TLSA usage with raw public keys and non-TLS

draft-ietf-dane-rawkeys-00

John Gilmore and Paul Wouters

IETF-90, Toronto 2014

How to use these protocols together

The TLSA record - RFC 6698

```
"The TLSA DNS resource record (RR) is used to associate
a TLS server certificate or public key with the domain
name where the record is found"
```

Raw public keys - RFC 7250

```
"This document specifies a new certificate type and two
TLS extensions for exchanging raw public keys in Transport
Layer Security (TLS) and Datagram Transport Layer Security
(DTLS). The new certificate type allows raw public keys to
be used for authentication."
```

non-TLS protocols - RFC XXXX

Combining TLSA and Raw Public Keys only covers port 443

- RFC 6698 and RFC 7250 only cover (D)TLS (port 443)
- Non-443 ports require their own document, re-using TLSA format, eg:
    - draft-ietf-dane-smtp-with-dane
    - draft-ietf-dane-srv

TLSA records require PKIX

- "This document only applies to PKIX certificates"
- "The certificate usages defined in this document explicitly only apply to PKIX-formatted certificates"

- A raw public key ("SPKI") is not a PKIX certificate.
- Need co-existance of Classic PKIX certs and raw public keys

TLSA Certificate Usage Registry

Value	Acronym	Short Description
0	PKIX-TA	CA constraint
1	PKIX-EE	Service certificate constraint
2	DANE-TA	Trust anchor assertion
3	DANE-EE	Domain-issued certificate

RFC 7218 named the RFC 6698 values, but did not solve the ambiguity of PKIX in RFC 6698

draft-ietf-dane-rawkeys-00

Draft would update RFC 6698 to enable raw public keys in TLS:

- Relax TLSA RR for use without "PKIX certificates"
- Allow TLSA RR usage 3 (DANE-EE) to match a raw public key

No change to wire formats. Extends existings formats to work in a new situation.

draft-ietf-dane-rawkeys-00

Draft would remove restrictions in RFC 6698 that impede interoperability:

- Relax TLSA RR limitation to authenticating TLS
- Provide method to securely publish raw public keys in a TLSA RR

No change to wire formats. Codifies how to interpret the wire formats we already have.

Allow other protocols to use TLSA RR without more RFC's

- Any applications that wish to use TLS (with raw public keys) can use TLSA
- Any non-TLS protocol that wish to securely publish raw key can use TLSA

```
_1234._tcp.www.example.com IN TLSA 3 1 0 BLOB
```

Whether port 1234 uses TLS or another protocol should not matter

draft-ietf-dane-rawkeys-00 discussion items

- Should IETF standards prohibit application behavior even when that prohibition does not promote interoperability? (No)
- Should non-TLS or non-PKIX crypto protocols use a new DNS RRtype, even if they need no more fields than the TLSA record already has? (No)
- Should raw public keys be matched with usage type 3 (DANE-EE) or with a usage type such as 4 that has not previously been specified? (Use 3)
- Should every protocol that uses TLSA records need its own RFC? (not really)

draft-ietf-dane-rawkeys-00: Relax TLS and PKIX restrictions in RFC 6698

Allow secure publishing of any non-PKIX public key with a TLSA record with:

- Certificate Usage 3 (DANE-EE)
- Selector 1 (SubjectPublicKeyInfo - "SPKI")
- Match 0 (Full public key)