OK, Time to stop flaffing around...

So I set a different challenge and tried to get a little bit more real. Rather than our client talking to our server, instead complete a TLS1.3 client negotiation with a real external TLS1.3 server. The server I chose is a test server provided at *tls13.cloudfare.com*, with the socket connection on the standard port 443.

My first attempt ended in dismal failure – I got an alert response from the server that indicated it wasn’t happy with my initial Client Hello. But at least it was a recognisable response. I quickly fixed the problem and got a lot further the second time.

As I indicated in my last blog a big issue is the client side handling of the certificate chain sent by the server. So the connection to *tls13.cloudfare.com* was an opportunity to see what a real certificate chain looked like. This chain had 3 elements: The server cert itself (the “leaf” certificate), which was signed by an intermediate certificate, which was in turn signed by a root certificate, the certificate of the Certificate Authority (CA). However the root certificate was not included, it was simply referred to as the “issuer” of the intermediate cert. Apparently this structure is quite common – server/intermediate/root, although there could be multiple intermediates.

So how to find the root cert to complete the chain and check it out? Well the root cert should be found in my local store of approved CA certs. And right enough in my Ubuntu distribution there is a file */etc/ssl/certs/ca-certificates.crt* which in a single file contains all of the worlds CA root certificates. So given the “issuer” a simple linear search through this file quickly found the right certificate. These root certificates are always self-signed.

In this case the root certificate was issued by "Baltimore CyberTrust Root", and the associated country was IE – Ireland. That brought back memories..

Back in 1998 at the height of the dotcom boom an ex-footballer and an academic set up what became Baltimore Technologies. At one time their capitalisation was 13.8 billion Euro. There main line of business was as a Certificate Authority. I remember visiting them in their trendy offices built under a railway bridge in the heart of Dublin. Even then I knew that setting up yet another Certificate Authority did not really constitute a viable long-term business plan. And right enough when the dotcom bubble burst, Baltimore Technologies spectacularly imploded.

So it was interesting to see that their root certificate is still in use. I did note that it was self-signed using SHA1, and hence should really be deprecated at this stage. But there it was, still in use and valid until 2024. And that’s the problem with the X509 certificate specification. It was designed more than 20 years ago, and hence it is not surprising that it is beginning to look inadequate. Various extensions have been approved in the interim, but that doesn’t help with 20-year old certificates that are still out there in the wild.

Anyway once the certificate chain checked out OK, the TLS1.3 handshake completed successfully, which was very gratifying. So at this stage we have a TLS1.3 client that works with at least one real TLS1.3 server. Next we need to test it against a wider range of servers and make the necessary adjustments so that it becomes a lot more robust.