Investigations of time synchronization in TLS/DTLS (Renzo)

Relative time:
 * TLS Resumption: upper limit of 24 hs suggested. How to enforce?
 * TCP User timeout (~15 minutes), Keepalive Time (~2 hours). Optional.
 * TCP Retransmission Timer . Needs measuring RTT, coarse grain clocks are ok.

Absolute/Wallclock Time:

* TLS/DTLS v1.2 ClientHello needs current time and date. But not really, is not required to be set correctly by the basic TLS protocol (no security implications. privacy issues could be, because of fingerprinting). In TLS v1.3-draft a random number is used instead.

* TLS Ciphersuites with Certificates. All ciphersuites that use certificates (e.g. RSA_WITH_X DH/DHE/ECDH/ECDHE_RSA/DSS/ECDSA, GHOST) will have problems validating them:
  - Certificate Validity period: Even if the object can validate the whole certificate chain (intermediate certificates can be signed with different algorithms), the certificate validity period (notBefore, notAfter) needs the current time. [Fallback: notbefore=min, notafter=max??]
  - Revocation: also needs current time notion: either an updated/fresh CRL, or any other OOBand mechanism (will need to be
'fresh') [fallback: no revocation?]
  - Fallback to this problem: rely on a third party to do certificate validation (will need the party to be online too)
  - Conclusion: no certificate validation can be done totally offline if the node do not have wall-clock time notion (and will exist the chance of accepting a revoked cert).

* TLS Ciphersuites w/ Kerberos. Has a timestamp (on the ticket) and needs to validate it.

* TLS Ciphersuites DH_ANON and other anonymous: Do not need time information. Vulnerable to man-in-the-middle attacks. Authentication would have to be assured by other means than TLS layer. (rfc5246#appendix-A.5) "Note that using non-anonymous key exchange without actually verifying the key exchange is essentially equivalent to anonymous key exchange, and the same precautions apply"

* OK. TLS Ciphersuites SRP (5054). With certificates same problems as before. Without digital signatures, server is authenticated by possession of the SRP verifier.
* OK. PSK ciphersuites can be used for authentication.

Problems:

* Problem of SRP and PSK: we already have to share the crypto material with the party we are trying to authenticate.
* Problem statement: Without reliable wallclock time information and no previous crypto material with the other party there does not exist any TLS ciphersuite that provides an authenticated channel between these parties (client/server).

* Authentication without time nor pre-shared-crypto material can be done but will need a TTP (at least trusted for the party that wants to authenticate the other, if its mutual authentication the party will have to be trusted by both or we will one TTP for each), and will involve contacting the TTP on the protocol execution ("online").