Time to implement less common features

Post handshake authentication. After the handshake has completed the server may at any time decide to issue a Certificate Request message. However this will only be accepted if the client sent a **post_handshake_auth** extension in its original client hello, indicating its willingness to supply a certificate post handshake. This willingness does not have to be responded to by the server.

Why would you want to do this? Well one reason arises from our IBE-PSK proposal blogged about recently. A resumption/PSK handshake does not allow for certificate based server or client authentication (indeed by design there is no PKI involvement at all). But whereas a PSK might authenticate the server, it may not authenticate the client, exactly the circumstance that arises with an IBE-PSK. So a client that wants to do a PKI-based authentication (and might have hardware support for it) must do it post-handshake.

Anyway, its part of the TLS1.3 standard, so we should really implement it regardless.

One wrinkle is the requirement for the certificate request to now include a non-zero **certificate_request_context** field, to uniquely identify each such request, and prevent replay attacks. 32 random bytes will suffice. When the client responds with a certificate message it must include the same context so that request and response can be matched up.

In fact the client responds with three messages, certificate, certificate verify and client finish. The certificate verify message includes a signature on the transcript, but what transcript??

In section 4.4.1 of the standard we find the answer "Note, however, that subsequent post-handshake authentications do not include each other, **just the messages through the end of the main handshake**."

So its the transcript up to and including the original client finish message in the main handshake, plus the Certificate Request that we are responding to. See the table at the end of section 4.4.

There is no really good reason for accepting more than one Certificate request, so our client will only respond to the first one.

It may be appropriate to send a ticket only after the client authenticates, so that the ticket captures the client-side authentication.

Immediately after receiving a Certificate request, the client must respond with Certificate, Certificate Verify, and Finish. Note that a lot can go wrong here – the certificate chain may be bad, the verification may not work out, so alerts may have to be fired off.

So lets do it!