## Sammanfattning 2 - Komplettering

**Hur fungerar digital signering?**

Om en sändare A vill generera en signatur för att B ska kunna verifiera A's identitet, och se till att meddelandet M inte har förändrats, behöver A använda sig av digital signering.

Detta görs genom att A skickar två delar. Den ena delen är bara M i sig. Den andra delen är en hash-digest av M, som sedan krypteras med A's privata nyckel. A skickar alltså [M],[Encrypted(Hash(M))] till B (omvänt till en "vanlig" kommunikation mellan A och B).

När B tar emot A's meddelande utförs först en hash av M, och en dekryptering av Encrypted(Hash(M)). Båda delarna ska nu vara hash-digests, och om de är likadana innebär det att den digitala signaturen är giltig.

Detta fungerar under antagandet att A är den enda som känner till den privata nyckeln i fråga.

**Hur fungerar digital certifikat?**

Ett digitalt certifikat använder digital signering och används för att bekräfta identiteten hos en nyckelägare - t.ex. A i ovanstående text. I många fall utfärdas ett sådant certifikat hos en s.k. CA (Certificate Authority) som agerar som en tredje part i kommande kommunikation.

En CA signerar certifikatet precis som A gjorde med M i ovanstående fråga, vilket gör att alla som kommunicerar med ägaren av ett certifikat, kan verifiera dess giltighet genom att använda CA's publika nyckel (precis som B gjorde ovan).

Detta fungerar under antagandet att båda parterna i en kommunikation litar på given CA.

**TLS och HTTPS**

TLS (Transport Layer Security) används för säker kommunikation mellan två enheter genom TLS certifikat. Detta är ett digital certifikat som vanligen utfärdas av en CA (som beskrivet ovan) och innehåller bland annat en publik nyckel för att säkerställa den digital signaturen. Vid klient-server kan ett TLS-certifikat finns på servern som klienten kan verifiera innan kommunikation inleds - en del av den s.k. TLS-handskakningen.

TLS-handskakningen för klient-server inleds med att servrarna förser klienten med sitt certifikat, och låter klienten verifiera detta. Klienten svarar med sitt eget certifikat och en bekräftelse att serverns certifikat är giltigt. Efter detta genereras en pre-master secret (stort tal) hos en av parterna och skickas krypterat över (då de nu känner till varandras publika nyckel). Detta tal används för att generera två sessionsnycklar (write keys) som används för att kryptera meddelanden i kommande kommunikation.

Fortsättningsvis är HTTPS en implementation av TLS ovanpå de osäkra HTTP-protokollet. HTTPS används för att kommunicera över internet på ett säkert sätt.