



Richtlinien zur Lizenzierung von SSL-Zertifikaten in Umgebungen mit mehreren Servern

Dieses Dokument fasst grob den Inhalt des VeriSign® SSL-Abonnentenvertrags zusammen und gibt Unternehmen dadurch einen Eindruck, was zur Einhaltung der Lizenzvereinbarung nötig ist. Der Abonnentenvertrag definiert VeriSigns Richtlinien für die Lizenzierung von SSL-Zertifikaten. Dieses Dokument beschreibt die „Licensed Certificate Option“ als Serviceoption, durch die einem Abonnenten das Recht zugesichert wird, ein Zertifikat auf einem physischen Gerät zu verwenden und zusätzliche Zertifikatslizenzen für jeden physischen Server, den jedes Gerät verwaltet, oder für sonstige Geräte mit replizierten Zertifikaten zu erhalten.

Daher ist für jede Serviceschnittstelle, die die logische Servicekomponente einer SSL-Verbindung darstellt, eine Zertifikatslizenz erforderlich, unabhängig davon, ob der SSL-Tunnel an der Serviceschnittstelle endet. Beispiele hierfür sind eine einzelne Instanz eines Webservers, bei dem die SSL-Sitzung am Webserver endet, oder mehrere Webserver hinter einem Load Balancer.

Im Folgenden werden einige übliche Situationen und die entsprechenden Lizenzvorschriften beschrieben.

+ Standby- und Disaster Recovery-Sites

Für jeden Server im Warm- (oder Hot-) Standby-Modus sind Lizenzen erforderlich. Für Cold-Standby-Server sind keine zusätzlichen Lizenzen erforderlich.

+ Reverse-Proxyserver und Caching

Für Proxyserver müssen keine zusätzlichen Lizenzen erworben werden, unabhängig davon, ob Inhalte im Cache gespeichert werden oder nicht. Lizenzen sind nur für diejenigen Server erforderlich, die sich hinter dem Reverse-Proxy befinden.

+ SSL-Beschleuniger und Offloaders

Für netzwerkgestützte Beschleuniger und Offloader ist eine Lizenz für jeden Server erforderlich, der sich auf ein von einem SSL-Beschleuniger oder Offloader verwaltetes SSL-Zertifikat stützt, unabhängig davon, ob die SSL-Sitzung am oder vor dem Webserver endet. Für den Beschleuniger selbst ist jedoch keine Lizenz erforderlich. Wenn beispielsweise ein oder zwei Luna SAs (redundant) vorhanden sind, die über ein von neun Webservern



verwendetes Zertifikat verfügen, müssten neun Lizenzen gekauft werden. Diese allgemeine Richtlinie (eine Lizenz für jeden Server, der sich auf ein von einem SSL-Beschleuniger verwaltetes Zertifikat stützt), gilt auch für PCI-Karten-gestützte Beschleuniger.

+ Load Balancers

Falls sich hinter einem Load Balancer Server befinden, muss für jeden Server hinter dem Load Balancer (und auf den der Load Balancer verweist) eine Lizenz gekauft werden. Für Load Balancer, die außerdem als SSL-Beschleuniger fungieren, lesen Sie bitte obigen Abschnitt zu „SSL-Beschleunigern“. Für diese Kombinationen aus Beschleuniger und Load Balancer benötigen Sie keine zusätzliche Lizenz für den Beschleuniger, falls die SSL-Sitzung an den Servern hinter dem Beschleuniger endet und für diese Server bereits eine Lizenz bezogen wurde.

+ Mehrere virtuelle Server auf einem physischen Server

Wenn Sie auf einem physischen Server mehrere virtuelle Server für mehrere Domains betreiben, benötigen Sie mehrere Lizenzen. Wie im VeriSign Abonnentenvertrag für SSL-Zertifikate (Version 4.0) erwähnt gelten für jeden virtuellen Server auf demselben physischen Server dieselben Regeln, wie wenn es sich um verschiedene physische Server handeln würde. Beispiel: Für einen physischen Server, auf dem zwei virtuelle Server gehostet werden (einer für abc.de und ein weiterer für xyz.de), sind zwei Lizenzen erforderlich, nicht nur eine.

+ Mehrschichtige Anwendungsmodelle mit SSL zwischen den Schichten

Bei zusätzlichen Anwendungsserverschichten hinter der ursprünglichen Serverschicht, die SSL zwischen den einzelnen Schichten verwenden, benötigen Sie zusätzliche Lizenzen. Wenn die Downstream-Schichten als Service fungieren und SSL nutzen, unterliegen die Server, die die Downstream-Schicht ermöglichen, denselben Regeln wie die Server der ersten Schicht und benötigen eine Lizenz für jede Serviceschnittstelle. Das gilt auch dann, wenn Downstream-Serviceschichten Teil derselben Benutzertransaktion auf der obersten Schicht sind.

+ Webdienste

Falls Sie Gateways für Webdienste nutzen, die SSL verwenden, ist für jede logische Webdienst-Schnittstelle eine Lizenz erforderlich, falls es sich bei der Schnittstelle um einen Webdienst-Server (keinen Client) handelt. Lesen Sie bitte den Abschnitt „Zertifikatsnutzung: Client-Authentifizierung im Vergleich zu Server-Authentifizierung“ für weitere Richtlinien zum Client-Verhalten im Vergleich zum Server-Verhalten für XML-Gateways.

+ Mainframe-Umgebungen

Für mainframe-gestützte Services, die SSL verwenden, ist für jedes Zertifikat im RACF-, TopSecret- oder ACF2-Server-Keyring eine Lizenz erforderlich.

+ Zertifikatsnutzung: Client-Authentifizierung im Vergleich zu Server-Authentifizierung

Wenn ein Zertifikat zur Client-Authentifizierung genutzt wird, gelten folgende Richtlinien: Falls ein physischer Rechner (etwa ein E-Mail-Server oder ein Webdienst-Gateway) über ein SSL-Zertifikat verfügt und dieses einmal zur Server-Authentifizierung (beim Kontakt durch andere E-Mail-Server oder als Webdienst) und ein anderes Mal zur Client-Authentifizierung (beim Kontakt zu anderen E-Mail-Servern oder als Webdienst-Client) verwendet, ist nur eine Lizenz erforderlich.

Falls das Zertifikat nur zur Client-Authentifizierung verwendet wird, ist für jeden physischen Rechner, der dieses Zertifikat nutzt, eine Lizenz erforderlich.

**+ Über VeriSign**

VeriSign (NASDAQ: VRSN) ist der führende Anbieter digitaler Infrastrukturdienste für die vernetzte Welt. Täglich ermöglichen unsere SSL-, Authentifizierungs-, Identitätsschutz- und Registrierungsdienste Unternehmen und Verbrauchern weltweit milliardenfach vertrauensvolle Kommunikation und sichere Transaktionen.

VeriSign ist die führende Secure Sockets Layer- (SSL) Zertifizierungsstelle für sicheren E-Commerce und sichere Kommunikation für Websites, Intranets und Extranets.

VeriSign ist in der Branche für SSL-Zertifikate weiterhin führend als Mitglied des CA/Browser Forum tätig, einer ehrenamtlichen Organisation, die Richtlinien und Methoden zur Implementierung von EV SSL-Zertifikaten festgelegt hat.

Weitere Informationen finden Sie unter www.Verisign.de.