Vad är SSL och hur fungerar det?

SSL (Secure Sockets Layer) är den standard av säkerhetsteknologi som används för upprättande av en krypterad länk mellan en webbserver och en webbläsare. SSL ser till att all data som skickas mellan en webbserver och webbläsare förblir privat och krypterad. SSL är en branschstandard och används av miljontals webbplatser för att kunna skydda deras transaktioner med kunder online.
Ett SSL-certifikat fungerar ungefär som ett slags bank ID, fast för webbplatser och används tillexempel för att skydda transaktioner mellan kunder och webbutiker.

Vad är ett SSL-certifikat?

För att skapa en SSL-anslutning på en webbsida krävs det ett **SSL-certifikat**. Ett SSL-certifikat fungerar ungefär som ett slags bank ID, fast för webbplatser. Om du vill aktivera SSL på din webbserver måste du verifiera den genom att fylla i ett antal frågor om din webbplats och ditt företag. Din webbserver skapar sedan två kryptografiska nycklar – en privat nyckel och en offentlig nyckel.
Den ena nyckeln, **Public Key** behöver inte vara hemlig och placeras med en **Certificate Signing Request (CSR)** i en datafil tillsammans med dina uppgifter. Under ansökningsprocessen för ett SSL-certifikat kommer certifikatutfärdare validera dina uppgifter. Om du godkänns kommer de sedan att utfärda ett SSL-certifikat som innehåller dina uppgifter och gör att du kan använda SSL. Din webbserver matchar ditt SSL-certifikat till din privata nyckel. Din webbserver kommer då att kunna etablera en krypterad länk mellan webbplatsen och din kunds webbläsare.
Komplexiteten i SSL-protokollet förblir osynligt för dina kunder. Istället så har webbläsaren ge en viktig indikator som låter användaren veta att de är skyddade av en SSL-krypterad session (**SSL kryptering**).
Ett typiskt SSL-certifikat kommer att innehålla ditt domännamn, ditt företagsnamn, din adress, din stad, din stat och ditt land. Det kommer också att innehålla datum för när certifikatet skapades och uppgifter om certifikatutfärdaren som ansvarar för utfärdandet av certifikatet.

När en webbläsare ansluter till en säker webbplats kommer det att hämta webbplatsens SSL-certifikat och kontrollera att det inte har gått ut, och om det har utfärdats av en certifikatutfärdare webbläsaren litar på, och att den används av webbplatsen för vilket det har utfärdats. Om webbplatsen misslyckas med någon utav dessa kontroller kommer webbläsaren att visa en varning till slutanvändaren där det står att webbplatsen inte är säkrad med SSL.