Raw Public Keys

Often the difficulty of obtaining a proper certificate chain anchored on a trusted authority is avoided by using a so-called self-signed certificate. These are free and they are shorter than a typical 3-link certificate chain.

Recall that the point of a certificate chain is to bind a public key to an identity. But simply stating "This is who I am and here is my public key" doesn't cut it. Anyone can claim any identity, generate a key pair, and sign their own certificate. Proves nothing, but self-signed certificates are quite commonly used. Typically when there exists some out-of-band method (like TOFU – see below) of binding the public key to an identity, as can arise in an Internet of Things context.

However if that is the case it would be simpler just to send the public key (or indeed a pointer to it - see RFC7924), without all of the extra baggage of a full certificate. And the TLS1.3 specification does support the use of raw public keys (RFC 7250), for both servers and clients.

Implementation

As is usual it is all negotiated via extensions. The client in its client Hello indicates a willingness to accept a raw public key from the server, and also optionally that it can itself offer a raw public key. The server responds with its own extensions in its server Hello indicating its agreement.

To simplify things in our implementation the server or client will simply rip the public key from an existing stored certificate chain or self-signed certificate generated by OpenSSL, and transmit that rather than the full certificate. And the savings can be substantial, particularly in the context of bloated Post-Quantum certificates with their attendant large signatures. This will work well with a TOFU (Trust On First Use) approach to establishing trust, where the full certificate chain may be used in a first connection, but only the by-now trusted public key is used in subsequent connections. Which if you think about it brings us quite close to ticket-based resumption, but can be used over a period longer than a week.

So, as long as the deployer has a good understanding of the security implications that arise from the use of raw public keys, they can have their uses.

So they are now supported!