



Directrices sobre Licencias de Certificados SSL en Entornos con Múltiples Servidores

Este documento constituye una extensa directriz de los elementos tratados en el contrato de suscripción de certificado SSL de VeriSign® y puede ayudar a las empresas a comprender los requisitos necesarios para conservar la conformidad con la licencia. El contrato de suscripción define la política de licencia de certificados SSL de VeriSign. El documento describe la “Opción de certificado con licencia” como la opción de servicio por la que se concede al suscriptor el derecho a utilizar un certificado en un dispositivo físico y obtener licencias de certificado adicionales para cada uno de los servidores físicos que los distintos dispositivos gestionan o donde las réplicas de los certificados residan.

Por ello, se requiere una licencia de certificado para cada interfaz de servicio que sea el componente de servicio lógico de una conexión SSL, independientemente de si el túnel SSL termina en la interfaz de servicio. Entre los ejemplos se incluye una única instancia de un servidor Web en la que la sesión SSL termina en el servidor Web, o de múltiples servidores Web tras un distribuidor de carga.

A continuación se describen situaciones comunes y los requisitos de licencia correspondientes.

+ Sitios de Recuperación de Desastres y Espera

Se requieren licencias para cada servidor en modo de espera de seguridad media (o alta). Los servidores de espera de seguridad baja no requieren licencias adicionales.

+ Servidores Proxy Inversos y de Caché

No tendrá que adquirir licencias adicionales para los servidores proxy, independientemente de si almacenan contenido en caché. Las licencias sólo son obligatorias para los servidores ubicados tras el proxy inverso.

+ Aceleradores SSL y Dispositivos de Offload

En el caso de los aceleradores y dispositivos de Offload basados en red, se necesita una licencia para cualquier servidor que se base en un certificado SSL gestionado por un acelerador SSL o dispositivo de Offload, independientemente de si la sesión SSL termina antes del servidor Web o en él. Sin embargo, no necesitará una licencia para el propio acelerador. Por ejemplo, si hay uno o dos servidores Luna SA (redundantes) que ostentan





un certificado utilizado por nueve servidores Web, deberá adquirir nueve licencias. Esta pauta general (una licencia para cada servidor basado en un certificado gestionado por un acelerador SSL) se aplica también a los aceleradores basados en tarjetas PCI.

+ Distribuidores de Carga

Si hay servidores tras un distribuidor de carga, deberá adquirir una licencia para cada servidor que se encuentre tras el distribuidor (y a los que señale el distribuidor). En el caso de los distribuidores de carga que también actúen como aceleradores SSL, consulte la sección “Aceleradores SSL” anterior. En estas combinaciones acelerador/distribuidor de carga, no necesitará una licencia adicional para el acelerador físico si la sesión SSL termina en los servidores que se encuentran tras el acelerador y si ya ha adquirido una licencia para esos servidores.

+ Múltiples Servidores Virtuales en un Servidor Físico

Si cuenta con múltiples servidores virtuales atendiendo múltiples dominios en un mismo equipo físico, necesitará múltiples licencias. Tal y como se declara en el contrato de suscripción de certificado SSL de VeriSign versión 4.0, los servidores virtuales que residan en el mismo equipo físico están sujetos a las mismas reglas que si se encontraran en equipos físicos independientes. Por ejemplo, un servidor físico que aloje dos servidores virtuales (uno que atienda a abc.com y otro que atienda a xyz.com) está sujeto a dos licencias, no sólo a una.

+ Modelos de Aplicaciones Multinivel con SSL entre Niveles

Si tiene niveles adicionales de servidores de aplicaciones tras el nivel del servidor inicial que emplean SSL entre niveles, necesitará licencias adicionales. Si los niveles posteriores actúan como un servicio y emplean SSL, los servidores que activen el nivel posterior estarán sujetos a las mismas reglas que los servidores del primer nivel, y necesitarán una licencia para cada interfaz de servicio. Esto es así aunque los niveles de servicio posteriores formen parte de la misma unidad a nivel de usuario dirigida desde el nivel superior.

+ Servicios Web

Si tiene puertas de enlace de servicio Web (WS) que utilicen SSL, se necesitará una licencia para cada interfaz de servicio Web lógica si la interfaz es un servidor WS (frente a un cliente). Consulte la sección “Uso de certificados: comparación entre la autenticación de clientes y la de servidores” si desea más información sobre la diferencia de comportamiento entre clientes y servidores de las puertas de enlace XML.

+ Entornos de Estructuras Principales

En el caso de los servicios basados en estructuras principales (mainframe) que utilicen SSL, se necesitará una licencia para cada certificado del patrón de claves del servidor RACF, TopSecret o ACF2.

+ Uso de Certificados: Comparación entre la Autenticación de Clientes y la de Servidores

En los casos en los que se utilice un certificado para la autenticación de clientes, las directrices son las siguientes: Si un equipo físico (como un servidor de correo o una puerta de enlace de servicio Web) tiene un certificado SSL que utiliza a veces para autenticación de servidor (cuando otros servidores de correo se ponen en contacto con él o como servicio WS) y otras para autenticación de cliente (cuando se pone en contacto con otros servidores de correo o como cliente WS), sólo es necesaria una licencia.

Si el certificado sólo se utiliza para la autenticación de cliente, será necesaria una licencia para cada equipo físico que utilice ese certificado.



+ Acerca de VeriSign

VeriSign (NASDAQ: VRSN) es el proveedor de confianza de servicios de infraestructura de Internet para el mundo en red. Millones de veces al día, nuestros servicios SSL, de autenticación, de protección de identidad y de registro, ayudan a las empresas y a los consumidores de todo el mundo a comunicarse y comercializar con confianza.

VeriSign es la empresa emisora de certificados SSL (Secure Sockets Layer) líder del mercado que permite las comunicaciones y el comercio electrónico seguro para sitios Web, intranets y extranets.

VeriSign sigue liderando el sector de los certificados SSL como miembro del CA/Browser Forum, una organización sin ánimo de lucro, que ha definido las directrices y los objetivos de la implementación de los certificados SSL con EV.

Si desea más información, visite www.Verisign.es.