Short-lived certificates

Short-lived leaf certificates are now offocially a thing. Lets Encrypt are issuing certificates with a lifetime of only 6 days. Google and Mozilla have just this year proposed certificates with lifetimes of just 24 hours. This is a big move from what we were used to, certs which had lifetimes measured in years. Its a move which appears to be gaining momentum.

Its a wave I think TiigetTLS should ride, as these short-lived certificates are proposed as a simple solution to the certificate revocation issue.

The point being that if the delay between a breech occurring, it being discovered, a CRL being issued, and a CRL being consumed, is longer than the lifetime of the certificate, then CRLs (and also OCSP) become irrelevant.

Clearly some automated process would need to be put in place to update certificates in this way. But now if even in the open Internet this is considered feasible, in a closed-world setting it would be even easier.

To get ready for short-lived certificates we have improved TiigerTLS certificate validity checking to ensure (to the second) that a certificate is within its validity period, between its start and its expiry time.