Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 18, 2014

P. Hoffman
VPN Consortium
J. Schlyter
Kirei AB

February 14, 2014

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

draft-ietf-dane-smime-05

Abstract

This document describes how to use secure DNS to associate an S/MIME user's certificate with the intended domain name, similar to the way that DANE (RFC 6698) does for TLS.

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 August 18, 2014.

Copyright Notice

Table of Contents

1. Introduction

S/MIME [RFC5751] messages often contain a certificate (some messages contain more than one certificate). These certificates assist 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 who 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. There are other requirements on the MUA, such as associating the identity in the certificate with that of the message, that are out of scope for this document.

Some people want to authenticate the association of the sender's certificate with the sender without trusting a configured trust anchor. 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.

This document describes a mechanism for associating a user's certificate with the domain that is similar to that described in DANE itself [RFC6698]. Most of the operational and security considerations for using the mechanism in this document are described in RFC 6698, and are not described here at all. Only the major differences between this mechanism and those used in RFC 6698 are described here. Thus, the reader must be familiar with RFC 6698 before reading this document.

NOTE FOR FUTURE DRAFTS OF THIS DOCUMENT: The DANE WG needs to have a serious discussion about what the DANE set of specifications covering TLS for HTTP, TLS for SMTP, S/MIME, OpenPGP, and so on are meant for. They could be used for acquisition of key assocation material, for discovering services that use the keying material, for having assurance that a service that uses the keying material should be available, or some combination of these.

1.1. 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 PKIX [RFC5280], DNSSEC [RFC4033], [RFC4034], [RFC4035], and SMIME [RFC5751] for these terms.

2. The SMIMEA Resource Record

The SMIMEA DNS resource record (RR) is used to associate an end entity certificate or public key with the associated email address, thus forming a "SMIMEA certificate association". The semantics of how the SMIMEA RR is interpreted are given later in this document. Note that the information returned in the SMIMEA record might be for the end entity certificate, or it might be for the trust anchor or an intermediate certificate.

The type value for the SMIMEA RRtype is defined in Section 5.1. The SMIMEA resource record is class independent. The SMIMEA resource record has no special TTL requirements.

The SMIMEA wire format and presentation format are the same as for the TLSA record as described in section 2.1 of RFC 6698. The certificate usage field, the selector field, and the matching type field have the same format; the semantics are also the same except where RFC 6698 talks about TLS at the target protocol for the certificate information.

3. 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 the mail message format definition [RFC2822] and the "local part" in the specification for internationalized email [RFC6530]), is hashed using the SHA2-224 [RFC5754] algorithm to become the left-most label in the prepared domain name 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. The string that is used for the local part is a Unicode string encoded in UTF-8.

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", first calculate the SHA-224 of "chris", which is 0x3f51f4663b2b798560c5b9e16d6069a28727f62518c3a1b33f7f5214. Next, calculate the Base32 of that value, which is "H5I7IZR3FN4YKYGFXHQW2YDJUKDSP5RFDDB2DMZ7P5JBI===". The request is thus:

```
H5I7IZR3FN4YKYGFXHQW2YDJUKDSP5RFDDB2DMZ7P5JBI===._smimecert.example.com
```

The corresponding resource record in the example.com zone might look like:

```
H5I7IZR3FN4YKYGFXHQW2YDJUKDSP5RFDDB2DMZ7P5JBI===._smimecert.example.com.
   IN SMIMEA (
   0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
         7983a1d16e8a410e4561cb106618e971 )
```

Design note: Hashing the user name with SHA-224 and then encoding with Base32 allows local parts that have characters that would prevent their use in domain names in typical applications. Even though the DNS protocol itself can use any octet value in a label, most applications that use DNS names are limited to a much smaller set of allowed characters. For example, a period (".") is a valid character in a local part, but would wreak havoc in a domain name unless the application using the name somehow quoted it. Similarly,

RFC 6530 allows non-ASCII characters in local parts, and encoding a local part with non-ASCII characters with Base32 renders the name usable in applications that use the DNS.

Wildcards can be more useful for SMIMEA than they are for TLSA. If a site publishes a trust anchor certificate for all users on the site (certificate usage 0 or 2), it could make sense to use a wildcard resource record such as "*._smimecert.example.com".

4. Mandatory-to-Implement Features

S/MIME MUAs conforming to this specification MUST be able to correctly interpret SMIMEA records with certificate usages 0, 1, 2, and 3. S/MIME MUAs conforming to this specification MUST be able to compare a certificate association with a certificate offered by another S/MIME MUA using selector types 0 and 1, and matching type 0 (no hash used) and matching type 1 (SHA-256), and SHOULD be able to make such comparisons with matching type 2 (SHA-512).

5. IANA Considerations

5.1. SMIMEA RRtype

This document uses a new DNS RRtype, SMIMEA, whose value will be allocated by IANA from the Resource Record (RR) TYPEs subregistry of the Domain Name System (DNS) Parameters registry.

TODO: there needs to be new registries for certificate usages, selectors, and maching types, pre-populated with the values from TLSA.

6. 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.

Client treatment of any information included in the trust anchor is a matter of local policy. This specification does not mandate that such information be inspected or validated by the domain name administrator.

7. Acknowledgements

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

8. References

8.1. 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.

[RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", RFC 5754, January 2010.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

8.2. 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