Using Secure DNS to Associate Certificates with Domain Names For S/MIME
draft-ietf-dane-smime-02

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 January 8, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.
Table of Contents

1. Introduction .................................................. 3
   1.1. Terminology ............................................... 3
2. The SMIMEA Resource Record ................................. 3
3. Domain Names for S/MIME Certificate Associations ........ 4
4. Mandatory-to-Implement Features ............................ 4
5. IANA Considerations ........................................... 5
   5.1. SMIMEA RRtype ........................................... 5
6. Security Considerations ....................................... 5
7. Acknowledgements .............................................. 5
8. References .................................................... 5
   8.1. Normative References ..................................... 5
   8.2. 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 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.

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.
The type value for the SMIMEA RR type is defined in Section 5.1. The SMIMEA RR is class independent. The SMIMEA RR has no special TTL requirements. The SMIMEA wire format and presentation format are the same as for the TLSA record.

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 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 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 "MNUHE2LT._smimecert.example.com" in the request. The corresponding RR in the example.com zone might look like:

```
MNUHE2LT._smimecert.example.com. IN SMIMEA ( 0 0 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971 )
```

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, 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 the DNS.

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 RR type, 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 matching 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


8.2. Informative References


Authors’ Addresses

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org
Jakob Schlyter
Kirei AB

Email: jakob@kirei.se