



Riktlinjer för Licenciering av SSL-Certifikat i Miljöer med flera Servrar

Detta dokument innehåller grundläggande riktlinjer för den information som ges i VeriSign® SSL:s prenumerantavtal och kan hjälpa företag att förstå vad som krävs för att uppfylla licenskraven. I prenumerantavtalet definieras VeriSigns policy för licensiering av SSL-certifikat. I detta dokument beskrivs ”licensierat certifikatalternativ”, vilket är det servicealternativ som ger en prenumerant rätt att använda ett certifikat på en fysisk enhet och få ytterligare certifikatlicenser för varje fysisk server som varje enhet styr eller där dublettcertifikat i övrigt kan finnas.

Därför krävs en certifikatlicens för varje tjänstegränssnitt som utgör den logiska tjänstekomponenten till en SSL-anslutning, oavsett om SSL-tunneln avslutas vid tjänstegränssnittet. Exempel på detta är en enskild webbserverinstans där SSL-sessionen avslutas vid webbservern eller flera webbserverar bakom en lastbalansering.

Nedan beskriver vi några vanliga situationer och motsvarande licenskrav.

+ Webbplats för Standby och Katastrofåterställning

Licens krävs för varje server i varmt (eller hett) standbyläge. Servrar med kall standby kräver inte ytterligare licenser.

+ Servrar med Omvänd Proxy och Cachning

Du behöver inte köpa ytterligare licenser för proxyservrar, oavsett om de cashar data. Licenser krävs endast för de servrar som ligger bakom den omvända proxyservern.

+ SSL-Acceleratorer och Offloaders

För nätverksbaserade acceleratorer och offloaders krävs en licens för varje server som använder ett SSL-certifikat som hanteras av en SSL-accelerator eller en offloader, oavsett om SSL-sessionen avslutas vid eller före webbservern. Du behöver dock inte någon licens för själva acceleratoren. Om det till exempel finns en eller två Luna SA-enheter (övertaliga) som har ett certifikat som används av nio webbserverar, måste nio licenser köpas in. Denna allmänna regel (en licens för varje server som har ett certifikat som hanteras av en SSL-accelerator) gäller även PCI-kortbaserade acceleratorer.



**+ Lastbalanserare**

Om det finns servrar bakom en lastbalanserare måste en licens köpas in för varje server som ligger bakom (och som pekas ut av) lastbalanseraren. Se avsnittet ”SSL-acceleratorer” ovan för information om lastbalanserare som även fungerar som SSL-acceleratorer. För dessa kombinationer av accelerator/lastbalanserare behövs ingen extra licens på den fysiska acceleratoren om SSL-sessionen avslutas vid servrarna bakom acceleratoren och om en licens redan har skaffats för dessa servrar.

+ Flera Virtuella Servrar på en Fysisk Server

Om du har flera virtuella servrar som servrar flera domäner på en fysisk maskin behövs flera licenser. I överensstämmelse med vad som står i VeriSign SSL:s prenumerantavtal version 4.0, är varje virtuell server som ligger på en och samma fysiska maskin föremål för samma regler som om de vore separata fysiska maskiner. För en fysisk server som till exempel är värd för två virtuella servrar (en som servrar abc.com och en annan som servrar xyz.com) behövs två licenser, inte en.

+ Flerlagrade Applikationsmodeller med SSL mellan Lagren

Om du har ytterligare lager med applikationsservrar bakom det första serverlagret som använder SSL mellan lagren behövs flera licenser. Om nedladdningslagren fungerar som en tjänst och använder SSL, är de servrar som möjliggör nedladdningslagret föremål för samma regler som förstalagersservrar och en licens för varje tjänstegränssnitt krävs. Detta gäller även om nedladdningstjänstlagren är del av samma atomiska transaktion på användarnivå som drivs av det översta lagret.

+ Webbtjänster

Om du har webbtjänstsgateways WS – Web Service som använder SSL, krävs en licens för varje logiskt webbtjänstgränssnitt om gränssnittet är en webbtjänstsserver (jämfört med en klientserver). Se avsnittet ”Certifikatanvändning: klientautentisering jämfört med serverautentisering” för mer information om klient- och serverbeteende för XML-gateways.

+ Stordatormiljöer

För stordatorbaserade tjänster som använder SSL krävs en licens för varje certifikat i en servernyckelring av typen RACF, TopSecret eller ACF2.

+ Certifikatanvändning: Klientautentisering Jämfört med Serverautentisering

När certifikat används för klientautentisering gäller följande riktlinjer: Om en fysisk maskin (till exempel en e-postserver eller en webbtjänstsgateway) har ett SSL-certifikat som den ibland använder för serverAuth (när andra e-postservrar kontaktar den eller som en webbtjänst) och ibland för clientAuth (när den kontaktar andra e-postservrar eller som webbtjänstsklient), behövs bara en licens.

Om certifikatet endast används för clientAuth krävs en licens för varje fysisk maskin som använder det aktuella certifikatet.

+ Om VeriSign

VeriSign (NASDAQ: VRSN) är en pålitlig leverantör av Internetinfrastrukturstjänster för den nätverksbaserade världen. Vår SSL-autentisering, vårt identitetsskydd och våra registertjänster hjälper företag och kunder i hela världen, miljarder gånger dagligen, att kommunicera och sköta sin handel med förtroende.



VeriSign är ledande inom SSL-certifikat och erbjuder säker e-handel och kommunikation för webbplatser, intranät och extranät.

VeriSign fortsätter att vara ledande inom SSL-certifikatsbranschen som medlem i CA/Browser Forum, en frivilligorganisation som har definierat riktlinjerna och metoderna för implementation av EV SSL-certifikat.

Besök www.Verisign.se för mer information.