

Internet Engineering Task Force (IETF)
Request for Comments: 7673
Category: Standards Track
ISSN: 2070-1721

T. Finch
University of Cambridge
M. Miller
Cisco Systems, Inc.
P. Saint-Andre
&yet
October 2015

Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records

Abstract

The DNS-Based Authentication of Named Entities (DANE) specification (RFC 6698) describes how to use TLSA resource records secured by DNSSEC (RFC 4033) to associate a server's connection endpoint with its Transport Layer Security (TLS) certificate (thus enabling administrators of domain names to specify the keys used in that domain's TLS servers). However, application protocols that use SRV records (RFC 2782) to indirectly name the target server connection endpoints for a service domain name cannot apply the rules from RFC 6698. Therefore, this document provides guidelines that enable such protocols to locate and use TLSA records.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc7673>.

Copyright Notice

Copyright (c) 2015 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
2. Terminology	4
3. DNS Checks	4
3.1. SRV Query	4
3.2. Address Queries	5
3.3. TLSA Queries	6
3.4. Impact on TLS Usage	6
4. TLS Checks	7
4.1. SRV Records Only	7
4.2. TLSA Records	8
5. Guidance for Protocol Authors	8
6. Guidance for Server Operators	8
7. Guidance for Application Developers	9
8. Internationalization Considerations	9
9. Security Considerations	10
9.1. Mixed Security Status	10
9.2. Certificate Subject Name Matching	10
10. References	11
10.1. Normative References	11
10.2. Informative References	12
Appendix A. Examples	13
A.1. IMAP	13
A.2. XMPP	13
Appendix B. Rationale	14
Acknowledgements	15
Authors' Addresses	16

1. Introduction

The base DNS-Based Authentication of Named Entities (DANE) specification [RFC6698] describes how to use TLSA resource records secured by DNSSEC [RFC4033] to associate a target server's connection endpoint with its Transport Layer Security (TLS) certificate (thus enabling administrators of domain names to specify the keys used in that domain's TLS servers). Some application protocols locate connection endpoints indirectly via SRV records [RFC2782]. As a result of this indirection, the rules specified in [RFC6698] cannot be directly applied to such application protocols. (Rules for SMTP [RFC5321], which uses MX resource records instead of SRV records, are described in [RFC7672].)

This document describes how to use DANE TLSA records with SRV records. To summarize:

- o We rely on DNSSEC to secure SRV records that map the desired service, transport protocol, and service domain name to the corresponding target server connection endpoints (i.e., the target server hostnames and port numbers returned in the SRV records for that service type).
- o Although in accordance with [RFC2782] a service domain name can advertise a number of SRV records (some of which might map to connection endpoints that do not support TLS), the intent of this specification is for a client to securely discover connection endpoints that support TLS.
- o The TLSA records for each connection endpoint are located using the transport protocol, port number, and hostname for the target server (not the service domain name).
- o When DNSSEC-validated TLSA records are published for a given connection endpoint, clients always use TLS when connecting (even if the connection endpoint supports cleartext communication).
- o If there is at least one usable TLSA record for a given connection endpoint, the connection endpoint's TLS certificate or public key needs to match at least one of those usable TLSA records.
- o If there are no usable TLSA records for a given connection endpoint, the target server hostname is used as one of the acceptable reference identifiers, as described in [RFC6125]. Other reference identifiers might arise through CNAME expansion of either the service domain name or target server hostname, as detailed in [RFC7671].

- o If there are no usable TLSA records for any connection endpoint (and thus the client cannot securely discover a connection endpoint that supports TLS), the client's behavior is a matter for the application protocol or client implementation; this might involve a fallback to non-DANE behavior using the public key infrastructure [RFC5280].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this memo are to be interpreted as described in [RFC2119].

This document uses the definitions for "secure", "insecure", "bogus", and "indeterminate" from Section 4.3 of [RFC4035]. This document uses the acronyms from [RFC7218] for the values of TLSA fields where appropriate.

Additionally, this document uses the following terms:

connection endpoint: A tuple of a fully qualified DNS hostname, transport protocol, and port number that a client uses to establish a connection to the target server.

service domain name: The fully qualified DNS domain name that identifies an application service; corresponds to the term "source domain" from [RFC6125].

This document uses the term "target server hostname" in place of the term "derived domain" from the so-called CertID specification [RFC6125].

3. DNS Checks

3.1. SRV Query

When the client makes an SRV query, a successful result will typically be a list of one or more SRV records (or possibly a chain of CNAME/DNAME aliases leading to such a list).

NOTE: Implementers need to be aware that unsuccessful results can occur because of various DNS-related errors; guidance on avoiding downgrade attacks can be found in Section 2.1 of [RFC7672].

For this specification to apply, the entire chain of DNS RRset(s) returned MUST be "secure" according to DNSSEC validation (Section 5 of [RFC4035]). In the case where the answer is obtained via a chain of CNAME and/or DNAME aliases, the whole chain of CNAME and DNAME RRsets MUST also be secure.

If the SRV lookup fails because the RRset is "bogus" (or the lookup fails for reasons other than no records), the client MUST abort its attempt to connect to the desired service. If the lookup result is "insecure" (or no SRV records exist), this protocol does not apply and the client SHOULD fall back to its non-DNSSEC, non-DANE (and possibly non-SRV) behavior.

When the lookup returns a "secure" RRset (possibly via a chain of "secure" CNAME/DNAME records), the client now has an authentic list of target server connection endpoints with weight and priority values. It performs server ordering and selection using the weight and priority values without regard to the presence or absence of DNSSEC or TLSA records. It also takes note of the DNSSEC validation status of the SRV response for use when checking certificate names (see Section 4). The client can then proceed to making address queries on the target server hostnames as described in the following section.

3.2. Address Queries

For each SRV target server connection endpoint, the client makes A and/or AAAA queries, performs DNSSEC validation on the address (A or AAAA) response, and continues as follows, based on the results:

- o If a returned RRSet is "secure", the client MUST perform a TLSA query for that target server connection endpoint, as described in the next section.
- o If no returned RRsets are "secure", the client MUST NOT perform a TLSA query for that target server connection endpoint; the TLSA query will most likely fail or produce spurious results.
- o If the address record lookup fails (a validation status of either "bogus" or "indeterminate"), the client MUST NOT connect to this connection endpoint; instead, it uses the next most appropriate SRV target. This helps prevent downgrade attacks.

3.3. TLSA Queries

The client SHALL construct the TLSA query name as described in Section 3 of [RFC6698], based on the fields from the SRV record: the port number from the SRV RDATA, the transport protocol from the SRV query name, and the TLSA base domain from the SRV target server hostname.

For example, the following SRV record for IMAP (see [RFC6186])

```
_imap._tcp.example.com. 86400 IN SRV 10 0 9143 imap.example.net.
```

leads to the TLSA query shown below:

```
_9143._tcp.imap.example.net. IN TLSA ?
```

3.4. Impact on TLS Usage

The client SHALL determine if the TLSA records returned in the previous step are usable according to Section 4.1 of [RFC6698]. This affects the use of TLS as follows:

- o If the TLSA response is "secure" and usable, then the client MUST use TLS when connecting to the target server. The TLSA records are used when validating the server's certificate as described in Section 4.
- o If the TLSA response is "bogus" or "indeterminate" (or the lookup fails for reasons other than no records), then the client MUST NOT connect to the target server (the client can still use other SRV targets).
- o If the TLSA response is "insecure" (or no TLSA records exist), then the client SHALL proceed as if the target server had no TLSA records. It MAY connect to the target server with or without TLS, subject to the policies of the application protocol or client implementation.

4. TLS Checks

When connecting to a server, the client **MUST** use TLS if the responses to the SRV and TLSA queries were "secure" as described above. The rules described in the next two sections -- Section 4.2 for cases where there is at least one usable TLSA record, and Section 4.1 otherwise -- apply to such secure responses.

4.1. SRV Records Only

If the client received zero usable TLSA certificate associations, it **SHALL** validate the server's TLS certificate using the normal PKIX rules [RFC5280] or protocol-specific rules (e.g., following [RFC6125]) without further input from the TLSA records. In this case, the client uses the information in the server certificate and the DNSSEC validation status of the SRV query in its authentication checks. It **SHOULD** use the Server Name Indication extension (TLS SNI) [RFC6066] or its functional equivalent in the relevant application protocol (e.g., in the Extensible Messaging and Presence Protocol (XMPP) [RFC6120], this is the 'to' address of the initial stream header). The preferred name **SHALL** be chosen as follows, and the client **SHALL** verify the identity asserted by the server's certificate according to Section 6 of [RFC6125], using a list of reference identifiers constructed as follows (note again that in RFC 6125 the terms "source domain" and "derived domain" refer to the same things as "service domain name" and "target server hostname" in this document). The examples below assume a service domain name of "im.example.com" and a target server hostname of "xmpp23.hosting.example.net".

SRV is insecure: The reference identifiers **SHALL** include the service domain name and **MUST NOT** include the SRV target server hostname (e.g., include "im.example.com" but not "xmpp23.hosting.example.net"). The service domain name is the preferred name for TLS SNI or its equivalent.

SRV is secure: The reference identifiers **SHALL** include both the service domain name and the SRV target server hostname (e.g., include both "im.example.com" and "xmpp23.hosting.example.net"). The service domain name is still the preferred name for TLS SNI or its equivalent (this reduces code complexity and the possibility of interoperability problems).

In the latter case, the client will accept either identity to ensure compatibility with servers that support this specification as well as servers that do not support this specification.

4.2. TLSA Records

If the client received one or more usable TLSA certificate associations, it SHALL process them as described in Section 2.1 of [RFC6698].

If the TLS server's certificate -- or the public key of the server's certificate -- matches a usable TLSA record with certificate usage DANE-EE, the client MUST ignore validation checks from [RFC5280] and reference identifier checks from [RFC6125]. The information in such a TLSA record supersedes the non-key information in the certificate.

5. Guidance for Protocol Authors

This document describes how to use DANE with application protocols in which target servers are discovered via SRV records. Although this document attempts to provide generic guidance applying to all such protocols, additional documents for particular application protocols could cover related topics, such as:

- o Fallback logic in the event that a client is unable to connect securely to a target server by following the procedures defined in this document.
- o How clients ought to behave if (1) they do not support SRV lookups or (2) they do support SRV lookups and encounter service domain names that do not offer SRV records.
- o Whether or not the application protocol has a functional equivalent for TLS SNI that is preferred within that protocol.
- o The use of SRV records with additional discovery technologies, such as the use of both SRV records and NAPTR records [RFC3403] for transport selection in the Session Initiation Protocol (SIP).

For example, [XMPP-DNA] covers such topics for XMPP.

6. Guidance for Server Operators

To conform to this specification, the published SRV records and subsequent address (A and AAAA) records MUST be secured with DNSSEC. There SHOULD also be at least one TLSA record published that authenticates the server's certificate.

When using TLSA records with certificate usage DANE-EE, it is not necessary for the deployed certificate to contain an identifier for either the source domain or target server hostname. However, operators need to be aware that servers relying solely on validation

using certificate usage DANE-EE TLSA records might prevent clients that do not support this specification from successfully connecting with TLS.

For TLSA records with certificate usage types other than DANE-EE, the certificate(s) MUST contain an identifier that matches:

- o the service domain name (the "source domain" in [RFC6125] terms, which is the SRV query domain), and/or
- o the target server hostname (the "derived domain" in [RFC6125] terms, which is the SRV target hostname).

Servers that support multiple service domain names (i.e., so-called "multi-tenanted environments") can implement TLS SNI [RFC6066] or its functional equivalent to determine which certificate to offer. Clients that do not support this specification will indicate a preference for the service domain name, while clients that support this specification will indicate the target server hostname. However, the server determines what certificate to present in the TLS handshake; e.g., the presented certificate might only authenticate the target server hostname.

7. Guidance for Application Developers

Developers of application clients that depend on DANE-SRV often would like to prepare as quickly as possible for making a connection to the intended service, thus reducing the wait time for end users. To make this optimization possible, a DNS library might perform the address queries and TLSA queries in parallel. (Because a TLSA record can be ignored if it turns out that the address record on which it depends is not secure, performing the TLSA queries in parallel with the address queries is not harmful from a security perspective and can yield some operational benefits.)

8. Internationalization Considerations

If any of the DNS queries are for an internationalized domain name, then they need to use the A-label form [RFC5890].

9. Security Considerations

9.1. Mixed Security Status

We do not specify that all of the target server connection endpoints for a service domain name need to be consistent in whether they have or do not have TLSA records. This is so that partial or incremental deployment does not break the service. Different levels of deployment are likely if a service domain name has a third-party fallback server, for example.

The SRV sorting rules are unchanged; in particular, they have not been altered in order to prioritize secure connection endpoints over insecure connection endpoints. If a site wants to be secure, it needs to deploy this protocol completely; a partial deployment is not secure, and we make no special effort to support it.

9.2. Certificate Subject Name Matching

Section 4 of the TLSA specification [RFC6698] leaves the details of checking names in certificates to higher-level application protocols, though it suggests the use of [RFC6125].

Name checks are not necessary if the matching TLSA record is of certificate usage DANE-EE. Because such a record identifies the specific certificate (or public key of the certificate), additional checks are superfluous and potentially conflicting.

Otherwise, while DNSSEC provides a secure binding between the server name and the TLSA record, and the TLSA record provides a binding to a certificate, this latter step can be indirect via a chain of certificates. For example, a certificate usage PKIX-TA TLSA record only authenticates the Certification Authority (CA) that issued the certificate, and third parties can obtain certificates from the same CA. Therefore, clients need to check to see whether or not the server's certificate matches one of the expected reference identifiers to ensure that the certificate was issued by the CA to the server the client expects (naturally, this is in addition to standard certificate-related checks as specified in [RFC5280], including but not limited to certificate syntax, certificate extensions such as name constraints and extended key usage, and handling of certification paths).

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [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, <<http://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, <<http://www.rfc-editor.org/info/rfc4033>>.
- [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <<http://www.rfc-editor.org/info/rfc4035>>.
- [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, <<http://www.rfc-editor.org/info/rfc5280>>.
- [RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <<http://www.rfc-editor.org/info/rfc5890>>.
- [RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <<http://www.rfc-editor.org/info/rfc6066>>.
- [RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <<http://www.rfc-editor.org/info/rfc6125>>.

- [RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <<http://www.rfc-editor.org/info/rfc6698>>.
- [RFC7218] Gudmundsson, O., "Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)", RFC 7218, DOI 10.17487/RFC7218, April 2014, <<http://www.rfc-editor.org/info/rfc7218>>.
- [RFC7671] Dukhovni, V. and W. Hardaker, "The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance", RFC 7671, DOI 10.17487/RFC7671, October 2015, <<http://www.rfc-editor.org/info/rfc7671>>.
- [RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <<http://www.rfc-editor.org/info/rfc7672>>.

10.2. Informative References

- [RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, DOI 10.17487/RFC3403, October 2002, <<http://www.rfc-editor.org/info/rfc3403>>.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <<http://www.rfc-editor.org/info/rfc5321>>.
- [RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <<http://www.rfc-editor.org/info/rfc6120>>.
- [RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, DOI 10.17487/RFC6186, March 2011, <<http://www.rfc-editor.org/info/rfc6186>>.
- [XMPP-DNA] Saint-Andre, P., Miller, M., and P. Hancke, "Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)", Work in Progress, draft-ietf-xmpp-dna-11, September 2015.

Appendix A. Examples

In the following, most of the DNS resource data is elided for simplicity.

A.1. IMAP

```
; mail domain
imap._tcp.example.com. SRV 10 0 9143 imap.example.net.
example.com. RRSIG SRV ...

; target server hostname
imap.example.net. A 192.0.2.1
imap.example.net. RRSIG A ...

imap.example.net. AAAA 2001:db8:212:8::e:1
imap.example.net. RRSIG AAAA ...

; TLSA resource record
_9143._tcp.imap.example.net. TLSA ...
_9143._tcp.imap.example.net. RRSIG TLSA ...
```

Mail messages received for addresses at example.com are retrieved via IMAP at imap.example.net. Connections to imap.example.net port 9143 that use STARTTLS will get a server certificate that authenticates the name imap.example.net.

A.2. XMPP

```
; XMPP domain
_xmpp-client._tcp.example.com. SRV 1 0 5222 im.example.net.
_xmpp-client._tcp.example.com. RRSIG SRV ...

; target server hostname
im.example.net. A 192.0.2.3
im.example.net. RRSIG A ...

im.example.net. AAAA 2001:db8:212:8::e:4
im.example.net. RRSIG AAAA ...

; TLSA resource record
_5222._tcp.im.example.net. TLSA ...
_5222._tcp.im.example.net. RRSIG TLSA ...
```

XMPP sessions for addresses at example.com are established at im.example.net. Connections to im.example.net port 5222 that use STARTTLS will get a server certificate that authenticates the name im.example.net.

Appendix B. Rationale

The long-term goal of this specification is to settle on TLS certificates that verify the target server hostname rather than the service domain name, since this is more convenient for servers hosting multiple domains (so-called "multi-tenanted environments") and scales up more easily to larger numbers of service domain names.

There are a number of other reasons for doing it this way:

- o The certificate is part of the server configuration, so it makes sense to associate it with the target server hostname rather than the service domain name.
- o In the absence of TLS SNI, if the certificate identifies the target server hostname, then it does not need to list all the possible service domain names.
- o When the server certificate is replaced, it is much easier if there is one part of the DNS that needs updating to match, instead of an unbounded number of hosted service domain names.
- o The same TLSA records work with this specification, and with direct connections to the connection endpoint in the style of [RFC6698].
- o Some application protocols, such as SMTP, allow a client to perform transactions with multiple service domain names in the same connection. It is not, in general, feasible for the client to specify the service domain name using TLS SNI when the connection is established, and the server might not be able to present a certificate that authenticates all possible service domain names. See [RFC7672] for details.
- o It is common for SMTP servers to act in multiple roles -- for example, as outgoing relays or as incoming MX servers, depending on the client identity. It is simpler if the server can present the same certificate regardless of the role in which it is to act. Sometimes the server does not know its role until the client has authenticated, which usually occurs after TLS has been established. See [RFC7672] for details.

This specification does not provide an option to put TLSA records under the service domain name, because that would add complexity without providing any benefit; security protocols are best kept simple. As described above, there are real-world cases where authenticating the service domain name cannot be made to work, so there would be complicated criteria regarding when service domain name TLSA records might be used and when they cannot. This is all avoided by putting the TLSA records under the target server hostname.

The disadvantage is that clients that do not complete DNSSEC validation must, according to [RFC6125] rules, check the server certificate against the service domain name, since they have no other way to authenticate the server. This means that SNI support or its functional equivalent is necessary for backward compatibility.

Acknowledgements

Thanks to Mark Andrews for arguing that authenticating the target server hostname is the right thing, and that we ought to rely on DNSSEC to secure the SRV lookup. Thanks to Stephane Bortzmeyer, James Cloos, Viktor Dukhovni, Ned Freed, Olafur Gudmundsson, Paul Hoffman, Phil Pennock, Hector Santos, Jonas Schneider, and Alessandro Vesely for helpful suggestions.

Carl Wallace completed an insightful review on behalf of the Security Directorate.

Ben Campbell, Brian Haberman, and Alvaro Retana provided helpful feedback during IESG review.

The authors gratefully acknowledge the assistance of Olafur Gudmundsson and Warren Kumari as the working group chairs and Stephen Farrell as the sponsoring Area Director.

Peter Saint-Andre wishes to acknowledge Cisco Systems, Inc., for employing him during his work on earlier draft versions of this document.

Authors' Addresses

Tony Finch
University of Cambridge Information Services
Roger Needham Building
7 JJ Thomson Avenue
Cambridge CB3 0RB
United Kingdom

Phone: +44 797 040 1426
Email: dot@dotat.at
URI: <http://dotat.at/>

Matthew Miller
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
United States

Email: mamille2@cisco.com

Peter Saint-Andre
&yet

Email: peter@andyet.com
URI: <https://andyet.com/>