertificate
            = { joint-iso-ccitt(2) ds(5) at(4) 37 }
                == 0x 03 55 04 25
        id-at-authorityRevocationList
            = { joint-iso-ccitt(2) ds(5) at(4) 38 }
                == 0x 03 55 04 26
        id-at-certificateRevocationList
            = { joint-iso-ccitt(2) ds(5) at(4) 39 }
                == 0x 03 55 04 27
```

3. Appropriate Owner Names for CERT RRs

It is recommended that certificate CERT RRs be stored under a domain
name related to their subject, i.e., the name of the entity intended
to control the private key corresponding to the public key being
certified. It is recommended that certificate revocation list CERT
RRs be stored under a domain name related to their issuer.

Following some of the guidelines below may result in the use in DNS
names of characters that require DNS quoting which is to use a
backslash followed by the octal representation of the ASCII code for
the character such as \000 for NULL.

3.1 X.509 CERT RR Names

Some X.509 versions permit multiple names to be associated with
subjects and issuers under "Subject Alternate Name" and "Issuer
Alternate Name". For example, x.509v3 has such Alternate Names with
an ASN.1 specification as follows:

```
    GeneralName ::= CHOICE {
        otherName                 [0] INSTANCE OF OTHER-NAME,
        rfc822Name                [1] IA5String,
        dNSName                   [2] IA5String,
        x400Address               [3] EXPLICIT OR-ADDRESS.&Type,
        directoryName             [4] EXPLICIT Name,
        ediPartyName              [5] EDIPartyName,
        uniformResourceIdentifier [6] IA5String,
        iPAddress                 [7] OCTET STRING,
        registeredID              [8] OBJECT IDENTIFIER
    }
```

The recommended locations of CERT storage are as follows, in priority

   order:

   (1) If a domain name is included in the identification in the
       certificate or CRL, that should be used.
   (2) If a domain name is not included but an IP address is included,
       then the translation of that IP address into the appropriate
       inverse domain name should be used.
   (3) If neither of the above it used but a URI containing a domain
       name is present, that domain name should be used.
   (4) If none of the above is included but a character string name is
       included, then it should be treated as described for PGP names in
       3.2 below.
   (5) If none of the above apply, then the distinguished name (DN)
       should be mapped into a domain name as specified in RFC 2247.

   Example 1: Assume that an X.509v3 certificate is issued to /CN=John
   Doe/DC=Doe/DC=com/DC=xy/O=Doe Inc/C=XY/ with Subject Alternative
   names of (a) string "John (the Man) Doe", (b) domain name john-
   doe.com, and (c) uri <https://www.secure.john-doe.com:8080/>. Then
   the storage locations recommended, in priority order, would be
       (1) john-doe.com,
       (2) www.secure.john-doe.com, and
       (3) Doe.com.xy.

   Example 2: Assume that an X.509v3 certificate is issued to /CN=James
   Hacker/L=Basingstoke/O=Widget Inc/C=GB/ with Subject Alternate names
   of (a) domain name widget.foo.example, (b) IPv4 address
   10.251.13.201, and (c) string "James Hacker
   <hacker@mail.widget.foo.example>". Then the storage locations
   recommended, in priority order, would be
       (1) widget.foo.example,
       (2) 201.13.251.10.in-addr.arpa, and
       (3) hacker.mail.widget.foo.example.

3.2 PGP CERT RR Names

   PGP signed keys (certificates) use a general character string User ID
   [RFC 2440]. However, it is recommended by PGP that such names include
   the RFC 822 email address of the party, as in "Leslie Example
   <Leslie@host.example>". If such a format is used, the CERT should be
   under the standard translation of the email address into a domain
   name, which would be leslie.host.example in this case. If no RFC 822
   name can be extracted from the string name no specific domain name is
   recommended.

4. Performance Considerations

Current Domain Name System (DNS) implementations are optimized for
small transfers, typically not more than 512 bytes including
overhead. While larger transfers will perform correctly and work is
underway to make larger transfers more efficient, it is still
advisable at this time to make every reasonable effort to minimize
the size of certificates stored within the DNS. Steps that can be
taken may include using the fewest possible optional or extensions
fields and using short field values for variable length fields that
must be included.

5. IANA Considerations

Certificate types 0x0000 through 0x00FF and 0xFF00 through 0xFFFF can
only be assigned by an IETF standards action [RFC 2434] (and this
document assigns 0x0001 through 0x0003 and 0x00FD and 0x00FE).
Certificate types 0x0100 through 0xFEFF are assigned through IETF
Consensus [RFC 2434] based on RFC documentation of the certificate
type. The availability of private types under 0x00FD and 0x00FE
should satisfy most requirements for proprietary or private types.

6. Security Considerations

By definition, certificates contain their own authenticating
signature. Thus it is reasonable to store certificates in non-secure
DNS zones or to retrieve certificates from DNS with DNS security
checking not implemented or deferred for efficiency. The results MAY
be trusted if the certificate chain is verified back to a known
trusted key and this conforms with the user's security policy.

Alternatively, if certificates are retrieved from a secure DNS zone
with DNS security checking enabled and are verified by DNS security,
the key within the retrieved certificate MAY be trusted without
verifying the certificate chain if this conforms with the user's
security policy.

CERT RRs are not used in connection with securing the DNS security
additions so there are no security considerations related to CERT RRs
and securing the DNS itself.

References

RFC 1034 - P. Mockapetris, "Domain Names - Concepts and Facilities", STD 13, November 1987.

RFC 1035 - P. Mockapetris, "Domain Names - Implementation and Specifications", STD 13, November 1987.

RFC 2119 - S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

RFC 2247 - S. Kille, M. Wahl, A. Grimstad, R. Huber, S. Sataluri, "Using Domains in LDAP/X.500 Distinguished Names", January 1998.

RFC 2396 - T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", August 1998.

RFC 2440 - J. Callas, L. Donnerhacke, H. Finney, R. Thayer, "OpenPGP Message Format", November 1998

RFC 2434 - T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", October 1998.

draft-ietf-dnssec-secext2-*.txt - D. Eastlake, "Domain Name System (DNS) Security Extensions".

Authors Addresses

    Donald E. Eastlake 3rd
    IBM
    65 Shindegan Hill Road
    RR#1
    Carmel, NY 10512 USA

    Telephone: +1-914-784-7913 (w)
                  +1-914-276-2668 (h)
    FAX: +1-914-784-3833 (w-fax)
    email: dee3@us.ibm.com

    Olafur Gudmundsson
    TIS Labs at Network Associates
    3060 Washington Rd, Route 97
    Glenwood MD 21738

    Telephone: +1 443-259-2389
    email: ogud@tis.com

Expiration and File Name

    This draft expires June 1999.

    Its file name is draft-ietf-dnssec-certs-04.txt.