Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 4, 2011

P. Hoffman
VPN Consortium
J. Schlyter
Kirei AB

March 3, 2011

Using Secure DNS to Associate Certificates with Domain Names For S/MIME
draft-hoffman-dane-smime-00

Abstract

S/MIME uses certificates for authenticating and encrypting messages. Users want their mail user agents to securely associate a certificate with the sender of an encrypted and/or signed message. DNSSEC provides a mechanism for a zone operator to sign DNS information directly. This way, bindings of certificates to users within a domain are asserted not by external entities, but by the entities that operate the DNS. This document describes how to use secure DNS to associate an S/MIME user's certificate with the the intended domain name.

IMPORTANT NOTE: This draft is intentionally sketchy. It is meant as a possible starting point for the DANE WG if it wants to consider making a protocol similar to TLSA, as described in draft-ietf-dane-protocol, but that applies to S/MIME. The WG may or may not want to adopt such work, or if it does, may want to use a very different scheme from the one described here.

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 September 4, 2011.

Copyright Notice

Table of Contents

1. Introduction

S/MIME [RFC5751] messages often contain a certificate. This certificate assists in authenticating the sender of the message and can be used for encrypting messages that will be sent in reply. In order for the S/MIME receiver to authenticate that a message is from the sender whom is identified in the message the receiver's mail user agent (MUA) must validate that this certificate is associated with the purported sender. Currently, the MUA must trust a trust anchor upon which the sender's certificate is rooted, and must successfully validate the certificate.

Some people want a different way to authenticate the association of the sender's certificate with the sender without trusting the CA. Given that the DNS administrator for a domain name is authorized to give identifying information about the zone, it makes sense to allow that administrator to also make an authoritative binding between email messages purporting to come from the domain name and a certificate that might be used by someone authorized to send mail from those servers. The easiest way to do this is to use the DNS.

[[More here about additional uses, such as CMS that is not S/MIME where the certificates have email addresses for the subject name.]]

1.1. Certificate Associations

In this document, a certificate association is based on a cryptographic hash of a certificate (sometimes called a "fingerprint") or on the certificate itself. For a fingerprint, a hash is taken of the binary, DER-encoded certificate, and that hash is the certificate association; the type of hash function used can be chosen by the DNS administrator. When using the certificate itself in the certificate association, the entire certificate in the normal format is used. This document also only applies to PKIX [RFC5280] certificates.

Certificate associations are made between a certificate or the hash of a certificate and an email address (sometimes called an "RFC 822 address" or a variation of that term). A DNS query can return multiple certificate associations, such as in the case of a mail user who is changing from one certificate to another.

1.2. Securing Certificate Associations

This document defines a secure method to associate the certificate that is in an S/MIME email message (or was received in some similar fashion) with a domain name using DNS protected by DNSSEC. Because the certificate association was retrieved based on a DNS query, the

domain name in the query is by definition associated with the certificate.

DNSSEC, which is defined in RFCs 4033, 4034, and 4035 ([RFC4033], [RFC4034], and [RFC4035]), uses cryptographic keys and digital signatures to provide authentication of DNS data. Information retrieved from the DNS and that is validated using DNSSEC is thereby proved to be the authoritative data. The DNSSEC signature MUST be validated on all responses in order to assure the proof of origin of the data.

This document only relates to securely getting the DNS information for the certificate association using DNSSEC; other secure DNS mechanisms are out of scope.

1.3. Terminology

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 [RFC2119].

A note on terminology: Some people have said that this protocol is a form of "certificate exclusion". This is true, but in a very unusual sense. That is, a DNS reply that contains two of the certificate types defined here inherently excludes every other possible certificate in the universe other than those found with a pre-image attack against one of those two. The certificate type defined here is better thought of as "enumeration" of a small number of certificate associations, not "exclusion" of a near-infinite number of other certificates.

Some of the terminology in this draft may not match with the terminology used in RFC 5280. This will be fixed in future versions of this draft, with help from the PKIX community. In specific, we need to say (in a PKIX-appropriate way) that when we say "valid up to" and "chains to", full RFC 5280 path processing including revocation status checking is intended.

2. Getting S/MIME Certificate Associations from the DNS

This document defines a new DNS resource record type, "SMIMEA". A query on a prepared domain name for the SMIMEA RR can return one or more records of the type SMIMEA. The SMIMEA RRType is TBD.

2.1. Requested Domain Name

Domain names are prepared for requests in the following manner.

1. The user name (the "left-hand side" of the email address, called the "local-part" in RFC 2822 [RFC2822]) becomes the left-most label in the prepared domain name. This does not include the "@" character that separates the left and right sides of the email address.

2. The string "_smimecert" becomes the second left-most label in the prepared domain name.

3. The domain name (the "right-hand side" of the email address, called the "domain" in RFC 2822) is appended to the result of step 2 to complete the prepared domain name.

For example, to request a SMIMEA resource record for a user whose address is "chris@example.com", you would use "chris._smimecert.example.com" in the request.

[[Need to discuss back-quoting, such as for chris.smith@example.com becoming chris\.smith._smimecert.example.com]]

2.2. Format of the Resource Record

[[This will be the same as for TLSA because there is no reason for the two to diverge. Lots of text lifted from the TLSA document.]]

2.3. Making Certificate Associations

[[Stuff here that sounds like TLSA but is actually about S/MIME senders and receivers. Lots of text lifted from the TLSA document.]]

2.4. Presentation Format

The RDATA of the presentation format of the SMIMEA resource record consists of two numbers (certificate and hash type) followed by the bytes containing the certificate or the hash of the associated certificate itself, presented in hex. An example of a SHA-256 hash (type 2) of an end-entity certificate (type 1) would be:

```
chris._smimecert.example.com. IN SMIMEA (
   1 2 5c1502a6549c423be0a0aa9d9a16904de5ef0f5c98
       c735fcca79f09230aa7141 )
```

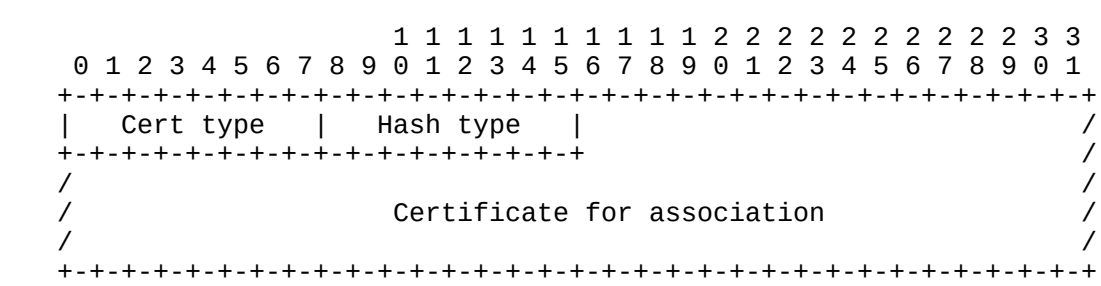
An example of an unhashed CA certificate (type 2) would be:

```
chris._smimecert.example.com. IN SMIMEA (
   2 0 308202c5308201ada00302010202090... )
```

Because the length of hashes and certificates can be quite long, presentation format explicitly allows line breaks and white space in the hex values; those characters are removed when converting to the wire format.

2.5. Wire Format

The wire format is:



The wire format for the RDATA in the first example given above would be:

```
chris._smimecert.example.com. IN TYPE65534 \# 34 ( 01025c1502a6549c42
             3be0a0aa9d9a16904de5ef0f5c98c735fcca79f09230aa7141 )
```

The wire format for the RDATA in the second example given above would be:

```
chris._smimecert.example.com. IN TYPE65534 \# 715 0200308202c5308...
```

Note that in the preceding examples, "TYPE65534" is given as an example. That RR Type is in the IANA "private use" range; the real RR Type for SMIMEA will be issued by IANA, as described in the IANA Considerations section below.

3. Use of S/MIME Certificate Associations in S/MIME

[[Stuff here that sounds like TLSA but is actually about S/MIME senders and receivers. Lots of text lifted from the TLSA document.]]

4. IANA Considerations

[[Mostly copied from TLSA but using "SMIMEA" instead.]]

5. Security Considerations

[[Stuff here that sounds like TLSA but is actually about S/MIME senders and receivers. Lots of text lifted from the TLSA document, but with some significant differences.]]

6. Acknowledgements

Many of the ideas in this document have been discussed over many years. More recently, the ideas have been discussed by the authors and others in a more focused fashion. In particular, some of the ideas here originated with Paul Vixie, Dan Kaminsky, Jeff Hodges, Phill Hallam-Baker, Simon Josefsson, Warren Kumari, Adam Langley, Ilari Liusvaara, Scott Schmit, and Ondrej Sury.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[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.

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

Specification", RFC 5751, January 2010.

7.2. Informative References

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

Authors' Addresses

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org

Jakob Schlyter
Kirei AB

Email: jakob@kirei.se