Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2012

P. Hoffman
VPN Consortium
J. Schlyter
Kirei AB

March 9, 2012

Using Secure DNS to Associate Certificates with Domain Names For S/MIME

draft-hoffman-dane-smime-03

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 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 10, 2012.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Certificate Associations 3
1.2. Securing Certificate Associations 3
1.3. Terminology 3
2. The SMIMEA Resource Record 3
3. TLSA RDATA Wire Format 4
4. TLSA RR Presentation Format 4
5. TLSA RR Examples 4
6. Domain Names for S/MIME Certificate Associations 4
7. Use of S/MIME Certificate Associations in S/MIME 5
8. Mandatory-to-Implement Features 5
9. IANA Considerations 5
10. Security Considerations 5
11. Acknowledgements 5
12. References 5
12.1. Normative References 5
12.2. Informative References 6
Authors' Addresses 6

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 a 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

[[Will mostly duplicate the text from Section 1.1 of draft-ietf-dane-protocol]]

1.2. Securing Certificate Associations

[[Will mostly duplicate the text from Section 1.2 of draft-ietf-dane-protocol]]

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].

This document also makes use of standard PKIX, DNSSEC, and S/MIME terminology. See [RFC5280], [RFC4033], [RFC4034], [RFC4035], and [RFC5751] respectively, for these terms.

2. The SMIMEA Resource Record

[[Mostly copied from draft-ietf-dane-protocol, but will define

"SMIMEA" instead of "TLSA".]]

3. TLSA RDATA Wire Format

[[Mostly copied from draft-ietf-dane-protocol.]]

4. TLSA RR Presentation Format

[[Mostly copied from draft-ietf-dane-protocol]]

5. TLSA RR Examples

[[Similar in format to draft-ietf-dane-protocol, but with very different examples, of course.]]

6. Domain Names for S/MIME Certificate Associations

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 [RFC2822] and the "local part" in [RFC6530]), is encoded with Base32 [RFC4648], to become 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 [RFC2822]) 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 "MNUHE2LT._smimecert.example.com" in the request.

Design note: Encoding the user name with Base32 allows local parts that have characters that would prevent their use in domain names. For example, a period (".") is a valid character in a local part, but would wreak havoc in a domain name. Similarly, [RFC6530] allows non-ASCII characters in local parts, and encoding a local part with non-ASCII characters with Base32 renders the name usable in the DNS.

7. 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 draft-ietf-dane-protocol.]]

8. Mandatory-to-Implement Features

[[Mostly copied from draft-ietf-dane-protocol.]]

9. IANA Considerations

[[Mostly copied from draft-ietf-dane-protocol but using "SMIMEA" instead.]]

10. Security Considerations

DNS zones that are signed with DNSSEC using NSEC for denial of existence are susceptible to zone-walking, a mechanism that allow someone to enumerate all the names in the zone. Someone who wanted to collect email addresses from a zone that uses SMIMEA might use such a mechanism. DNSSEC-signed zones using NSEC3 for denial of existence are significantly less susceptible to zone-walking. Someone could still attempt a dictionary attack on the zone to find SMIMEA records, just as they can use dictionary attacks on an SMTP server to see which addresses are valid.

[[More copied from draft-ietf-dane-protocol but is actually about S/MIME senders and receivers.]]

11. Acknowledgements

Miek Gieben and Martin Pels contributed technical ideas and support to this document.

12. References

12.1. 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.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[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.

12.2. Informative References

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

[RFC6530] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, February 2012.

Authors' Addresses

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org

Jakob Schlyter
Kirei AB

Email: jakob@kirei.se