dnsop
Internet-Draft
Updates: 6698 (if approved)
Intended status: Standards Track
Expires: 4 September 2025

B. M. Schwartz
Meta Platforms, Inc.
R. Evans
Google LLC

3 March 2025

Using DNSSEC Authentication of Named Entities (DANE) with DNS Service Bindings (SVCB) and QUIC
draft-ietf-dnsop-svcb-dane-05

Abstract

Service Binding (SVCB) records introduce a new form of name indirection in DNS. They also convey information about the endpoint's supported protocols, such as whether QUIC transport is available. This document specifies how DNS-Based Authentication of Named Entities (DANE) interacts with Service Bindings to secure connections, including use of port numbers and transport protocols discovered via SVCB queries. The "_quic" transport name label is introduced to distinguish TLSA records for DTLS and QUIC.

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

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 records when one or more CNAME records are present, aliasing either the hostname or the initial TLSA query name, and the resulting server names used in TLS or DTLS.

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 document 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.

The contents of this document apply equally to all SVCB-compatible record types, such as SVCB and HTTPS records. For brevity, the abbrevation "SVCB" is used to refer to these record types generally.

3. Using DANE with Service Bindings (SVCB)

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 document 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).

Resolution security is assessed according to the criteria in Section 4.1 of [RFC6698].

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]. However, domain owners SHOULD NOT place a CNAME record on a SVCB TargetName, as this arrangement is unusual, inefficient, and at risk for deprecation in a future revision.

If any TLSA QNAME is aliased by a CNAME, clients MUST follow the TLSA CNAME to complete the resolution of the TLSA records. (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. Adding a TLSA protocol prefix for QUIC

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

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

When this text was written, 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 document updates the above sentence as follows:

The transport names defined for this protocol are "tcp" (TLS over TCP [RFC8446]), "udp" (DTLS [RFC9147]), "sctp" (TLS over SCTP [RFC3436]), and "quic" (QUIC [RFC9000]).

5. Operational considerations

5.1. Recommended configurations

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

```
alias.example.                  HTTPS 0 xyz.provider.example.
www.alias.example.              CNAME xyz.provider.example.
xyz.provider.example.           HTTPS 1 . alpn=h2 ...
xyz.provider.example.           A     192.0.2.1
_443._tcp.xyz.provider.example. TLSA  ...
```

If the service needs its own SvcParamKeys, it cannot use CNAME or AliasMode, so it publishes its own SVCB ServiceMode record with SvcParams that are compatible with the provider, e.g.:

```
_dns.dns.example. HTTPS 1 xyz.provider.example. ( alpn=h2 ...
                                                  dohpath=/doh{?dns} )
```

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

```
_443._tcp.xyz.provider.example. CNAME dane-central.provider.example.
dane-central.provider.example.  TLSA  ...
```

Any DANE certificate usage mode is compatible with SVCB, but the usage guidelines from Section 4 of [RFC7671] continue to apply.

5.2. Unintended pinning

As noted in Section 6 of [RFC7671], DANE encounters operational difficulties when the TLSA RRset is published by an entity other than the service provider. For example, a customer might copy the TLSA records into their own zone, rather than publishing an alias to the TLSA RRset hosted in the service provider’s zone. When the service subsequently rotates its TLS keys, DANE authentication will fail, resulting in an outage for this customer. 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 prevent 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 avoid publishing SvcParams for a TargetName that they do not control, and service operators should exercise caution when making incompatible configuration changes.

6. Security Considerations

The use of TLSA records specified in this document is independent for each SVCB connection attempt. In environments where DANE is optional, this means that the client might use DANE for some connection attempts but not others when processing a single SVCB RRSet.

This document only specifies the use of TLSA records when all relevant DNS records (including SVCB, TLSA, and CNAME records) were resolved securely. If any of these resolutions were insecure (as defined in Section 4.3 of [RFC4035]), the client MUST NOT rely on the TLSA record for connection security. However, if the client would otherwise have used an insecure plaintext transport, it MAY use an insecure resolution result to achieve opportunistic security.

Certain protocols that can run over TLS, such as HTTP/1.0, do not confirm the name of the service after connecting. With DANE, these protocols are subject to an Unknown Key Share (UKS) attack, in which the client believes it is connecting to the attacker’s domain, but is actually connecting to an unaffiliated victim domain [I-D.barnes-dane-uks-00]. Clients SHOULD NOT use DANE with vulnerable protocols. (HTTP/1.1 and later and encrypted DNS are not normally vulnerable to UKS attacks, but see Appendix A for some important exceptions.)

7. Examples

The following examples demonstrate Service 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.cdn.example.
xyz.cdn.example.     A     192.0.2.1
```

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

7.3. QUIC and CNAME

Given service URI https://www.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.cdn.example.
```

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.cdn.example
* _8443._tcp.xyz.cdn.example

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. DNS ServiceMode

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

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

The TLSA QNAME is _853._tcp.dns.my-dns-host.example. The port and protocol are inferred from the "dot" ALPN value.

7.5. DNS AliasMode

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

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

The TLSA QNAME is _853._quic.dns.my-dns-host.example. The port and protocol are inferred from the "doq" ALPN value.

7.6. 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 .

7.7. 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.

7.8. 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.)

8. IANA Considerations

IANA is requested to add the following entry to the "Underscored and Globally Scoped DNS Node Names" registry ([RFC8552], Section 4):

RR Type	_NODE NAME	Reference
TLSA	_quic	(This document)

Table 1

9. References

9.1. 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, <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>.

[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, <https://www.rfc-editor.org/rfc/rfc4035>.

[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>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

[SVCB] Schwartz, B. M., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-12, 11 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-12>.

9.2. Informative References

[I-D.barnes-dane-uks-00]
Barnes, R., Thomson, M., and E. Rescorla, "Unknown Key-Share Attacks on DNS-based Authentications of Named Entities (DANE)", Work in Progress, Internet-Draft, draft-barnes-dane-uks-00, 9 October 2016, <https://datatracker.ietf.org/doc/html/draft-barnes-dane-uks-00>.

[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>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/rfc/rfc7858>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/rfc/rfc8094>.

[RFC8441] McManus, P., "Bootstrapping WebSockets with HTTP/2", RFC 8441, DOI 10.17487/RFC8441, September 2018, <https://www.rfc-editor.org/rfc/rfc8441>.

[RFC8552] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <https://www.rfc-editor.org/rfc/rfc8552>.

[RFC9103] Toorop, W., Dickinson, S., Sahib, S., Aras, P., and A. Mankin, "DNS Zone Transfer over TLS", RFC 9103, DOI 10.17487/RFC9103, August 2021, <https://www.rfc-editor.org/rfc/rfc9103>.

[RFC9110] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

Appendix A. Unknown Key-Share Attacks

In the Unknown Key-Share (UKS) Attack [I-D.barnes-dane-uks-00], a hostile domain ("attacker.example") claims the IP addresses and TLSA records of another domain ("victim.example"). A client who attempts to connect to "attacker.example" will actually be connecting to "victim.example".

The client then sends some commands or requests over this connection. If the server rejects these requests, or if the attacker could have forwarded these requests itself, the attack confers no advantage. However, if the client issues commands that the attacker could not have issued, and the victim does not ignore these requests, then the attack could change state at the victim server, reveal confidential information to the attacker (e.g., via same-origin data sharing in the client), or waste resources.

Here are some examples of requests that the attacker likely could not have issued themselves:

* Requests authenticated using a TLS Client Certificate or other credential that is bound to the connection but not the domain.

* Requests that are only permitted if they appear to come from a particular IP range.

This section lists some protocols that can be used with SVCB, analyzes their vulnerability to this attack, and indicates any resulting restrictions on their use:

* HTTP/0.9 and HTTP/1.0: *Vulnerable*

  - Clients MUST NOT use TLS Client Authentication with DANE and these protocol versions.

    o Example attack: "https://attacker.example/" fetches "/profile" in Javascript. The second request is directed to "victim.example" and authenticated by a client certificate, revealing the user's profile to the attacker.

  - Use of these protocol versions with DANE is NOT RECOMMENDED.

* HTTP/1.1 and later: *Slightly Vulnerable*

  - The CONNECT method ([RFC9110], Section 3.6) MUST NOT be used on a connection authenticated with DANE.

    o Example attack: "attacker.example" advertises a CONNECT proxy service to existing customers of the "victim.example" proxy, which is access-controlled by client IP. To reduce its own operating costs, "attacker.example" uses UKS to send users back to "victim.example", resulting in the attacker's service appearing to work but silently consuming clients' transfer quota on "victim.example".

  - Clients MAY use all other methods with DANE, including Extended CONNECT [RFC8441]. These methods are defended from misdirection attacks by server verification of the Host or :authority header ([RFC9110], Section 7.4).

* DNS over TLS, DTLS, or QUIC [RFC7858][RFC8094][RFC9250]:

  - For resolution: *Not Vulnerable*

    o DNS resolution does not change state at the server, reveal confidential information to the attacker, or waste significant resources.

- For other uses: *Mitigation Required*

  - When using DNS for other purposes such as zone transfers [RFC9103], clients relying on DANE for server authentication MUST NOT use a client certificate that is authorized by multiple potentially hostile servers.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Benjamin M. Schwartz
Meta Platforms, Inc.
Email: ietf@bemasc.net

Robert Evans
Google LLC
Email: evansr@google.com