



DATA SHEET



## Guidelines for SSL Certificate Licensing in Multi-Server Environments

This document is a broad guideline of the VeriSign® SSL Subscriber Agreement and can help businesses understand the requirements for remaining license compliant. The subscriber agreement defines VeriSign's policy for the licensing of SSL Certificates. The document describes the "Licensed Certificate Option" as the service option that grants a Subscriber the right to use a certificate on one physical device, and obtain additional certificate licenses for each physical server managed by a device, or where replicated certificates may otherwise reside.

Therefore, a certificate license is required for every service interface that is the logical service component of an SSL connection, regardless of whether the SSL tunnel terminates at the service interface. Examples include a single instance of a Web server where the SSL session terminates at the Web server, or multiple Web servers behind a load balancer.

Below we describe some common situations and their corresponding licensing requirements.

### + Standby and Disaster Recovery Sites

Licenses are required for each server in a warm (or hot) standby mode. Cold standby servers do not require additional licenses.

### + Reverse Proxy Servers and Caching

You will not be required to buy additional licenses for proxy servers, regardless of whether they cache content. Licenses are only required for the servers that are behind the reverse proxy.

### + SSL Accelerators and Offloaders

For network-based accelerators and offloaders, one license is needed for any server that relies on an SSL Certificate managed by an SSL accelerator or offloader, regardless of whether the SSL session terminates at or before the Web server. However, you do not need a license for the accelerator itself. For instance, if there are one or two Luna SAs (redundant) that hold a certificate used by nine Web servers, then nine licenses would have to be purchased. This general guidance (one license for each server that relies on a certificate managed by an SSL accelerator) also applies to PCI-card-based accelerators.



**+ Load Balancers**

If there are servers behind a load balancer, a license must be purchased for each server behind (and pointed to by) the load balancer. For load balancers that also act as an SSL accelerator, please refer to the above section “SSL Accelerators”. For these accelerator/load balancer combinations, you will not need an additional license on the physical accelerator if the SSL session terminates at the servers behind the accelerator and if a license has already been obtained for those servers.

**+ Multiple Virtual Servers on One Physical Server**

If you have multiple virtual servers serving multiple domains on one physical machine, you will require multiple licenses. As stated in the VeriSign SSL Subscriber Agreement version 4.0, each virtual server that resides on the same physical machine is subject to the same rules as if it were a separate physical machine. As an example, a physical server hosting two virtual servers (one that services abc.com and another that services xyz.com) is subject to two licenses, not just one.

**+ Multi-tiered Application Models with SSL between Tiers**

If you have additional tiers of application servers behind the initial server tier that employ SSL between tiers, you will need additional licenses. If the downstream tiers act as a service and employ SSL, the servers that enable the downstream tier are subject to the same rules as first-tier servers and require a license for each service interface. This is true even if downstream service tiers are part of the same atomic, user-level transaction driven from the top tier.

**+ Web Services**

If you have Web Service (WS) gateways that use SSL, a license will be required for each logical Web Service interface if the interface is a WS server (versus client). Please refer to the section “Certificate Usage: Client Authentication versus Server Authentication” for more guidance on client versus server behaviour for XML gateways.

**+ Mainframe Environments**

For mainframe-based services that employ SSL, a license will be required for every certificate in the RACF, Top Secret or ACF2 server key ring.

**+ Certificate Usage: Client Authentication versus Server Authentication**

For instances where a certificate is used for client authentication, the guidelines are as follows: if a physical machine (such as a mail server or Web Service gateway) has an SSL Certificate that it sometimes uses for serverAuth (when other mail servers contact it or as a WS service) and sometimes for clientAuth (when it contacts other mail servers or as a WS client), then only one license is needed.

If the certificate is used only for clientAuth, then one license is needed for each physical machine that makes use of that certificate.

**+ About VeriSign**

VeriSign (NASDAQ: VRSN) is the trusted provider of internet infrastructure services for the networked world. Billions of times daily, our SSL, authentication, identity protection and registry services help companies and consumers all over the world to communicate and conduct commerce with confidence.



## DATA SHEET

VeriSign is the leading Secure Sockets Layer (SSL) Certificate Authority enabling secure e-commerce and communications for Web sites, intranets and extranets.

VeriSign continues to lead the SSL Certificate industry as a member of the CA/Browser Forum, a voluntary organisation that has defined guidelines and means of implementing EV SSL Certificates.

**For more information, visit [www.Verisign.ch](http://www.Verisign.ch).**