

Installation och användning av SSL-certifikat: en vägledning





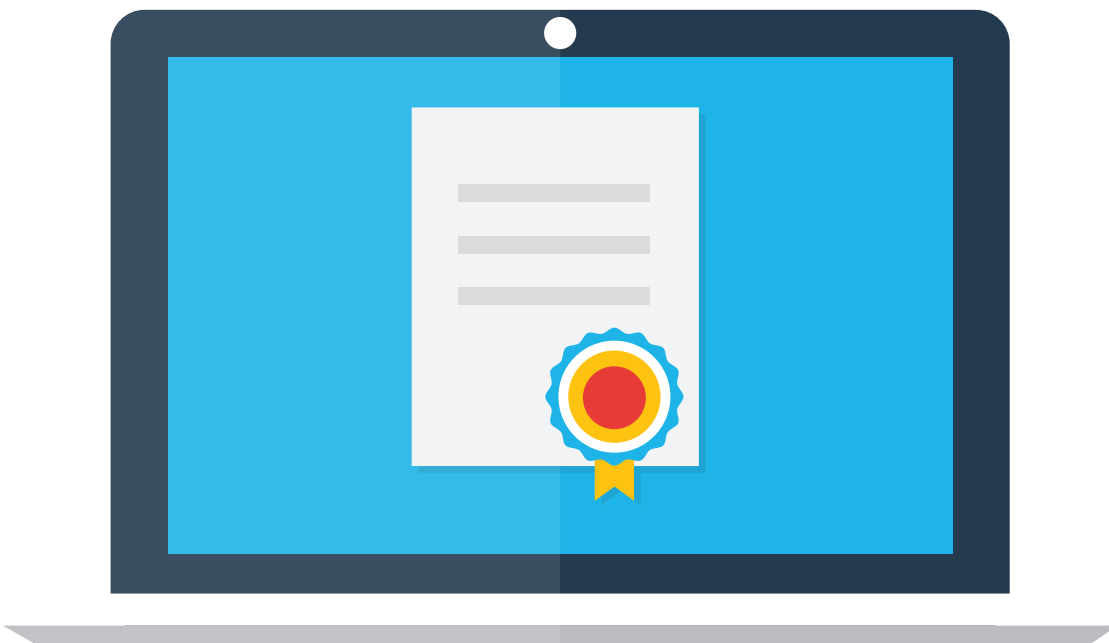
Nu har du alltså köpt ett SSL-certifikat.

Det är det första av många steg mot att säkra webbplatsen. Tyvärr är det vanligt att certifikaten inte installeras ordentligt, att känsliga sidor glöms bort och att formulärdata skickas okrypterade, vilket innebär att många webbplatser är sårbara för angrepp.

Därför har Symantec sammanställt följande tips om hur du gör helt rätt från första början. Vi lotsar dig över de mer stormiga haven och varnar för blindskären som kan få SSL att gå på grund. Ditt SSL-certifikat är din livbåt till en säkrare och tryggare webbplats för dig, din personal och dina kunder.

Det finns bara ett sätt att installera SSL – det rätta!

Som så många andra företag har ni insett behovet av att köpa ett SSL-certifikat. Det är det första och viktigaste steget. Nu måste du installera det korrekt. Om era kunder inte känner sig fullständigt säkra på webbplatsen vill de helt enkelt inte handla något där.





TIPS 1 - Förbered den privata nyckeln och begäran om certifikatsignering



Innan ett digitalt certifikat installeras måste den privata nyckeln skapas, och från den en begäran om certifikatsignering (CSR) för servern där certifikatet ska installeras. Därefter skickas certifikatbegäran in för registrering av ett certifikat. Så här går det till.

Om du har IIS 6 eller senare eller en Red Hat Linux-server kan du hämta vårt verktyg – [Symantec SSL Assistant](#) – och följa de användarvänliga anvisningarna. En lista med instruktioner om hur en certifikatbegäran skapas med andra servrar finns i artikeln [skapa en certifikatbegäran](#). Om du vill registrera dig för någon av Symantecs SSL-certifikattjänster behöver du ta fram följande uppgifter:

- Certifikatets giltighetsperiod: ett, två eller tre år
- Hur många servrar som hanterar en viss domän (högst fem)
- Serverplattformen
- Organisationen, organisationsenheten, adressen
- Betalningsuppgifter och en kontaktperson för fakturafrågor
- Nätverksnamnet. Detta är värd- och domännamnet, t.ex. [www.mindomän.se](#) eller [webbmejl.mindomän.se](#)
- En e-postadress där Symantec kan nå er för att få uppgifterna verifierade
- En begäran om certifikatsignering (CSR) som har genererats på servern som ska skyddas

Följ anvisningarna i tips 3 när certifikatet har levererats.

Om er server inte finns med på listan, eller om du behöver mer information, kan du läsa serverdokumentationen eller kontakta serverleverantören. Tala med IT-administratörerna om du inte vet vilket program som används på servern.

Skicka in certifikatbegäran – även huvud och fot – när du registrerar dig:

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



TIPS 2 - Installera ett SSL-certifikat på rätt sätt!



Ska du installera ett SSL-certifikat för första gången och känner att marken gungar lite under fötterna? Oroa dig inte. Det är mycket enklare än du tror. Låt oss titta närmare på hur ett certifikat installeras på en server med Symantecs hjälp.

Proceduren ser likadan ut på alla servrar:

Steg 1 – Spara certifikatet.

Följ anvisningarna i bekräftelsebrevet om hur du sparar SSL-certifikatet på skrivbordet från den webbadress som anges i e-postmeddelandet. Då sparar du både certifikatet och de mellanliggande certifikatutfärdarnas certifikat som du behöver.

Steg 2 – Installera eller flytta till en certifikatsmapp.

Steg 3 – Konfigurera certifikatet på webbplatsen.

Steg 4 – Referera till certifikatet.

[Klicka här](#) om du vill ha mer detaljerad information och noggranna anvisningar om varje servertyp.

För största möjliga nytta av SSL-certifikatet bör du även lägga in Norton Secured-sigillet på din webbplats. Då känner kunderna sig tryggare när de gör affärer med dig.

Det är bara att kopiera och klistra in de relevanta raderna från Symantecs Norton Secured-sigillsidor om du vill lägga till sigillet på din webbplats. Det finns lättbegripliga anvisningar via länken i slutet av det här tipset. Där förklarar vi även hur du kan testa certifikatet med installationskontrollen för certifikat genom att ange ditt domännamn.

Nu är SSL-certifikatet installerat och klart att använda!

Har du kört fast?

Symantec har en mängd olika filmer om olika servrar: [Visa handledningarna](#)

Kontrollera installationen

Ange bara webbadressen till servern som du vill kontrollera: [Kontrollera installationen](#)

Generera webbplatsens sigill

Installationsanvisningar för Norton Secured-sigillet: [Generera sigillet](#)

Felsökning

Besök Symantecs supportwebbplats: [Kontakta supporten](#)



TIPS 3 - Skydda de privata nycklarna – och välj det bästa alternativet



Offentliga och privata nycklar är väsentliga delar av SSL-funktionen. Den privata nyckeln hålls hemlig på din server och används för att kryptera allting på webbplatsen. Den offentliga nyckeln som finns i certifikatet är en annan del av webbplatsens identitet, t.ex. ditt domännamn och information om organisationen.

Behandla de privata nycklarna som oersättliga tillgångar. Låt bara betrodda kolleger eller anställda hantera dem, och så få som möjligt. Tänk dig att du vore bankdirektör: skulle du lämna ut nycklarna till valvet till vem som helst? Nej. Här är därför några handfasta råd:

- **Generera privata nycklar på en betrodd server.** Låt inte någon utomstående göra det!
- **Lösenordsskydda de privata nycklarna** för att förhindra att de avslöjas om de lagras på säkerhetskopieringssystem.
- **Förnya certifikaten varje år** – och skapa alltid nya privata nycklar på samma gång.

Storleken på den privata nyckeln påverkar i hög grad den kryptografiska "hälsningen" som används för att etablera säkra anslutningar. Det är inte säkert att använda en för kort nyckel, men alla åtgärder kan sinkas av en nyckel som är för lång.

ECC (Elliptic Curve Cryptography) röner allt mer intresse, eftersom tekniken ger god säkerhet med kortare nyckellängder. Symantec erbjuder ECC med nyckelstorlekar som har betydligt färre bitar än vad RSA och DSA kräver, men ändå är tekniken mer än 10 000 gånger svårare att knäcka (256 bitar för ECC motsvarar den kryptografiska styrkan hos RSA med 3 072 bitar). ECC ger högre säkerhet med kraftigt reducerade prestandakrav på servern, och detta minskar antalet processorcykler som krävs för serverns kryptografiska beräkningar.

Det finns mer information om ECC på sidan 7.



TIPS 4 - Avlägsna alla svaga länkar i kedjan



I de flesta SSL-installationer räcker inte enbart servercertifikatet till: tre eller fler certifikat krävs för att upprätta en komplett förtroendekedja. En certifikatkedja består av alla de certifikat som krävs för att certifiera det objekt som befinner sig längst ut i kedjan.

I praktiken omfattar denna kedja ändpunktscertifikatet, certifikaten för mellanliggande certifikatutfärdare och rotcertifikatutfärdarens certifikat.

Processen för att verifiera äktheten och giltigheten hos ett nyligen mottaget certifikat innebär att samtliga certifikat kontrolleras, från den universellt betrodda rotcertifikatutfärdaren via eventuella mellanliggande certifikatutfärdare och ned till det certifikat som just har mottagits – ändpunktscertifikatet. Det går bara att lita på ett certifikat om varje certifikat i dess kedja har utfärdats och verifierats på lämpligt sätt.

Ett vanligt misstag är att konfigurera ändpunktscertifikatet korrekt men glömma bort att inkludera de mellanliggande certifikatutfärdarnas certifikat. Kontrollera om de mellanliggande certifikatutfärdarna har installerats korrekt genom vår [certifikatskontroll](#).



TIPS 5 - RSA, ECC och varför nyckellängden är viktig



ECC (Elliptic Curve Cryptography) erbjuder ditt företag ökad säkerhet och bättre prestanda än nuvarande krypteringsmetoder.

Tekniken har godkänts av USA:s regering och rekommenderas av National Security Agency. ECC skapar krypteringsnycklar utifrån idén om att använda punkter på en elliptisk kurva för att definiera ett par med en offentlig och en privat nyckel. Den är svår att knäcka med ren beräkningskraft, en metod som hackers brukar använda, och den är snabbare och kräver mindre processorkraft än RSA-kryptering.

RSA är en algoritm för kryptering och digitala signaturer som har legat till grund för säkerheten på internet under nästan två decennier. Den fungerar fortfarande, men med tiden har man ökat den minsta nyckelstorleken för att den ska kunna ge skydd mot förbättrade kryptografiska angrepp. Med ECC får du alltså bättre prestanda, eftersom tekniken klarar sig med kortare nyckellängd och ger ändå högre säkerhet. En 256-bitars ECC-nyckel ger t.ex. samma säkerhet som en RSA-nyckel med 3 072 bitar. Vad leder detta till? Du får precis den säkerhet du behöver utan att göra avkall på prestanda.

Dessutom innebär kortare nycklar mindre certifikat, som använder mindre bandbredd. Eftersom fler av företagets kunder börjar använda mindre enheter när de handlar på nätet, ger ECC sammantaget kunderna bättre erfarenheter.

Symantecs ECC-rotcertifikat har funnits sedan 2007 i de tre främsta webbläsarna, så Symantecs ECC-certifikat fungerar i din befintliga infrastruktur – förutsatt att moderna webbläsare används – och de kostar inget extra.

Läs mer om [ECC och algoritmisk flexibilitet](#).



TIPS 6 - Always-On SSL överallt



Du bör alltid kryptera hela webbplatsen med SSL, och det gör du genom att använda Always On SSL. Detta är en kostnadseffektiv säkerhetsåtgärd som skyddar besökarna på webbplatsen från ankomst till avfärd, vilket gör det säkrare att söka, lämna information och handla på nätet.

Företag som verkligen anstränger sig för att skydda sina kunder och sitt rykte använder Always On SSL med SSL-certifikat från en välrenommerad certifikatsutfärdare som Symantec. Always On SSL är enkelt att införa. Det verifierar webbplatsens identitet och krypterar all information som går mellan webbplatsen och användaren (inklusive eventuella cookies). Den skyddar data mot obehörig läsning, påverkan eller användning.

Betecknande nog uppmanar Online Trust Alliance alla webbplatser att börja använda Always On SSL. Organisationen säger att "Always On SSL är en beprövad och praktisk säkerhetsåtgärd som bör införas på alla webbplatser där användarna lämnar eller ser känslig information".

Många av världens mest framgångsrika webbplatser har insett värdet av att införa Always On SSL, eftersom det skyddar dem mot sidnappning och intrång genom hot som Firesheep och injektion av skadlig kod.

Always On SSL kan upprätthålla det förtroende som användarna har fått för din webbplats. Det visar att du tar användarnas säkerhet och integritet på allvar – och att du gör allt du kan för att skydda dem på nätet.



TIPS 7 - "Public key pinning": en fråga om förtroende



Public key pinning (en teknik vars egentliga namn är Public key pinning extension for HTTP) är avsett att ge webbplatsinnehavare möjlighet att begränsa vilka certifikatutfärdare som får utfärda certifikat för deras servrar.

Det handlar i grunden om att en värd kopplas till ett förväntat certifikat eller en förväntad offentlig nyckel (certifikatet eller nyckeln "fästs" – blir "pinned" – till värden). Så snart en offentlig nyckel är känd såsom tillhörande en värd, eller den upptäcks för den värden, "fästs" den till den värden.

Enligt CA Security Council medför public key pinning att webbplatsinnehavaren kan meddela att webbplatsens SSL-certifikat måste ha en eller flera av följande egenskaper:

- En viss offentlig nyckel
- Vara signerad av en certifikatutfärdare med denna offentliga nyckel
- Hierarkiskt förtroende för en certifikatutfärdare med denna offentliga nyckel

Om ett certifikat för webbplatsinnehavarens domän utfärdas av en certifikatutfärdare som inte finns med på listan (och alltså inte är "fäst") visar webbläsare som stöder tekniken en varningsruta. Webbplatsinnehavaren kan även fästa flera nycklar från flera certifikatutfärdare. Webbläsarna behandlar dem alla som giltiga.

Innehavaren litar på att de valda certifikatutfärdarna inte av misstag utfärdar ett certifikat för innehavarens domän. Dessa certifikatutfärdare begränsar i många fall vilka som kan begära att ett certifikat utfärdas för innehavarens specifika domäner, vilket ger ytterligare skydd mot att certifikat utfärdas felaktigt till någon obehörig.

Tyvärr hävdar CA Security Council att den public key pinning-teknik som Google implementerade 2011 inte går att skalanpassa, eftersom den kräver att de offentliga nycklarna för varje domän måste läggas till i webbläsaren. En ny lösning för public key pinning som går att skalanpassa dokumenteras i ett RFC-förslag från IETF (Internet Engineering Task Force).

I detta förslag definieras så kallade public key pins genom ett HTTP-huvud från servern till webbläsaren. Informationen i huvudet kan t.ex. innehålla en SHA-1- och/eller en SHA-256-nyckelalgorithm, den maximala åldern för fästningen, huruvida den stöder underdomäner och hur strikt fästningen är.



TIPS 8 - Mota undan tjuvlyssnare med Perfect Forward Secrecy



Vad skulle du säga om en tjuvlyssnare som registrerar trafik – din trafik – här och nu skulle kunna dekryptera den någon gång i framtiden? Det skulle du förstås inte gilla. Men just så kan det vara för din organisation, även om ni inte är medvetna om faran.

Vi kan ta RSA som exempel. Med denna teknik skapas en offentlig och en privat nyckel för att kryptera och avkoda meddelanden. Men om återvinnbara nycklar fortsätter att användas, skulle lagrade krypterade data kunna bli åtkomliga om nycklarna avslöjas någon gång i framtiden. I många fall kan en angripare som känner till din privata nyckel och har sparat SSL-trafik använda den privata nyckeln för att dekryptera alla sessionsnycklar som har förhandlats fram under sparade SSL-hälsningar. Då går det att dekryptera alla sparade sessionsdata med hjälp av sessionsnycklarna. Det är ett scenario som gör de flesta illa till mods. Men det finns ett bättre sätt, och det kallas Perfect Forward Secrecy.

Om du använder denna lösning skapas och används temporära sessionsnycklar som inte går att återställa, och sedan slängs de bort. Och om PFS implementeras korrekt med ECC (Elliptical Curve Cryptography, se tips 5) är det säkrare än RSA-algoritmerna och har bättre prestanda.

När PFS används finns det ingen koppling mellan serverns privata nyckel och någon sessionsnyckel. Om både klienten och servern stöder PFS använder de en variant av Diffie-Hellman-protokollet (som heter så efter sina upphovsmän). Då utbyter bägge parterna slumpstal och räknar ut samma delade hemlighet. Det är en fiffig algoritm som hindrar tjuvlyssnare från att komma fram till samma hemlighet, även om all trafik avlyssnas.

Mer information finns i den här infografiken från Symantec:
[Se infografiken](#)



TIPS 9 - HTTP Strict Transport Security: ditt skyddsnät



Total säkerhet är A och O på nätet. Och ibland innebär det att man behöver anstränga sig lite mer – gå bortom standardsäkerheten – för att komma dit man vill.

Hackers kan – via trådlösa nätverk – använda man-in-the-middle-angrepp såsom SSL-skalning för att snappa upp en begäran från en webbläsare till HTTPS-webbplatser och skicka tillbaka de sidor som efterfrågas via HTTP. Detta innebär att anslutningen inte längre är krypterad och att hackern kan snappa upp informationen som offret lämnar på den föregivet säkra webbplatsen. Offret kanske inte ens upptäcker förändringen om han inte tittar noga på webbläsarens adressfält varje gång han klickar sig vidare till en ny sida på webbplatsen. Webbläsaren kan inte veta att informationen från en webbplats bör levereras säkert, så den varnar inte om att en webbplats hämtas via en okrypterad anslutning.

HTTP Strict Transport Security (HSTS) hindrar att detta händer genom att tillåta serverna att skicka ett meddelande till webbläsaren med ett krav om att alla sådana anslutningar måste vara krypterade. Webbläsarna tar hänsyn till detta meddelande, så alla webbsidor som kunden besöker är krypterade som avsett. Det skyddar dig och dina kunder från angrepp.

Du kan aktivera HSTS-skyddet genom att ange ett svarshuvud på dina webbplatser. Därefter respekterar webbläsare som stöder HSTS (t.ex. Chromium, Google Chrome, Firefox, Opera och Safari) dina anvisningar. Efter aktiveringen tillåter HSTS inte osäker kommunikation med din webbplats. Det sker genom att alla länkar i klartext konverteras till säkra länkar.

Internet Explorer stöder ännu inte HSTS, men Microsoft har meddelat att så blir fallet i Internet Explorer 12.

© 2015 Symantec Corporation. Med ensamrätt.
Symantec, Symantec-logotypen, logotypen med en bock
i en cirkel och Norton Secured-logotypen är varumärken
eller registrerade varumärken som tillhör Symantec
Corporation eller dess dotterbolag i USA och andra
länder. Övriga namn kan vara varumärken som tillhör
sina respektive innehavare.