Storing Certificates in the Domain Name System (DNS)
draft-josefsson/rfc2538bis-01

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of section 3 of RFC 3667. By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with RFC 3668.

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 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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on July 4, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

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).

More information on this document, including rfcdiff output, may be found at <http://josefsson.org/rfc2538bis/>.
Table of Contents

1. Introduction ............................................. 3
2. The CERT Resource Record .................................. 3
   2.1 Certificate Type Values ............................... 4
   2.2 Text Representation of CERT RRs ......................... 5
   2.3 X.509 OIDs ........................................ 5
3. Appropriate Owner Names for CERT RRs ....................... 6
   3.1 Content-based X.509 CERT RR Names ..................... 7
   3.2 Purpose-based X.509 CERT RR Names ..................... 8
   3.3 Content-based PGP CERT RR Names ....................... 8
   3.4 Purpose-based PGP CERT RR Names ....................... 9
4. Performance Considerations ................................ 9
5. IANA Considerations ................................... 9
6. Security Considerations ................................ 10
7. Open Issues ........................................ 10
8. Changes since RFC 2538 .................................. 10
   Author's Address ......................................... 12
A. Acknowledgements ................................... 12
9. References .......................................... 11
   9.1 Normative References .................................. 11
   9.2 Informative References ................................. 12
B. Copying conditions .................................. 12
   Intellectual Property and Copyright Statements ......... 13
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 OpenPGP certificates/revocations used by OpenPGP 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 [11].

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 1 1 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             type              |             key tag        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   algorithm   |                                               /
+---------------+            certificate or CRL                 /[algorithm]
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  type             | key tag             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  algorithm         |
+-+-+-+-+        certificate or CRL       /[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 DNSKEY and RRSIG RRs [10] 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 DNSSEC.
The key tag field is the 16 bit value computed for the key embedded in the certificate, using the RRSIG Key Tag Algorithm described in Appendix B of [10]. 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 DNSKEY 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:

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>Certificate Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>PKIX</td>
<td>X.509 as per PKIX</td>
</tr>
<tr>
<td>2</td>
<td>SPKI</td>
<td>SPKI certificate</td>
</tr>
<tr>
<td>3</td>
<td>PGP</td>
<td>OpenPGP packet</td>
</tr>
<tr>
<td>4-252</td>
<td>available for IANA assignment</td>
<td></td>
</tr>
<tr>
<td>253</td>
<td>URI</td>
<td>URI private</td>
</tr>
<tr>
<td>254</td>
<td>OID</td>
<td>OID private</td>
</tr>
<tr>
<td>255-65534</td>
<td>available for IANA assignment</td>
<td></td>
</tr>
<tr>
<td>65535</td>
<td>reserved</td>
<td></td>
</tr>
</tbody>
</table>

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 formatted as to be specified by the IETF SPKI working group.

The PGP type indicates an OpenPGP packet as described in [5] and its extensions and successors. Two uses are to transfer public key material and revocation signatures. The data is binary, and MUST NOT be encoded into an ASCII armor. An implementation SHOULD process transferable public keys as described in section 10.1 of [5], but it MAY handle additional OpenPGP packets.

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 [4] 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 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 decimal integer or as a mnemonic symbol as listed in section 2.1 above.

The key tag field is represented as an unsigned decimal integer.

The algorithm field is represented as an unsigned decimal integer or a mnemonic symbol as listed in [10].

The certificate / CRL portion is represented in base 64 [8] 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.

The choice of name under which CERT RRs are stored is important to clients that perform CERT queries. In some situations, the client may not know all information about the CERT RR object it wishes to retrieve. For example, a client may not know the subject name of an X.509 certificate, or the e-mail address of the owner of an OpenPGP key. Further, the client may only know the hostname of a service that uses X.509 certificates or the OpenPGP key id of an OpenPGP key.

This motivate describing two different owner name guidelines. We call the two rules content-based owner names and purpose-based owner names. A content-based owner name is derived from the content of the CERT RR data; for example the Subject field in an X.509 certificate or the User ID field in OpenPGP keys. A purpose-based owner name is selected to be a name that clients that wishes to retrieve CERT RRs knows; for example the host name of a X.509 protected service or a OpenPGP key id of an OpenPGP key. Note that in some situations, the content-based and purpose-based owner name can be the same; for example when a client look up keys based on e-mail addresses for incoming e-mail.

[Editorial note: Purpose-based owner name guidelines were introduced
in RFC 2538bis. Earlier, in RFC 2538, only content-based owner name guidelines were described. Implementation experience suggested that the content-based owner name guidelines were not generally applicable. It was realized that purpose-based owner name guidelines were required to use CERT RRs in some ways.]

3.1 Content-based 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 is 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 [3].

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,

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 Purpose-based X.509 CERT RR Names

It is difficult for clients that do not already posses a certificate to reconstruct the content-based owner name that should be used to retrieve the certificate. For this reason, purpose-based owner names are recommended in this section. Because purpose-based owner names by nature depend on the specific scenario, or purpose, for which the certificate will be used, there are more than one recommendation. The following table summarize the purpose-based X.509 CERT RR owner name guidelines.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Owner name</th>
</tr>
</thead>
<tbody>
<tr>
<td>S/MIME Certificate</td>
<td>Standard translation of RFC 822 email address. Example: A S/MIME certificate for &quot;<a href="mailto:postmaster@example.org">postmaster@example.org</a>&quot; will use a standard hostname translation of the owner name, i.e. &quot;postmaster.example.org&quot;.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Hostname of the SSL server.</td>
</tr>
<tr>
<td>IPSEC Certificate</td>
<td>Hostname of the IPSEC machine, and/or for the in-addr.arpa reverse lookup IP address.</td>
</tr>
<tr>
<td>CRLs</td>
<td>Hostname of the issuing CA.</td>
</tr>
</tbody>
</table>

3.3 Content-based PGP CERT RR Names

OpenPGP signed keys (certificates) use a general character string User ID [5]. However, it is recommended by PGP that such names include the RFC 2822 [7] 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 2822 name can be extracted from the string name no specific
domain name is recommended.

If a user has more than one email address, the CNAME type can be used to reduce the amount of data stored in the DNS. For example:

```
$ORIGIN example.org.
smith        IN CERT PGP 0 0 <OpenPGP binary>
john.smith   IN CNAME smith
js           IN CNAME smith
```

### 3.4 Purpose-based PGP CERT RR Names

Applications that receive an OpenPGP packet but do not know the email address of the sender will have difficulties guessing the correct owner name, and cannot use the content-based owner name guidelines. However, the OpenPGP packet typically contain the Key ID of the key. In these situations, it is recommended to use an owner name derived from the Key ID. For example:

```
$ORIGIN example.org.
F835EDA21E94B565716F  IN CERT PGP ...
B565716F              IN CNAME F835EDA21E94B565716F
```

As before, if the same key material is stored at several owner names, using CNAME can be used to avoid data duplication.

### 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 [6]. This document assigns 0x0001 through 0x0003 and 0x00FD and 0x00FE. Certificate types 0x0100 through 0xFEFF are assigned through IETF Consensus [6] 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.

7. Open Issues

1. How to handle PGP certificates larger than 64kb? In draft-josefsson-cert-openpgp I outline one approach, but it may not be the best one.

2. Whether to enforce owner name guidelines with SHOULD/MUST. From David Shaw (on OpenPGP): "One of the things that struck me when reading this draft is that while there are several suggested ways to name keys in DNS, there is no one canonical name as a SHOULD or MUST. I suggest that the key fingerprint be the canonical name, and all others be CNAMEs pointing to the fingerprint name.". From Sean P. Turner (on PKIX): "Should "recommended" be "RECOMMENDED" in the 1st and 2nd sentences?" referring to the text in section 3 that recommend appropriate owner names.

3. Should the document suggest use of both full fingerprints, 4/8 byte OpenPGP key id owner names? Perhaps only fingerprint version.

8. Changes since RFC 2538

1. Editorial changes to conform with new document requirements, including splitting reference section into two parts and updating references to point at latest versions.

2. Improve terminology. For example replace "PGP" with "OpenPGP", to align with RFC 2440.

3. In section 2.1, clarify that OpenPGP public key data are binary, not the ASCII armored format, and reference 10.1 in RFC 2440 on how to deal with OpenPGP keys, and acknowledge that implementations may handle additional packet types.
4. Clarify that integers in the representation format are decimal.
5. Replace KEY/SIG with DNSKEY/RRSIG etc, to align with DNSSECbis terminology.
6. Add examples that suggest use of CNAME to reduce bandwidth.
7. In section 3, add three paragraphs that discuss "content-based" vs "purpose-based" owner names. Add section 3.2 for purpose-based X.509 CERT owner names, and section 3.4 for purpose-based OpenPGP CERT owner names.

9. References

9.1 Normative References


9.2 Informative References


Author's Address

Simon Josefsson

EMail: simon@josefsson.org

Appendix A. Acknowledgements

The majority of this document is copied verbatim from RFC 2538, by Donald Eastlake 3rd and Olafur Gudmundsson.

The author wishes to thank David Shaw and Michael Graff for their contributions to the earlier work that motivated this revised document.

Florian Weimer suggested to clarify wording regarding what data can be stored in RRDATA portion of OpenPGP CERT RRs. Olivier Dubuisson confirmed that the X.509 OID were indeed correct.

Appendix B. Copying conditions

In addition to the IETF/ISOC copying conditions, the following statement grant third parties further rights to the parts of this document ("the work") that were written by Simon Josefsson.

Copyright (C) 2004, 2005 Simon Josefsson

Copying and distribution of the work, with or without modification, are permitted in any medium without royalty provided the copyright notice and this notice are preserved.
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.