



Directives Concernant La Concession de Licences de Certificats SSL Pour Les Environnements Multiserveurs

Ce document reprend les grandes lignes du Contrat d'abonnement SSL VeriSign® et a pour but d'aider les entreprises à comprendre ce qui est exigé pour rester dans le cadre de la licence. Le contrat d'abonnement définit la politique de concession de licences de certificats SSL appliquée par VeriSign. Il décrit l'« Option Certificat sous licence » comme une option de service accordant à un Abonné le droit d'utiliser un certificat sur un dispositif physique et d'obtenir des licences de certificat supplémentaires pour chaque serveur physique géré par chaque dispositif, où sur lequel existent des certificats répliqués.

Par conséquent, une licence de certificat est requise pour chaque interface de service qui est aussi le composant de service logique d'une connexion SSL, que le tunnel SSL se termine ou non au niveau de l'interface de service. À titre d'exemple, on peut citer l'instance unique d'un serveur Web, dans le cas de laquelle la session SSL se termine au niveau du serveur Web, ou encore plusieurs serveurs Web derrière un équilibreur de charge.

Ci-dessous, vous trouverez des cas de figure courants et les exigences de licences correspondantes.

+ Centres Informatiques de Secours

Une licence est requise pour chaque serveur en mode de secours partiel (ou total). Les serveurs de secours minimum ne requièrent pas de licences supplémentaires.

+ Relais Inverses et Mise en Cache

Vous n'avez pas besoin d'acheter de licences supplémentaires pour les serveurs proxy, qu'ils servent ou non de caches. Des licences sont requises uniquement pour les serveurs qui se trouvent derrière les relais inverses.

+ Périphériques d'Accélération et de Déchargement SSL

Pour ce qui est des périphériques d'accélération et de déchargement intégrés à un réseau, une licence est requise pour chaque serveur associé à un certificat SSL géré par un périphérique d'accélération ou de déchargement SSL, que la session SSL se termine ou non au niveau du serveur Web ou avant celui-ci. Cependant, vous n'avez pas besoin de licence pour le périphérique d'accélération lui-même. Par exemple, avec un ou deux Luna SA (redondants) associés à un certificat utilisé par neuf serveurs Web, il faudrait





acheter neuf licences. Cette recommandation générale (une licence pour chaque serveur associé à un certificat géré par un périphérique d'accélération SSL) vaut également pour les périphériques d'accélération basés sur carte PCI.

+ Équilibreur de Charge

Avec les serveurs derrière un équilibreur de charge, vous devez acheter une licence pour chaque serveur qui se trouve derrière l'équilibreur (et vers lequel l'équilibreur dirige les utilisateurs). Pour les équilibreurs de charge utilisés également comme accélérateurs SSL, veuillez vous référer à la section « Périphériques d'accélération SSL » ci-dessus. Pour ces combinaisons accélérateur/équilibreur de charge, aucune licence supplémentaire n'est requise au niveau de l'accélérateur physique si la session SSL se termine au niveau des serveurs qui se trouvent derrière l'accélérateur et si une licence a déjà été achetée pour ces serveurs.

+ Serveurs Virtuels Multiples Sur Un Seul Serveur Physique

Si vous avez plusieurs serveurs virtuels pour de multiples domaines sur une seule machine physique, vous devez acheter plusieurs licences. Comme spécifié dans le Contrat d'abonnement SSL VeriSign version 4.0, chaque serveur virtuel résidant sur une même machine physique est régi de la même manière que s'il s'agissait d'une machine physique à part entière. Par exemple, un serveur physique qui héberge deux serveurs virtuels (un pour abc.com et l'autre pour xyz.com) requiert deux licences, pas seulement une.

+ Modèles Applicatifs Multi-niveaux Avec Sécurité SSL Entre Niveaux

Si vous disposez de niveaux supplémentaires de serveurs applicatifs derrière le serveur initial et si ces serveurs utilisent la sécurité SSL entre les niveaux, vous devez acheter des licences supplémentaires. Si les couches en réception font office de service et utilisent la sécurité SSL, les serveurs dont dépend la couche en réception sont régis de la même manière que les serveurs de la première couche et requièrent l'achat d'une licence pour chaque interface de service. Cette règle s'applique même si les couches de service en réception font partie de la même transaction atomique utilisateur transmise à partir de la couche supérieure.

+ Services Web

Avec les passerelles de services Web (WS) qui utilisent la sécurité SSL, une licence est requise pour chaque interface logique de service Web s'il s'agit d'un serveur WS (par opposition à un serveur client). Veuillez vous référer à la section « Utilisation des certificats : authentification client ou authentification serveur » pour de plus amples informations sur le comportement client ou serveur pour les passerelles XML.

+ Ordinateurs Centraux

Avec les services basés sur des ordinateurs centraux et utilisant la sécurité SSL, une licence est requise pour chaque certificat de l'ensemble de clés du serveur RACF, TopSecret ou ACF2.

+ Utilisation des Certificats : Authentification Client ou Authentification Serveur

Les directives suivantes s'appliquent lorsqu'un certificat est utilisé pour l'authentification client. Si une machine physique (par exemple un serveur de messagerie électronique ou une passerelle de services Web) est associée à un certificat SSL qu'elle utilise tantôt pour l'authentification serveur (lorsque d'autres serveurs de messagerie électronique la contactent ou comme service WS), tantôt pour l'authentification client (lorsqu'elle contacte d'autres serveurs de messagerie électronique ou comme serveur WS), alors une seule licence est requise.



Si le certificat sert uniquement à l'authentification client, alors une licence est requise pour chaque machine physique qui se sert de ce certificat.

+ À Propos de VeriSign

VeriSign (NASDAQ : VRSN) est le fournisseur réputé de services d'infrastructure sur Internet pour le monde en réseau. Des milliards de fois par jour, les entreprises ainsi que les particuliers du monde entier utilisent les services SSL, d'authentification, de protection de l'identité et d'enregistrement pour communiquer et effectuer des transactions en toute confiance.

VeriSign est la première autorité de certification SSL (Secure Sockets Layer) sécurisant le commerce électronique et les communications sur les sites Web, les intranets et les extranets.

VeriSign reste le leader de l'industrie des certificats SSL en tant que membre du CA/Browser Forum, organisation à but non lucratif qui a défini des directives et moyens de mise en œuvre des certificats SSL EV.

Pour plus d'informations, visitez le site www.Verisign.fr.