# DD1389 Labb 5 Rapport

1. Det finns två generella sätt att leverera certifikatet till datorn/webbläsaren
   1. Root certifikatet kan levereras manuellt som kallas för ”Out of Band”
      1. Detta kan göras genom att överföra genom USB direkt till datorn, eller under systeminstallering eller genom ett verktyg som IT har gjort. Detta görs utan internet.
   2. Certificate Pinning
      1. Detta sker hos webbläsaren som håller koll på källkoden till certifikaten för publika litade på certifikatutfärdare. Detta innebär att vid koppling till en HTTPS sida, så gör webbläsaren en kontroll att certifikatet matchar det av de hårdkodade certifikatutfärdarna.
2. Certifikaten innehåller information gällande ägaren och utfärdaren. Dessa saker bland annat kan vara
   1. Identiteten på ägaren, exempelvis namn
   2. Ägarens publika nyckel
   3. Giltighetsperiod
   4. Certifikatets id
   5. Användningsområde
   6. Utfärdarens identitet
   7. Utfärdarens signatur
   8. Utfärdarens privata nyckel

När det kommer till autentisering och verifiering så är användarens publika nyckel det viktigaste. Den publika nyckeln som används för att kontrollera att certifikatet faktiskt utfärdats av certifikatets utfärdare.

1. En trust chain sker då varje del av hårdvaran och mjukvaran valideras genom hela kedjan från end till rotcertifikatet. Alla mellanlager av certifikat kontrolleras och valideras och på det sättet så skapas det säkerhet. Detta innebär att hårdvaran kommer endast köra program som är signerade utav en litad källa.
2. Skulle det vara så att programkoden läcks ut så skulle någon utomstående ha tillgång till certifikatet. Detta innebär att denna person kan använda certifikatet och då framstå att servern är någon annans. Dvs. om lösenordet till person A:s certifikat läcks ut, så kan person B använda den för sin server och då framstå till klienten att denna server är server A. Detta blir osäkert såklart då klienten tror att den kopplar till server A, när den egentligen kopplar till server B och kan utsättas för attacker.
   1. HTTPS: I HTTPS så överförs kommunikationen mellan server och klient med användning av en TLS (Transport Layer Security). Autentiseringen och därmed säkerheten uppnås genom användning av digitala certifikat som visar legitimitet.
   2. TLS: TLS protokollet implementerar användning av digitala certifikat med kryptografi. Detta tillåter ett lager av säkerhet vid kommunikation mellan klient och server. Digitala certifikaten kan användas för att säkerställa serverns autenticitet.
   3. X.509 är publika nyckel certifikaten som används i TLS protokollet. Certifikatet binder en publik nyckel till en digital signatur. Certifikatet innehåller för övrigt annan information kring ägaren och annat. Den publika nyckeln som kan vara i RSA formatet är signerad av en certifikatutgivare eller självsignerad.
   4. En signatur är likt en vanlig handskriven signatur och erbjuder mottagaren en anledning att tro att meddelandet var skickad av den påstådda avsändaren.
   5. RSA är en krypteringsalgoritm som använder sig av nycklar (publika och hemliga) för att kryptera och dekryptera. Denna egenskap utnyttjas för att kunna signera certifikat och på så sätt säkerställa att avsändaren är den som framstås. Den publika nyckeln används för att signera och kryptera med, medan den hemliga används för att dekryptera och undersöka autenticitet.
   6. Privat nyckel är den nyckel som används i RSA algoritmen för att dekryptera ett meddelande från en avsändare. Dekrypteringen funkar endast ifall privata och publika nyckelparet stämmer överens med varandra, och på så sätt kan autenticitet säkerställas ifall den hemliga nyckeln lyckas dekryptera meddelandet.
   7. Publika nyckeln är den nyckel som används av avsändaren för att kryptera meddelandet som sedan endast kan dekrypteras med en privat nyckel. På så sätt kan en avsändare ”signera” ett meddelande och bekräfta sin autenticitet.
   8. AES är standardiserad krypteringsalgoritm som använder antingen 128-bit eller 256-bit nycklar. AES som utgavs av NIST utmärks för dess säkerhet, komputeringseffektivitet och minneseffektivitet och flexibilitet att kunna användas på alla möjliga system och applikationer.
   9. MD5 och SHA är två hashfunktioner som kan användas för certifikat för att kryptera meddelandet. MD5 dock anses inte vara säker då man har lyckat skapa ett falskt certifikat som lyckats verka legitimt vid kontroll. SHA-1 algoritmen används fortfarande utspritt även fast den med har blivit bruten. Andra varianter av SHA algoritmen har dock skapats som är än idag säkra och kan användas för kryptering av certifikat.