

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 17, 2019

B. Haberman
JHU APL
J. Levine
Taughannock Networks
July 16, 2018

Using a DNS SRV Record to Locate an X.509 Certificate Store
draft-bhjl-x509-srv-04

Abstract

This document describes a method to allow parties to locate X.509 certificate stores with Domain Name System Service records in order to retrieve certificates and certificate revocation lists. The primary purpose of such retrievals is to facilitate the association of X.509 and PGP public keys with e-mail addresses to allow for encrypted e-mail exchanges.

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 <https://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 17, 2019.

Copyright Notice

Copyright (c) 2018 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 (<https://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

Internet-Draft

Cert Store SRV Record

July 2018

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Service Record Format	2
3.	Certificate Store Queries	3
4.	Name Matching	4
5.	Certificate Validation	4
6.	Certificate use and cacheing	5
7.	Security Considerations	5
8.	IANA Considerations	5
8.1.	Certificates service	6
8.2.	Smimeca service	6
9.	Acknowledgements	6
10.	Normative References	7
	Authors' Addresses	7

[1.](#) Introduction

X.509 and PGP public keys can be used to encrypt or sign e-mail messages. In order to verify a sender's signature or encrypt an e-mail, the e-mail client needs to locate the appropriate public key. The X.509-based Public Key Infrastructure (PKI) [[RFC5280](#)] provides the necessary services to allow for the retrieval of certificates and certificate revocation lists, but lacks the discovery mechanism needed to associate e-mail domains with specific PKI servers.

This document specifies an approach that uses a Domain Name System (DNS) Service Record (SRV) that allows mail service providers to advertise the X.509 or PGP certificate store [[RFC4387](#)] that contains certificates and certificate revocation lists for their e-mail users. Additionally, this document specifies the appropriate query strings to use when accessing the certificate store.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

[2.](#) Service Record Format

The general format of a DNS SRV record is documented in [[RFC2782](#)] as:

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

To support the advertisement of an X.509 certificate store, service providers publish an SRV record for the certificates service with the appropriate parameters, as described in [[RFC4387](#)], [section 3.2](#). An example of such an SRV record is:

```
_certificates._tcp 86400 IN SRV 0 0 443 certs.example.com
```

The parameters of the DNS SRV record are set based on the operational needs of the service provider. The DNS SRV record SHOULD be signed via DNSSEC [[RFC4033](#)][RFC4034]. The server MUST be an https server and will typically use port 443. The certificate of the https server SHOULD be validated by a DNSSEC signed TLSA record, and MAY also be validated by a certificate authority.

[3.](#) Certificate Store Queries

To retrieve an X.509 S/MIME certificate, the attribute type is "uri", and the URI is constructed using the path described in [[RFC4387](#)], [Section 3.3](#), specifically "/certificates/search.cgi". Using the SRV record above to look up a certificate for bob@example.com, the URI would be:

```
https://certs.example.com/certificates/search.cgi?uri=bob%40example.com
```

X.509 certificate stores MUST support the uri attribute and MAY support other attributes.

To retrieve a PGP certificate, the attribute type is "email", and the URI is constructed using the path described in [[RFC4387](#)],

[Section 3.3](#), specifically `"/pgpkeys/search.cgi"`. Using the SRV record above to look up a certificate for `bob@example.com`, the URI would be:

`https://certs.example.com/pgpkeys/search.cgi?email=bob%40example.com`

PGP certificate stores **MUST** support the email attribute and **MAY** support other attributes.

[4.](#) Name Matching

SMTP [[RFC5321](#)] specifies that the local part of a mailbox is interpreted only by the mailbox domain itself. This document does not update or modify that document.

If a certificate store has no certificate with an e-mail address that matches the uri or email attribute in a retrieval request, but it does have a certificate with an e-mail address that the mailbox domain treats similarly to the requested address, the server **MAY** return that certificate. The definition of what is sufficiently similar is a matter of local policy, but the intention is that a human correspondent would consider the the two addresses to deliver mail to the same person or entity.

[5.](#) Certificate Validation

The certificate is returned as a blob of binary data. If multiple certificates are returned, the response is encoded as multipart/mixed as described in [[RFC4387](#)] [section 2](#).

X509 S/MIME certificates are validated by checking for a signature by a Certificate Authority (CA) that is acceptable to the validating party. This specification defines an additional validation technique. The domain **MAY** publish validation certificates using TLSA records at the name `_smimeca._tcp`. The TLSA records **MUST** have PKIX-TA or DANE-TA usage[RFC7218]. A validation certificate published by a domain **MUST NOT** be used to validate certificates other than those with e-mail addresses in that domain.

Since the relationship between a domain and its mailbox users is in general unknown to correspondents, a client applies a local policy to decide whether to use a S/MIME certificate validated only by a signing certificate published by the domain.

PGP certificates are validated by the PGP web of trust. A domain can endorse the certificates it publishes by signing them with a signature of postmaster@<domain>. Since the relationship between a domain and its mailbox users is in general unknown to correspondents, a client applies a local policy to decide whether to use a PGP certificate retrieved from a certificate server. This policy would typically be the same one used to decide whether to use a certificate retrieved from a traditional PGP key server.

[6.](#) Certificate use and caching

Clients SHOULD cache responses to queries as advised by http cache headers. This includes both returned certificates, and 404 failures saying that an address (or other search key) has no certificate.

S/MIME keys retrieved from the certificate store SHOULD NOT be used for validation of signatures on incoming mail without further validation of the certificate. S/MIME signed mail includes a copy of the signing certificate which, if it can be validated, typically would be used instead.

[7.](#) Security Considerations

Certificate queries could be used to try to validate lists of e-mail addresses. This is essentially the same problem that mail servers face with VRFY, EXPN, and RCPT TO probes, and the same countermeasures would apply, such as rate limiting, blacklisting abusive clients, and returning fake results for non-existent addresses.

DNSSEC signatures on the SRV record and the https server certificate

ensure that any keys retrieved by the technique described in this document are the ones published by the domain's management. But since correspondents often do not know the relationship between a domain and its mailbox users, it would be imprudent to assume that such certificates are in fact ones issued to or used by mailbox recipients or to assume that mail encrypted using the certificates will be readable only by the intended recipient without further information about the certificates.

A domain could publish man-in-the-middle certificates that allowed it to decode and read mail, and perhaps re-encrypt it using different certificates used by the recipients. In some cases this would be entirely legitimate, e.g., a financial institution that is required to log all of its employees' correspondence. In other cases, it could be intrusive or improper surveillance of the contents of users' mail. Identifying or describing the relationship between a domain and its mail users is beyond the scope of this document.

[8.](#) IANA Considerations

IANA is requested to update two entries in the Service Name and Transport Protocol Port Number Registry.

Haberman & Levine	Expires January 17, 2019	[Page 5]
-------------------	--------------------------	----------

Internet-Draft	Cert Store SRV Record	July 2018
----------------	-----------------------	-----------

[8.1.](#) Certificates service

Service Name: certificates

Transport Protocol(s): tcp

Assignee: IESG

Contact: <chair@ietf.org>

Description: Server for S/MIME and PGP certificates

Reference: [this document]

Port Number: none

Service Code: none

Known Unauthorized Uses: none

8.2. Smimeca service

Service Name: simeca

Transport Protocol(s): tcp

Assignee: IESG

Contact: <chair@ietf.org>

Description: Per-domain authority certificate for S/MIME certificates

Reference: [this document]

Port Number: none

Service Code: none

Known Unauthorized Uses: none

9. Acknowledgements

We thank Wei Chuang, Nicolas Lidzborski, and Andreas Schulze for comments and suggestions.

10. Normative References

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", [RFC 2782](#), DOI 10.17487/RFC2782, February 2000, <<https://www.rfc-editor.org/info/rfc2782>>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S.

Rose, "DNS Security Introduction and Requirements",
[RFC 4033](#), DOI 10.17487/RFC4033, March 2005,
<<https://www.rfc-editor.org/info/rfc4033>>.

- [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", [RFC 4034](#), DOI 10.17487/RFC4034, March 2005, <<https://www.rfc-editor.org/info/rfc4034>>.
- [RFC4387] Gutmann, P., Ed., "Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP", [RFC 4387](#), DOI 10.17487/RFC4387, February 2006, <<https://www.rfc-editor.org/info/rfc4387>>.
- [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](#), DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", [RFC 5321](#), DOI 10.17487/RFC5321, October 2008, <<https://www.rfc-editor.org/info/rfc5321>>.
- [RFC7218] Gudmundsson, O., "Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)", [RFC 7218](#), DOI 10.17487/RFC7218, April 2014, <<https://www.rfc-editor.org/info/rfc7218>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

Authors' Addresses

Brian Haberman
Johns Hopkins University Applied Physics Lab

Email: brian@innovationslab.net

Taughannock Networks
PO Box 727
Trumansburg, NY 14886

Phone: +1 831 480 2300
Email: standards@taugh.com