

SSL-certifikat

Från Wikipedia

Ett SSL-certifikat är en typ av elektronisk legitimation. På samma sätt som personer kan legitimera sig med ID-kort eller pass, så kan exempelvis en webbplats legitimera sig med ett SSL-certifikat. Genom en webbläsare kan en sorts legitimationskontroll av certifikatet göras för att se vem som innehar det. SSL-certifikat används för att kunna säkra en server, till exempel en webbserver eller en mailserver. För att kunna ta emot kortbetalningar på en webbplats är det obligatoriskt att inneha ett SSL-certifikat. SSL-certifikat bygger på tekniken och standarden SSL som utvecklades av Netscape 1994.

Utfärdare

Precis som ett pass så har ett SSL-certifikat en utfärdare. För SSL-certifikat kallas utfärdaren på engelska Certificate Authority (CA). För att staten ska utfärda ett pass behövs giltig dokumentation. På samma sätt kräver en utfärdare giltig dokumentation av den som ansöker om ett SSL-certifikat innan certifikatet utfärdas. Utfärdaren intygar och står således som garant för att SSL-certifikatet är korrekt.

Typer av certifikat

Det går att skapa ett certifikat själv, då ett självsignerat certifikat. Om ett självsignerat certifikat används på en webbserver får besökaren upp en varning vid besök till webbplatsen. För att slippa denna dialogruta behövs ett certifikat utfärdat av en Certificate Authority. Det finns tre huvudtyper av utfärdade certifikat: domänvaliderade (förkortas DV), organisationsvaliderade (OV) och certifikat med utökad validering (EV = Extended Validation).

Domänvalidering (DV) innebär att endast en kontroll görs av att den som söker certifikatet har kontroll över domännamnet. Detta innebär rent praktiskt att ett meddelande skickas till den e-post-adress som är registrerad för domännamnet i fråga. Ingen kontroll görs över vilket företag som innehar domännamnet.

Organisationsvalidering (OV) är den vanligaste typen av SSL-certifikat, och innebär att kontroll dessutom görs av att uppgifterna för organisationen eller företaget som beställer SSL-certifikatet är korrekta.

EV-certifikat (EV) är en typ av SSL-certifikat med en hög nivå av kontroll vid utfärdandet. Många internetbanker innehar denna certifikattyp. Med ett EV-certifikat syns företagets namn i grönt i webbläsarens adressrad, vilket gör att besökaren lätt kan verifiera att han/hon besöker den korrekta webbplatsen.

Hämtad från "<http://sv.wikipedia.org/w/index.php?title=SSL-certifikat&oldid=15447079>"

Kategori: Datasäkerhet

-
- Sidan ändrades senast den 10 december 2011 kl. 09.28.
 - Wikipedias text är tillgänglig under licensen Creative Commons Attribution-Share Alike 3.0 Unported. För bilder, se respektive bildsida (klicka på bilden). Se vidare Wikipedia:Upphovsrätt och användarvillkor.