Network Working Group
Internet-Draft
Expires: May 11, 2002

J. Schlyter
Carlstedt Research & Technology
S. Josefsson
RSA Security
R. Arends
Nominum

November 10, 2001

Storing certificates in DNS for email applications
draft-schlyter-mailcert-dns-00.txt

Status of this Memo

Copyright Notice

Abstract

The Domain Name System (DNS) can be used to store certificates used to identify mail addresses. This document describes on how to name these certificates when stored in DNS. This document updates RFC 2538.

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 RFC 2119 [2].

Table of Contents

1. Introduction

RFC 2538 [5] section 3.1 describes how to translate X.509 subject and issuer names and into a domain name. The translation used is a fairly complicated set of recommendations to use in priority order depending on what is available in the X.509 certificate.

RFC 2538 section 3.2 describes how to translate a general character string PGP User ID, as defined in RFC 2440 [3], that includes a RFC 2822 [6] email address into a domain name. The translation used is the standard translation of an email address into a domain name.

Using the translations described in RFC 2538 has several disadvantages. We explore these disadvantages in section 2 and propose a new representation in section 3.

2. Problems with the current representation

2.1 Name collisions

When the standard translation, as specified in RFC 2538 [5] 3.2 is used, translated mailbox names, as specified in RFC 2822 [6], may collide with hostnames and/or other mailboxes.

For example <Leslie.Example@example.com> translated to label "leslie.example.example.com" collides with the translated mailbox <Leslie@example.example.com> as this would translate to the equal label. Another example is <hostmaster@example.com> that would collide with the host called "hostmaster.example.com".

2.2 No automatic locating of PKI material of entities

The RFC 2538 [5] X.509 owner name guidelines is not adequate because they focus on the content of a certificate to determine how it should be stored. This imposes a dilemma for a third party that wishes to locate a certificate for an remote entity (e.g. identified with an mail address) - they need to know parts of the certificate they want to retrieve. In email applications the parties can in general only be assumed to know a limited set of information about the other entity. Such as the mail address. They do not know apriori the X.509 DN of the remote entity.

When the RFC 2538 owner names for X.509 certificates are used, clients that only knows e.g. the email address of a certificate owner cannot infer the DNS name where the certificate is used.

For example, when the certificate for <Leslie.Example@example.com> is stored in DNS the owner name depends on what the certificate

contains. For instance if the users's URI is present in the certificate the owner name for the certificate should, according to the RFC 2538 rules, be the domain name in the URI. A mail client that only knows the email address but not the URI cannot infer the domain name used.

2.3 Administrative boundaries

3. Proposed representation

As we have seen, the DNS "owner name" guidelines described in RFC 2538 has several flaws. They also do not make the owner name guidelines mandatory, which would be a advantage for interoperable secure email. Below we specify a scheme for applications that use RFC 2822 addresses to identify identities, such as Internet Mail and the UseNet News.

N.B., the RFC 2538 guideliness MAY still be used in addition to the owner names specified here. One of the owner names MAY be CNAMEs to the other.

3.1 Algorithm to convert RFC 2822 address to domain name

To encode a RFC 2822 "addr-spec" into the string used to a DNS domain name as represented in zone files, the "local-part" is appended with "._mail." and concatenated with the "domain" part.

```
;; INPUT (from RFC 2882 EBNF):
addr-spec       =       local-part "@" domain

;; OUTPUT (domain name for DNS zone file):
local-part._mail.domain.
```

3.2 Case handling

Even though the local-part of a mail address may be case sensitive in theory, the address SHOULD be converted to lower case before use.

3.3 Examples

A certificate for <leslie@example.com> is stored at leslie._mail.example.com.

A certificate for <firstname.lastname@example.com> is stored at firstname.lastname._mail.example.com.

4. Security Considerations

Since certificates are digitally signed, no additional integrity service is necessary. Certificates do not need to be kept secret, and anonymous access to certificates is generally acceptable, thus no privacy service is necessary. However, clients that retrieve CRLs without some way of verifying the server run the risk of being sent a still current but superceded CRL.

Operators of DNS servers should authenticate end entities, CAs and RAs who publish certificates. However, authentication is not necessary to retrieve certificates.

When a zone is signed and published using the DNS security extensions, it is feasible to traverse a zone by NXT-chaining to collect mailboxes. This may not be desired. One solution might be to store the certificates as unsigned RRsets [7] or use a hashed alternative to the NXT chain [8].

References

[1] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Callas, J., Donnerhacke, L., Finney, H. and R. Thayer, "OpenPGP Message Format", RFC 2440, November 1998.

[4] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[5] Eastlake, D. and O. Gudmundsson, "Storing Certificates in the Domain Name System (DNS)", RFC 2538, March 1999.

[6] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[7] Arends, R., Kosters, M. and D. Blacka, "DNSSEC Opt-In", work in progress draft-ietf-dnsext-dnssec-opt-in-01, November 2001.

[8] Josefsson, S., "Authenticating denial of existence in DNS with minimum disclosure", work in progress draft-ietf-dnsext-not-existing-rr-01, November 2000.

Authors' Addresses

Jakob Schlyter
Carlstedt Research & Technology
Stora Badhusgatan 18-20
Goteborg SE-411 21
Sweden

EMail: jakob@crt.se
URI: http://www.crt.se/~jakob/

Simon Josefsson
RSA Security
Arenavagen 29
Stockholm SE-121 29
Sweden

Phone: +46 8 725 09 14
EMail: sjosefsson@rsasecurity.com

Roy Arends
Nominum
1e Atjehstraat 174-2
Amsterdam 1094 KX
The Netherlands

EMail: roy.arends@nominum.com
URI: http://www.nominum.com/

Appendix A. Acknowledgements

The authors gratefully acknowledges, in no particular order, the contributions of the following persons:

Mats Dufberg

Olafur Gudmundsson

Dan Massey

Full Copyright Statement

Acknowledgement

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