



Vejledning for SSL-Certifikatlicenser i Multiservermiljøer

Dette dokument er en generel vejledning til, hvad der omfattes af VeriSign® SSL-abonnentaftalen, og den skal hjælpe virksomhederne med at forstå kravene til licensoverholdelse. Abonnentaftalen definerer VeriSigns politik for licenstildeling til SSL-certifikater. I dette dokument beskrives "Licenstildelt certifikat" som den mulighed, der giver en abonnent ret til at bruge et certifikat på en fysisk enhed og til at indhente yderligere certifikatlicenser til hver fysisk server, som hver enhed administrerer, eller hvor kopierede certifikater kan befinde sig.

Derfor kræves der en certifikatlicens for hver tjenestegrænseflade, som er den logiske servicekomponent for en SSL-forbindelse, uanset om SSL-tunnellen afsluttes ved tjenestegrænsefladen. Eksemplerne tager udgangspunkt i en enkelt forekomst af en webserver, hvor SSL-sessionen afsluttes ved webserveren eller ved flere webservere bag en opgavefordeler.

Nedenfor beskrives nogle almindelige situationer med tilsvarende licenskrav.

+ Websteder for Standby og Gendannelse efter Nedbrud

Der kræves en licens for hver server i en "warm" (eller "hot") standby-tilstand. Der kræves ikke ekstra licenser for "cold" standby-servere.

+ Reverse-Proxy-Servere og Cachelagring

Der skal ikke købes ekstra licenser til proxy-servere, uanset om de cachelagrer indhold. Der kræves kun licenser til servere, som er placeret bag reverse-proxy-serveren.

+ SSL-Acceleratorer og Offloadere

Til netværksbaserede acceleratorer og offloadere kræves der en licens for hver server, som er afhængig af et SSL-certifikat, der styres af en SSL-accelerator eller offloader, uanset om SSL-sessionen afsluttes ved eller før webserveren. Der behøves imidlertid ikke en licens til selve acceleratoren. Hvis der f.eks. bruges en eller to Luna SA'er (redundant), som indeholder et certifikat, der benyttes af ni webservere, skal der købes ni licenser. Denne generelle vejledning (en licens for hver server, som afhænger af et certifikat, der styres af en SSL-accelerator) gælder også for PCI-kortbaserede acceleratorer.



**+ Opgavefordelere**

Hvis serverne er placeret bag en opgavefordeler, skal der købes en licens for hver server bag (og som henvises til af) opgavefordeleren. Se ovenstående afsnit "SSL-acceleratorer" for at få oplysninger om opgavefordelere, der også fungerer som en SSL-accelerator. Til disse acceleratorer-/opgavefordelerkombinationer kræves der ikke en ekstra licens på den fysiske accelerator, hvis SSL-sessionen afsluttes ved serveren bag acceleratoren, og hvis der allerede er blevet indhentet en licens til de servere.

+ Flere Virtuelle Servere på en Fysisk Server

Hvis der er flere virtuelle servere, som benyttes af flere domæner på en enkelt fysisk maskine, kræves der flere licenser. Som det står beskrevet i VeriSign SSL-abbonnentaftale version 4.0, er hver enkelt virtuelle server på den samme fysiske maskine underlagt samme regler, som hvis der var tale om særskilte fysiske maskiner. En fysisk server, der er vært for to virtuelle servere (en, der er vært for abc.com og en, der er vært for xyz.com), skal f.eks. bruge to licenser og ikke bare en.

+ Multigraduerede Programmodeller med SSL mellem Niveauerne

Hvis der er flere niveauer af applikationsservere bag det første serverniveau, som benytter SSL mellem niveauerne, kræves der ekstra licenser. Hvis downstreamniveauerne fungerer som en tjeneste og benytter SSL, er de servere, der muliggør downstreamniveauet, underlagt samme regler som serverne på første niveau, og der kræves derfor en licens for hver tjenestegrænseflade. Dette gælder, selv hvis downstreamtjenesteniveauerne er en del af den samme atomiske, brugerniveau-transaktion, som styres fra topniveauet.

+ Webtjenester

Hvis der benyttes webtjeneste-gateways, som bruger SSL, kræves der en licens for hver logisk webtjenestegrænseflade, hvis grænsefladen er en WS-server (WS, Web Service) (i modsætning til en klient-server). Se afsnittet "Certifikatbrug: klientautenticering vs. serverautenticering" for at få flere oplysninger om klient-serveradfærd for XML-gateways.

+ Mainframe-Miljøer

Der kræves en licens for hvert certifikat i RACF-, TopSecret- eller ACF2-servernøgleringen i en mainframe-baseret tjeneste, som anvender SSL.

+ Certifikatbrug: Klientautenticering vs. Serverautenticering

I situationer, hvor der anvendes et certifikat til klientautenticering, gælder følgende vejledning: Hvis en fysisk maskine (f.eks. en mail-server eller en webtjeneste-gateway) har et SSL-certifikat, som den nogle gange benytter til serverautenticering (når andre mail-servere kontakter den eller som en WS-tjeneste) og nogle gange til klientautenticering (når den kontakter andre mail-servere eller som en WS-klient), kræves der kun én licens.

Hvis certifikatet kun anvendes som klientautenticering, kræves der en licens for hver fysisk maskine, som benytter det certifikat.

**+ Om VeriSign**

VeriSign (NASDAQ: VRSN) er den sikre udbyder af internetinfrastruktur-tjenester til den netværksforbundne verden. Vores SSL-, autentificerings-, identitetsbeskyttelses- og registreringstjenester hjælper utallige gange dagligt virksomheder og forbrugere over hele verden med at gennemføre sikker kommunikation og handel på internettet.

VeriSign er det førende SSL-certificeringscenter (Secure Sockets Layer), der gør e-handel og kommunikation sikker for websteder, intranet og ekstranet.

VeriSign er fortsat førende i SSL-certifikatbranchen og er medlem af CA/Browser Forum, en frivillig organisation, som har udarbejdet et sæt retningslinjer og metoder til implementering af EV SSL-certifikater.

Gå til www.Verisign.dk for at få flere oplysninger.