Workgroup: dnsop
Internet-Draft: draft-rebs-dnsop-svcb-dane-01
Updates: rfc6698 (if approved)
Published: 22 June 2022
Intended Status: Standards Track
Expires: 24 December 2022
Authors: B. M. Schwartz R. Evans
Google LLC Google LLC

Using Service Bindings with DANE

Abstract

Service Binding records introduce a new form of name indirection in DNS. This document specifies DNS-Based Authentication of Named Entities (DANE) interaction with Service Bindings to secure endpoints including use of ports and transports discovered via Service Parameters.

Discussion Venues

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/bemasc/svcb-dane.

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 24 December 2022.

Copyright Notice

Table of Contents

1. Introduction

The DNS-Based Authentication of Named Entities specification [RFC7671] explains how clients locate the TLSA record for a service of interest, starting with knowledge of the service's hostname, transport, and port number. These are concatenated, forming a name like _8080._tcp.example.com. It also specifies how clients should locate the TLSA record when one or more CNAME records are present, aliasing either the hostname or the TLSA record's name, and the resulting server names used in TLS.

There are various DNS records other than CNAME that add indirection to the host resolution process, requiring similar specifications. Thus, [RFC7672] describes how DANE interacts with MX records, and [RFC7673] describes its interaction with SRV records.

This draft describes the interaction of DANE with indirection via Service Bindings [SVCB], i.e. SVCB-compatible records such as SVCB and HTTPS. It also explains how to use DANE with new TLS-based transports such as QUIC.

2. Conventions and Definitions

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Using DANE with Service Bindings

Section 6 of [RFC7671] says:

> With protocols that support explicit transport redirection via DNS MX records, SRV records, or other similar records, the TLSA base domain is based on the redirected transport endpoint rather than the origin domain.

This draft applies the same logic to SVCB-compatible records. Specifically, if SVCB resolution was entirely secure (including any AliasMode records and/or CNAMEs), then for each connection attempt derived from a SVCB-compatible record,

- The initial TLSA base domain **MUST** be the final SVCB TargetName used for this connection attempt. (Names appearing earlier in a resolution chain are not used.)

- The transport prefix **MUST** be the transport of this connection attempt (possibly influenced by the "alpn" SvcParam).

- The port prefix **MUST** be the port number of this connection attempt (possibly influenced by the "port" SvcParam).

If the initial TLSA base domain is the start of a secure CNAME chain, clients **MUST** first try to use the end of the chain as the TLSA base domain, with fallback to the initial base domain, as described in Section 7 of [RFC7671].

If any TLSA QNAME is aliased by a CNAME, clients **MUST** follow the TLSA CNAME to complete the resolution of the TLSA record. (This does not alter the TLSA base domain.)

If a TLSA RRSet is securely resolved, the client **MUST** set the SNI to the TLSA base domain of the RRSet. In usage modes other than DANE-EE(3), the client **MUST** validate that the certificate covers this base domain, and **MUST NOT** require it to cover any other domain.

If the client has SVCB-optional behavior (as defined in Section 3 of [SVCB]), it **MUST** use the standard DANE logic described in Section 4.1 of [RFC6698] when falling back to non-SVCB connection.

4. Updating the TLSA protocol prefixes

Section 3 of [RFC6698] defined the protocol prefix used for constructing TLSA QNAMEs, and said:

> The transport names defined for this protocol are "tcp", "udp", and "sctp".

At that time, there was exactly one TLS-based protocol defined for each of these transports. However, with the introduction of QUIC [RFC9000], there are now multiple TLS-derived protocols that can operate over UDP, even on the same port. To distinguish the availability and configuration of DTLS and QUIC, this draft Updates the above sentence as follows:

> The transport names defined for this protocol are "tcp" (TLS over TCP [RFC8446]), "udp" (DTLS [I-D.draft-ietf-tls-dtls13]), "sctp" (TLS over SCTP [RFC3436]), and "quic" (QUIC [RFC9000]).

5. Operational considerations

5.1. Recommended configurations

Service consumers are expected to use CNAME or SVCB AliasMode to point at provider-controlled records, e.g.:

```
alias.net.                  HTTPS 0 xyz.provider.com.
www.alias.net.              CNAME xyz.provider.com.
xyz.provider.com.           HTTPS 1 . alpn=h2 ...
xyz.provider.com.           A     192.0.2.1
_443._tcp.xyz.provider.com. TLSA  <provider keys>
```

For ease of management, providers may want to alias various TLSA QNAMEs to a single RRSet:

```
_443._tcp.xyz.provider.com. CNAME dane-central.provider.com.
dane-central.provider.com.  TLSA  <provider keys>
```

5.2. Accidental pinning

When a service is used by third-party consumers, DANE allows the consumer to publish records that make claims about the certificates used by the service. When the service subsequently rotates its TLS keys, DANE authentication will fail for these consumers, resulting in an outage. Accordingly, zone owners **MUST NOT** publish TLSA records

for public keys that are not under their control unless they have an explicit arrangement with the key holder.

To prevents the above misconfiguration and ensure that TLS keys can be rotated freely, service operators **MAY** reject TLS connections whose SNI does not correspond to an approved TLSA base domain.

Service Bindings also enable any third party consumer to publish fixed SvcParams for the service. This can cause an outage or service degradation if the service makes a backward-incompatible configuration change. Accordingly, zone owners **SHOULD NOT** publish SvcParams for a TargetName that they do not control, and service operators should take caution when making incompatible configuration changes.

6. Security Considerations

This document specifies the use of TLSA as a property of each connection attempt. In environments where DANE is optional, this means that the fallback procedure might use DANE for some conection attempts but not others.

This document only specifies the use of TLSA records when the SVCB records were resolved securely. Use of TLSA records in conjunction with insecurely resolved SVCB records is not safe in general, although there may be some configurations where it is appropriate (e.g. when only opportunistic security is available).

7. Examples

The following examples demonstrate Serving Binding interaction with TLSA base domain selection.

All of the RRSets below are assumed fully-secure with all related DNSSEC record types omitted for brevity.

7.1. HTTPS ServiceMode

Given service URI https://api.example.com and record:

```
api.example.com. HTTPS 1 .
```

The TLSA QNAME is _443._tcp.api.example.com.

7.2. HTTPS AliasMode

Given service URI https://api.example.com and records:

```
api.example.com.     HTTPS 0 svc4.example.net.
svc4.example.net.    HTTPS 0 xyz.example-cdn.com.
xyz.example-cdn.com. A     192.0.2.1
```

The TLSA QNAME is _443._tcp.xyz.example-cdn.com.

7.3. QUIC and CNAME

Given service URI https://api.example.com and records:

```
www.example.com.  CNAME api.example.com.
api.example.com.  HTTPS 1 svc4.example.net alpn=h2,h3 port=8443
svc4.example.net. CNAME xyz.example-cdn.com.
```

If the connection attempt is using HTTP/3, the transport label is set to _quic; otherwise _tcp is used.

The initial TLSA QNAME would be one of:

*_8443._quic.xyz.example-cdn.com

*_8443._tcp.xyz.example-cdn.com

If no TLSA record is found, the fallback TLSA QNAME would be one of:

*_8443._quic.svc4.example.net

*_8443._tcp.svc4.example.net

7.4. New scheme ServiceMode

Given service URI foo://api.example.com:8443 and record:

```
_8443._foo.api.example.com. SVCB 1 api.example.com.
```

The TLSA QNAME is _8443._$PROTO.api.example.com, where $PROTO is the appropriate value for the client-selected transport as discussed in Section 4 .

7.5. New scheme AliasMode

Given service URI foo://api.example.com:8443 and records:

```
_8443._foo.api.example.com. SVCB 0 svc4.example.net.
svc4.example.net.           SVCB 1 .
svc4.example.net.           A    192.0.2.1
```

The TLSA QNAME is _8443._$PROTO.svc4.example.net (with $PROTO as above). This is the same if the ServiceMode record is absent.

7.6. New protocols

Given service URI foo://api.example.com:8443 and records:

```
_8443._foo.api.example.com. SVCB 0 svc4.example.net.
svc4.example.net. SVCB 3 . alpn=foo,bar port=8004
```

The TLSA QNAME is _8004._$PROTO1.svc4.example.net or _8004._$PROTO2.svc4.example.net, where $PROTO1 and $PROTO2 are the transport prefixes appropriate for "foo" and "bar" respectively. (Note that SVCB requires each ALPN to unambiguously indicate a transport.)

7.7. DNS ServiceMode

Given a DNS server dns.example.com and record:

```
_dns.dns.example.com. SVCB 1 dns.example.com. alpn=dot
```

The TLSA QNAME is _853._tcp.dns.example.com. The TLSA base name is taken from the SVCB TargetName. The port and protocol are taken from the "dot" ALPN value.

7.8. DNS AliasMode

Given a DNS server dns.example.com and records:

```
_dns.dns.example.com. SVCB 0 dns.my-dns-host.net.
dns.my-dns-host.net.  SVCB 1 . alpn=dot
```

The TLSA QNAME is _853._tcp.ns1.my-dns-host.net.

8. IANA Considerations

IANA is instructed to add the following entry to the "Underscored and Globally Scoped DNS Node Names" registry:

RR Type	_NODE NAME	Reference
TLSA	_quic	(This document)

Table 1

9. References

9.1. Normative References

[I-D.draft-ietf-tls-dtls13] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13-43, 30 April 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-dtls13-43>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3436] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, DOI 10.17487/RFC3436, December 2002, <https://www.rfc-editor.org/rfc/rfc3436>.

[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, <https://www.rfc-editor.org/rfc/rfc6698>.

[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, <https://www.rfc-editor.org/rfc/rfc7671>.

[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/rfc/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[SVCB] Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-10, 24 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-10>.

9.2. Informative References

[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, <https://www.rfc-editor.org/rfc/rfc7672>.

[RFC7673]
Finch, T., Miller, M., and P. Saint-Andre, "Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records", RFC 7673, DOI 10.17487/RFC7673, October 2015, <https://www.rfc-editor.org/rfc/rfc7673>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Benjamin M. Schwartz
Google LLC

Email: bemasc@google.com

Robert Evans
Google LLC

Email: evansr@google.com