



## Linee Guida per la Concessione in Licenza di Certificati SSL in Ambienti con Più Server

In questo documento viene fornita una descrizione generale dei termini inclusi nel Contratto di registrazione dei certificati SSL di VeriSign® allo scopo di aiutare le aziende a comprendere i requisiti necessari per mantenere la piena conformità con la licenza. Il contratto di registrazione definisce le regole di VeriSign relative alla concessione in licenza dei certificati SSL. Nel documento, per “opzione certificato con licenza” si intende un’opzione di servizio che concede al sottoscrittore il diritto di utilizzare un certificato su un dispositivo fisico e di acquistare ulteriori licenze per il certificato per ciascun server fisico gestito da ogni dispositivo o su cui potrebbero risiedere certificati replicati.

Ciò implica che è necessario acquistare una licenza per ogni interfaccia di servizio che costituisce il componente logico del servizio di una connessione SSL, indipendentemente dal fatto che il tunnel SSL termini o meno su tale interfaccia. Tali interfacce possono includere, ad esempio, una singola istanza di un server Web, nel caso in cui la sessione SSL termini sul server Web, o più server Web, dietro un bilanciatore di carico.

Di seguito vengono descritte alcune situazioni comuni e i relativi requisiti per le licenze.

### **+ Siti in Standby e per il Ripristino in Caso di Disastro**

È necessario acquistare una licenza per ogni server in standby a caldo, ma non sono necessarie licenze aggiuntive per i server in standby a freddo.

### **+ Server Proxy Surrogati e Caching**

Non è necessario acquistare ulteriori licenze per i server proxy, indipendentemente dal fatto che vengano utilizzati o meno per salvare contenuto nella cache. Le licenze sono necessarie solo per i server dietro al server proxy surrogato.

### **+ Acceleratori e Offloader SSL**

Per gli acceleratori e gli offloader di rete è necessario acquistare una licenza per ogni server che utilizza un certificato SSL gestito da un acceleratore o un offloader SSL, indipendentemente dal fatto che la sessione SSL termini su o prima del server Web. Non è tuttavia necessaria alcuna licenza per l’acceleratore. Ad esempio, in una configurazione





con uno o due server Luna SA (ridondante) con un certificato utilizzato da nove server Web, è necessario acquistare nove licenze. Questa indicazione generale (una licenza per ogni server che dipende da un certificato gestito da un acceleratore SSL) si applica anche agli acceleratori basati su schede PCI.

#### **+ Bilanciatori di Carico**

È necessario acquistare una licenza per ogni server dietro o che punta a un bilanciatore di carico, se presente. Per i bilanciatori di carico che fungono anche da acceleratori SSL, consultare la sezione precedente “Acceleratori e Offloader SSL”. Nel caso si utilizzino combinazioni di acceleratori/bilanciatori di carico, non è necessario acquistare una licenza aggiuntiva per l’acceleratore fisico se la sessione SSL termina sui server dietro all’acceleratore e se per questi server è già stata ottenuta una licenza.

#### **+ Più Server Virtuali su un Singolo Server Fisico**

Se si utilizzano più server virtuali per gestire più domini su un singolo sistema fisico è necessario acquistare più licenze. Come indicato nella versione 4.0 del Contratto di registrazione dei certificati SSL di VeriSign®, per ogni server virtuale che risiede su un sistema fisico vengono applicate le stesse regole come se si trattasse di due sistemi fisici distinti. Ad esempio, se un server fisico funge da host per due server virtuali (uno per abc.com e l’altro per xyz.com), è necessario acquistare due licenze e non una sola.

#### **+ Modelli di Applicazioni Multi-livello con Certificati SSL tra i Livelli**

In presenza, dietro al livello del server iniziale, di ulteriori livelli di server applicativi che utilizzano certificati SSL tra i livelli, è necessario acquistare licenze aggiuntive. Se i livelli dipendenti fungono da servizi e utilizzano certificati SSL, i server che supportano tali livelli vengono considerati come server di primo livello e richiedono pertanto una licenza per ogni interfaccia del servizio, anche nel caso in cui i livelli dei servizi secondari facciano parte della stessa transazione atomica di livello utente controllata dal livello superiore.

#### **+ Servizi Web**

Se sono presenti gateway per servizi Web (WS) che utilizzano certificati SSL è necessario acquistare una licenza per ogni interfaccia logica del servizio Web, se l’interfaccia è un server WS e non un client. Consultare la sezione “Utilizzo dei certificati: differenze tra autenticazione di client e server” per ulteriori informazioni sul comportamento dei gateway XML in caso di client e server.

#### **+ Ambienti Mainframe**

Per i servizi basati su mainframe che utilizzano certificati SSL è necessario acquistare una licenza per ogni certificato presente nell’anello di server RACF, TopSecret o ACF2.

#### **+ Utilizzo dei Certificati: Differenze tra Autenticazione di Client e Server**

Se il certificato viene utilizzato per l’autenticazione di client attenersi alle seguenti linee guida. Se il sistema fisico, ad esempio il server di posta o gateway WS, dispone di un certificato SSL che viene utilizzato sia per l’autenticazione di server (serverAuth), quando riceve richieste da altri server di posta o funge da servizio WS, che di client (clientAuth), quando contatta altri server di posta o funge da client WS, è necessaria una sola licenza.

Se il certificato viene utilizzato solo per l’autenticazione di client, è necessario acquistare una licenza per ogni sistema fisico che utilizza tale certificato.

**+ Informazioni su VeriSign**

VeriSign (NASDAQ: VRSN) è il fornitore di servizi di infrastruttura Internet più affidabile a livello mondiale. Miliardi di volte al giorno i nostri servizi SSL, di autenticazione, di protezione dell'identità e di registrazione consentono ad aziende e consumatori in tutto il mondo di comunicare e completare transazioni commerciali in piena tranquillità.

VeriSign è il principale ente di certificazione SSL (Secure Sockets Layer) che garantisce commercio elettronico e comunicazioni sicure per siti Web, Intranet ed extranet.

VeriSign continua a distinguersi nel settore dei servizi di certificazione SSL in qualità di membro di CA/Browser Forum, un'organizzazione di volontari che ha definito indicazioni e metodologie per l'implementazione dei certificati SSL EV.

**Per ulteriori informazioni, visitare il sito all'indirizzo [www.Verisign.it](http://www.Verisign.it).**