OpenPGP data in the CERT RR
draft-josefsson-cert-openpgp

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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 February 3, 2003.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

This draft describes the decisions made in one pair of applications [4][5] that respectively serves and retrieve OpenPGP [3] Certificates and Revocation Signatures using the CERT Resources Record [2]. The intent is to provide a discussion on the kind of general updates needed to the CERT specification, and some suggested specific updates for the OpenPGP sub-type. It is offered in the hope that this specification, together with similar efforts for other applications, can be reviewed when designing a generic solution or guidelines for storing application keying material in the Domain Name System (DNS), should it ever happen.
Table of Contents

1. Introduction ............................................. 3
2. Owner name guidelines .................................. 4
  2.1 OpenPGP Key ID Based RR Owner Name .................. 4
  2.2 E-mail Based RR Owner Name .......................... 4
3. CERT PGP RDATA Clarification ........................... 5
4. Handling OpenPGP data exceeding 64 kilobytes ............ 5
5. Improved Key Tag and Algorithm Field Usage ............... 6
6. CERT Sub-type for OpenPGP Key Revocation Signatures .... 6
7. Security Considerations .................................. 7
8. IANA Considerations ................................. 7
    References ......................................... 7
    Author's Address ................................. 8
    Full Copyright Statement .......................... 9
1. Introduction

OpenPGP data (e.g., certificates and revocation signatures) are sometimes distributed using so-called "key servers". Traditionally, key servers use protocols such as HTTP/HTML or HKP. This document explores in detail how the Domain Name System (DNS) protocol is used for OpenPGP data distribution. It is currently implemented in a prototype server (CKS-DNS [4]) and a prototype client (GPGKEYS-JKP [5]).

This specification uses the CERT resource record [2] to store OpenPGP certificates and revocation signatures. OpenPGP certificates are stored using the type "PGP" (value 3) CERT field. OpenPGP revocation signatures are stored using the type "OpenPGPrevocation" (value TBD) CERT field. The key tag and algorithm fields are set to 0, although an (unimplemented) approach utilizing these fields better is discussed below. As the CERT specification is unclear on the exact format of the RDATA field, this document clarifies it to be the binary OpenPGP format (as opposed to the ASCII armored format, which includes an additional CRC-24 checksum). Two owner name formats are discussed, one being the 4 byte hex OpenPGP Key ID used when the data is stored on third-party key servers, and the other being the e-mail address translated into a domain name (similar to SOA resource records), used when the data is stored on a server controlled by the OpenPGP data owner.

Briefly, some advantages of storing OpenPGP data in DNS rather than in existing systems are listed below. This is not a conclusive list, nor are these features strictly unique for DNS. However, we are not aware of implementations of these features in other OpenPGP key server protocols, hence they are currently unique to the DNS approach.

- End-users or their administrators can be in full control over their own key data, rather than relying on third-party servers.

- Data can be stored on several servers, providing seamless and well-understood fail-over.

- Data can be cached closer to clients, reducing bandwidth, increasing response times and improving resistance to temporary network or hardware problems.

- Sometimes DNS resolvers perform geographical optimizations, e.g., locates the closest server using IP round trip measurements.
2. Owner name guidelines

The CERT specification has the following owner name guideline:

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.

When seen from the point of view of a client looking at an OpenPGP message and needing the OpenPGP key to verify it, this owner name recommendation is not useful as a client in general do not know the User ID of the OpenPGP Certificate unless she already possess the certificate. However, a client can extract the Key ID from the OpenPGP message. Thus, instead we define a owner name recommendation based on the Key ID in the next sub-section. When used in a Internet E-mail environment, a client may be able to extract From: lines from the RFC 2822 message wrapping the OpenPGP message. In this case, the original owner name recommendation do make some sense, although we clarify some issues related to multiple User ID Packets in the sub-section after the next sub-section.

2.1 OpenPGP Key ID Based RR Owner Name

The Key ID owner name format is usually used in a situation where a party is serving keys on behalf of someone else. This is usually a big server containing lots of keys, used by many clients. The owner name should be the 4 byte OpenPGP Key ID prepended with "0x" (sans quotes) appended to the system's zone. An example:

0x789ABCDE.dnskeys.example.org. IN CERT PGP 0 0 <OpenPGP binary>

2.2 E-mail Based RR Owner Name

The E-mail based RR Owner name format is usually used in a situation where the OpenPGP data owner is publishing her own data. Its most common use would be when OpenPGP is used in the Internet E-mail environment, where the client is expected to have the e-mail address (extracted from the From: header). Thus the OpenPGP data should be published under the standard translation of the e-mail address(es) used in the RFC 2822 envelope of OpenPGP messages. A secondary use may be to publish OpenPGP Key Revocation Signatures for revoked OpenPGP Certificates, in this case the owner name should be the
standard translation of the email address found in the User ID packet(s). An example:

smith.example.org. IN CERT PGP 0 0 <OpenPGP binary>
john.smith.example.org. IN CNAME smith.example.org.

3. CERT PGP RDATA Clarification

The CERT specification says this regarding the RDATA of CERT RR's of the "PGP" type:

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

Ideally, the terms PGP and Pretty Good Privacy certificates should not be used, and should be replaced by "OpenPGP" and "OpenPGP data".

More seriously though, is that it is not clear exactly what data format is intended. The OpenPGP specification contains two data format, one binary and one ASCII armored. Although the ASCII armored version offers a CRC-24 checksum of the data, that the binary version doesn't, we felt IP/UDP or IP/TCP checksum are sufficient. Therefore we specify that the RDATA portion of an CERT RR of the PGP type (value 3) should contain binary OpenPGP data, as defined in RFC 2440 and its extensions and successors. Note that this redefinition intentionally includes other data than certificates.

4. Handling OpenPGP data exceeding 64 kilobytes

RDATA fields are ultimately limited in size, by a 16 bit RDLENGTH field, to 65535 bytes. As OpenPGP certificates and other OpenPGP data can exceed this limit, a method to overcome this is needed.

Whenever OpenPGP data do not fit into one 65535 byte RDATA field, the excess data should be stored in another CERT RR with the owner name appended with "-2" (sans quotes). If data do not fit these two RR's, a third is created with "-3" appended instead of "-2", and so on until all of the OpenPGP data is stored.

A client receiving a CERT RR with OpenPGP data should thus send another query, appending "-2" to the owner name, and append the data in the second RDATA to the RDATA in the first response, should the first response contain an RDLENGTH of 65535. Should the second RDATA also be of length 65535, the client needs to try one more time with "-3" instead of "-2" in the owner name, and so on until it receives a RR with size less than 65535 or receives a NXDOMAIN (in which case the client should assume that the entire OpenPGP data has already
An ASCII representation of a DNS zone file containing three large (defined as exceeding 65535 bytes) OpenPGP data records may look like:

0xDEADBEEF.example.org. IN CERT PGP 0 0 <RDATA of size 65535>
0xDEADBEEF-2.example.org. IN CERT PGP 0 0 <RDATA of size less than 65535>
0xCAFEBABE.example.org. IN CERT PGP 0 0 <RDATA of size 65535>
0xCAFEBABE-2.example.org. IN CERT PGP 0 0 <RDATA of size 65535>
0xCAFEBABE-3.example.org. IN CERT PGP 0 0 <RDATA of size less than 65535>
0xABBAD00D.example.org. IN CERT PGP 0 0 <RDATA of size 65535>
0xABBAD00D-2.example.org. IN CERT PGP 0 0 <RDATA of size 65535>

5. Improved Key Tag and Algorithm Field Usage

In cases where a person with multiple OpenPGP Certificates is publishing her OpenPGP data herself (i.e., published under a "smith.example.org." owner name, rather than a Key Id based owner name), clients must parse all OpenPGP data to find the wanted OpenPGP data. The CERT Key Tag field was added to enable optimizations in this situation. To be useful by a OpenPGP implementation faced with an OpenPGP message and wanting to locate the proper OpenPGP certificate, the Key Tag should equal the Key ID, although truncated to 16 bits.

This document suggest that a new Algorithm "OpenPGPKeyID" with value TBA is allocated that indicates that the value stored in the Key Tag is computed as defined in RFC 2440 for Key IDs, and then truncated to 16 bits to fit the CERT Key Tag field. Algorithms and Key Tags are discussed and defined in [2], but used by CERT as well.

susan.example.org. IN CERT PGP 4711 TBA <OpenPGP cert with Key ID 4711...>
susan.example.org. IN CERT PGP 1717 TBA <OpenPGP cert with Key ID 1717...>

6. CERT Sub-type for OpenPGP Key Revocation Signatures

This section contains an experimental proposal, it may be removed if it turns out it does not provide substantial advantages.

When OpenPGP Certificates are revoked, a small data structure called a Key Revocation Signature is created. To be able to locate this structure efficiently, we propose that it should be stored under a
separate CERT type with mnemonic "OpenPGPrevocation" and value TBA.

Open issue: The point in storing revocation signatures separately is that they are small, and would fit into a UDP packet, making for more efficient retrieval. However, if the same RRset contains data with other CERT sub-types, the packet overflow and the advantage is spoiled. It may thus make sense to create a new RR for this purpose.

7. Security Considerations

This draft discusses operational considerations for existing technology, and as such the security consideration of the technology used (DNS, OpenPGP) must be followed. The purpose of the operational considerations themselves are intended to ease deployment of OpenPGP in e-mail for the Internet, but are not itself expected to have any separate security consequences.

The draft do suggest some clarifications to the CERT resource record specification. These are merely intended to make the original specification non-ambiguous, it does not modify any security properties.

8. IANA Considerations

The IANA is asked to register a new CERT RR sub-type with mnemonic "OpenPGPrevocation" and a newly allocated value, for storing OpenPGP Key Revocation Signatures as defined in RFC 2440 and this document.

The IANA is asked to register a new CERT Algorithm with mnemonic "OpenPGPKeyID" and a newly allocated value for the OpenPGP Key ID computation algorithm as defined in [3], but truncated to 16 bits.

Acknowledgments

I'd like to thank David Shaw and Michael Graff for commenting and raising issues related to this work.

References


josefsson.org/cks-dns/", August 2002.


Author's Address

Simon Josefsson
Extundo
Drottningholmsvägen 70
Stockholm 112 42
Sweden

Phone: +46 8 6190422
EMail: simon@josefsson.org
Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgement

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