



DOCUMENTO TECNICO

Come controllare i certificati
SSL per garantire una maggiore
sicurezza e affidabilità





SOMMARIO

+ Introduzione	3
+ Gestire crescita e complessità	3
+ Sei fasi verso il controllo centralizzato	4
+ SSL per le aziende	8
+ Conclusioni	9



Come controllare i certificati SSL per garantire una maggiore sicurezza e affidabilità

SCENARIO 1: SCADENZA IMPROVVISA

Il server che ospita il sito di commercio elettronico si arresta e nessuno ne capisce il motivo. Mentre il personale IT cerca di identificare il problema, ogni ora si perdono migliaia di Euro in mancate vendite. Alla fine si scopre che un certificato SSL è scaduto e che l'amministratore che lo aveva acquistato due anni fa non lavora più per la società. Per questo motivo l'amministratore corrente non aveva ricevuto alcuna notifica di rinnovo. Managed PKI per SSL di VeriSign® consente di specificare fino a tre indirizzi e-mail per le notifiche.

SCENARIO 2: PROGETTO DI CONSOLIDAMENTO

A seguito di una recente fusione, è necessario integrare due sistemi di rete. In tal ambito, è necessario acquistare cinque certificati SSL premium e cinque standard e aggiornare le informazioni di contatto per il dominio su tre certificati esistenti. L'acquisto di certificati singoli sottrarrebbe tempo prezioso alle altre attività di integrazione. Mediante Managed PKI per SSL di VeriSign è però possibile acquistare più certificati affinché vengano rinnovati ed emessi immediatamente.

+ Introduzione

Il numero di utenti Internet in tutto il mondo ha superato la soglia di 1 miliardo nel 2005 e si prevede che raggiunga i 2 miliardi entro il 2011.¹ Internet svolge un ruolo critico nelle attività operative e di vendita di organizzazioni di piccole o grandi dimensioni, a livello locale o globale, per mercati a larga diffusione o specifici. Prima di condividere informazioni personali e riservate online, le persone vogliono vedere indicatori di sicurezza che garantiscano che l'applicazione o il sito Web in questione sia affidabile e che le loro informazioni verranno crittografate. Quando un certificato SSL (Secure Sockets Layer) scade, non solo il proprietario perde delle occasioni di vendita, ma rischia anche di perdere la fiducia dei propri clienti. Il supporto per transazioni sicure su reti sempre più complesse richiede un processo migliore di gestione dei certificati SSL per le aziende.

+ Gestire crescita e complessità

I certificati SSL non vengono più utilizzati solo per il commercio elettronico. Se un'applicazione o un sito Web richiede l'immissione di un nome utente e di una password, la trasmissione di tali informazioni deve essere protetta mediante crittografia. Quando è necessario garantire la protezione di 10 o più server, la gestione dei singoli certificati diventa complicata, in quanto tali certificati potrebbero essere stati acquistati in momenti diversi, da diverse persone, mediante diversi fornitori. Per questi motivi potrebbe risultare difficile tenere traccia di quando tali certificati devono essere rinnovati e da chi. L'autenticazione di ogni singolo certificato inoltre rallenta il processo di acquisto di più certificati. Infine è possibile che alcuni amministratori acquistino e installino certificati SSL senza comunicarlo all'ufficio centrale.

Uno strumento di gestione dei certificati a livello aziendale aiuta a consolidare informazioni e gestione. Tuttavia la maggior parte degli strumenti di gestione consente di accedere a un solo tipo di certificato. Per una visione completa della sicurezza, è necessario disporre in tempo reale di informazioni sui tipi di certificati SSL utilizzati nei vari domini e reparti. Sebbene la centralizzazione del controllo sia una soluzione adatta ad alcune organizzazioni IT, altre preferiscono delegare la responsabilità amministrativa, mantenendo però un metodo per verificare le modifiche e gli aggiornamenti apportati.

Nessuno vuole infatti che un certificato SSL scada sotto la propria supervisione. La possibilità di monitorare i rinnovi a scadenze di 90, 60 e 30 giorni consente agli amministratori di sistema di pianificare e preparare il budget per tali rinnovi. Una migliore gestione delle notifiche e delle informazioni di contatto garantisce che vengano avvisate le persone giuste quando un certificato deve essere rinnovato. Rinnovi tempestivi e periodi di validità più estesi aiutano ad evitare interruzioni delle attività e a ridurre i costi di proprietà.

¹ Computer Industry Almanac, Inc. gennaio 2006. <http://www.c-i-a.com/pr0106.htm>

SCENARIO 3: CONTROLLO LOCALE CON SUPERVISIONE

L'ufficio in Cina deve emettere localmente un certificato per un server di sviluppo che deve essere messo online, ma a causa del fuso orario sono necessarie 24 ore per ricevere l'approvazione dalla sede centrale. Questo ritardo risulta essere un onere elevato da sostenere per un utilizzo preapprovato di un certificato in un dominio autorizzato da parte di un utente autenticato. Utilizzando Managed PKI per SSL di VeriSign è possibile delegare l'amministrazione per consentire l'emissione immediata di questo certificato.

SCENARIO 4: SPOSTAMENTO DI CERTIFICATI

A seguito della fusione di alcuni data center, è necessario spostare fisicamente dei certificati. Sebbene non si vogliono acquistare nuovi certificati per il nuovo sito e perdere il periodo di validità di quelli esistenti, non si è pronti nemmeno ad accettare l'interruzione dell'attività. Con Managed PKI per SSL di VeriSign è possibile utilizzare la funzione Revoca e sostituisci per spostare i certificati da una posizione all'altra.

+ Sei fasi verso il controllo centralizzato

In questa guida per professionisti IT viene illustrato come consolidare i certificati SSL in un singolo sistema di gestione basato su Web, utilizzando Managed PKI per SSL di VeriSign® per acquistare, emettere e gestire tutti i tipi di certificati SSL per l'intera azienda.

1. Analizzare tutti i domini e i certificati.
2. Confermare le informazioni di contatto di tutti i certificati.
3. Eseguire la migrazione di tutti i certificati in un conto gestito.
4. Definire un processo amministrativo per l'organizzazione.
5. Generare periodicamente report sui rinnovi e sulle unità disponibili.
6. Revocare e sostituire i certificati quando necessario.

Guida verso un controllo centralizzato

Quello che all'inizio è un server Web può rapidamente trasformarsi in una server farm, così come una società che inizia operando a livello locale può in poco tempo diventare un'azienda internazionale. Quando si verifica una crescita di questo genere, gli amministratori di sistema devono improvvisamente gestire diversi amministratori. Prima che la situazione diventi critica, è importante che l'organizzazione assuma il controllo dei certificati SSL dell'intera azienda e crei un sistema di gestione migliore, delineato dalle seguenti 6 fasi.

1. Analizzare tutti i domini e i certificati.

Durante questa fase è necessario prendere nota della posizione, della data di scadenza, del periodo di validità, del fornitore e del contatto per ogni certificato SSL dell'azienda. Sia che si incominci da zero o si faccia riferimento a un elenco esistente, è importante avvisare tutte le persone che potrebbero aver acquistato un certificato SSL e richiedere loro di contribuire. Oltre che per domini e server Web, i certificati possono essere utilizzati anche per proteggere applicazioni come i server di posta. Lo strumento NSLookup associa nomi di dominio a indirizzi IP per consentire di identificare i certificati mancanti. Se un certificato non è reperibile o non è più necessario, revocarlo per evitarne un uso improprio.

Questa fase è un buon momento per valutare i tipi di certificati utilizzati e assicurarsi che soddisfino le esigenze attuali. Ci si può domandare, ad esempio, se per un server Web pubblico ad elevata visibilità sia opportuno passare a un nuovo certificato SSL che soddisfi gli standard CA/Browser Forum Extended Validation o chiedersi se la intranet richiede protezione mediante certificati SSL.

Risultato: un elenco completo di tutti i domini e certificati.

2. Confermare le informazioni di contatto di tutti i certificati.

Durante il processo di registrazione della maggior parte dei certificati SSL, l'acquirente fornisce informazioni per il contatto tecnico, inclusi nome, numero di telefono e indirizzo e-mail. Il contatto tecnico svolge un ruolo importante durante il processo di autenticazione e rinnovo. Se questa persona lascia la società senza passare le consegne ad altri, è possibile che gli avvisi di rinnovo vengano spediti all'indirizzo sbagliato. La scadenza di un certificato potrebbe compromettere l'erogazione di un servizio critico. L'aggiornamento delle informazioni di contatto con un alias, ad esempio `admin_ssl@dominio.com`, garantisce che l'amministratore corrente riceva i messaggi.

Risultato: informazioni di contatto aggiornate in tutti i certificati.

VANTAGGI PRINCIPALI

Riduzione del costo di proprietà
È possibile ridurre il costo e la complessità della gestione di più certificati SSL per l'intera organizzazione mediante il controllo centralizzato e acquistando più certificati a un prezzo scontato.

Opzioni di gestione flessibili
È possibile definire il livello di controllo ideale per la gestione del ciclo di vita dei certificati grazie alla delega delle funzioni amministrative, al controllo degli accessi basato sui ruoli e all'assegnazione dinamica dei privilegi.

Migliore gestione dei rischi e del controllo
Monitoraggio dettagliato delle operazioni eseguite durante il ciclo di vita dei certificati. Blocco degli acquisti di certificati singoli da parte di business unit e consociate.

Maggiore fiducia dei clienti con VeriSign
Oltre il 93% delle società nell'elenco Fortune 500 e dei 40 più importanti istituti bancari a livello mondiale hanno scelto VeriSign come fornitore di certificati SSL. Questi clienti hanno fiducia nella nostra tecnologia di crittografia e nelle nostre rigorose procedure di autenticazione delle aziende.

3. Eseguire la migrazione di tutti i certificati in un conto gestito.

Se l'azienda richiede 10 o più certificati SSL, il consolidamento dei certificati in un singolo conto gestito consente di risparmiare tempo e denaro. Man mano che i certificati correnti si avvicinano alla data di scadenza, sostituirli con unità provenienti dal conto gestito principale. Per il consolidamento selezionare un conto di gestione principale che supporti tutti i tipi di certificati necessari. I certificati SSL oggi disponibili offrono diversi livelli di autenticazione e crittografia. Purtroppo molti degli strumenti di gestione dei certificati SSL a livello aziendale richiedono dati di accesso diversi per ogni tipo di certificato. Con la crescita dell'organizzazione e del numero di amministratori, la gestione di più conti per i diversi tipi di certificati SSL diventa onerosa a meno che il controllo non venga centralizzato.

Risultato: un singolo conto gestito per tutti i certificati dell'azienda.

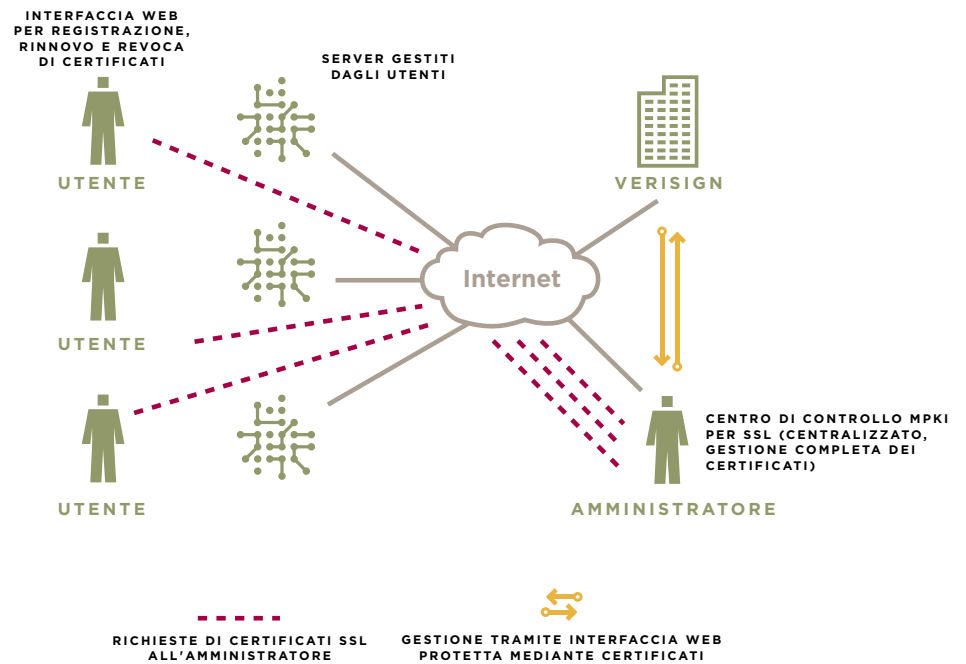
4. Definire un processo amministrativo per l'organizzazione.

Un conto di gestione dei certificati a livello aziendale consente agli amministratori autorizzati di acquistare contemporaneamente più unità di certificato da emettere, in base alle necessità, per l'intera organizzazione. L'amministratore definisce un processo per l'amministrazione in base al livello di controllo desiderato, ad esempio la gestione dei privilegi di accesso, la procedura di registrazione e chi riceve i diversi tipi di notifica.

Tipo di amministratore	Attività consentite
Amministratore della sicurezza	Assegnazione di ruoli (privilegi di amministratori e accesso wizard) ad altri amministratori.
Amministratore di configurazione	Configurazione di Managed PKI per SSL di VeriSign, definizione del contenuto della pagina di registrazione e gestione delle funzioni di database e generazione di report.
Amministratore della gestione dei certificati	Approvazione e rifiuto delle richieste di certificato, revoca dei certificati, delega delle richieste ad altri amministratori e gestione del ciclo di vita del certificato. Per semplificare il processo di autenticazione, potrebbe essere utile assegnare il ruolo di gestione dei certificati a una persona che conosce bene un determinato gruppo di utenti.
Sola lettura	Visualizzazione delle richieste correnti, dei dati dei certificati e dei file di log. Si tratta del ruolo predefinito per tutti gli amministratori dopo il primo amministratore.

Il sistema di gestione dei certificati deve offrire la flessibilità e gli strumenti di personalizzazione necessari per adattarsi all'ambiente. Un controllo degli accessi basato sui ruoli e l'assegnazione dinamica dei privilegi consentono di definire il processo amministrativo. Gli amministratori accedono al sistema specificando credenziali univoche che consentono loro di completare le attività che possono svolgere in base al proprio ruolo e organizzazione.

Figura 1: Modello Managed PKI per SSL di VeriSign



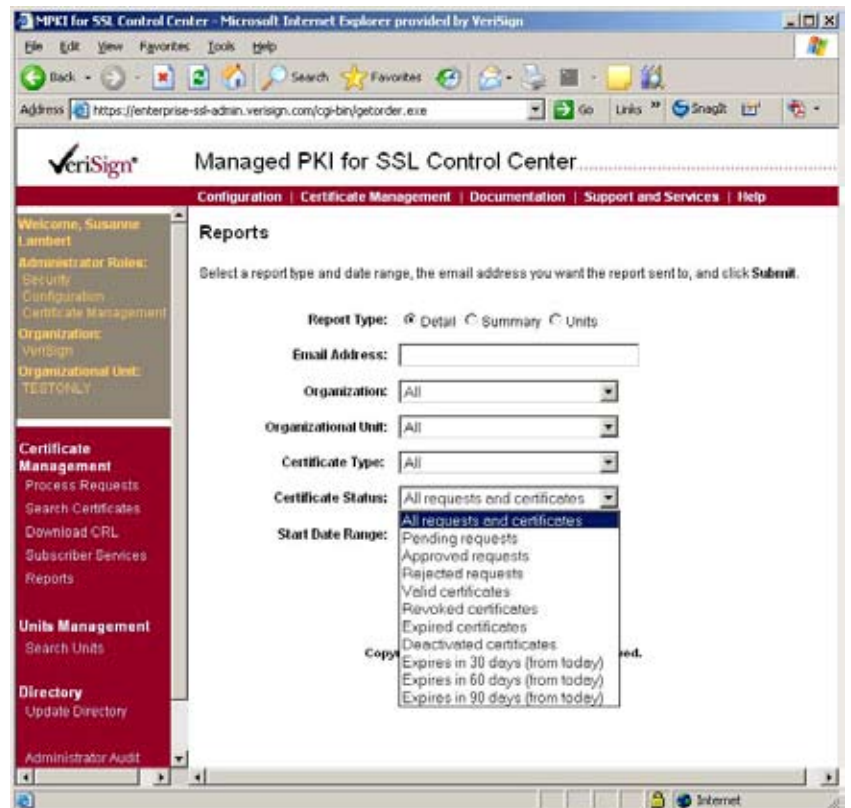
Quando un utente deve richiedere un certificato SSL, visita una pagina di registrazione e compila un modulo Web. Il certificato può venire immediatamente approvato o rifiutato o impostato come in sospeso, a seconda delle regole amministrative configurate. Il blocco dei domini impedisce agli utenti di acquistare singoli certificati per domini gestiti, indirizzandoli alla pagina di registrazione del conto gestito.

Le notifiche preimpostate consentono di velocizzare il processo mantenendo gli amministratori sempre informati. Gli avvisi di scadenza possono venire inviati, come e-mail o SMS, a più amministratori e a un conto alias. Quando il numero di unità di certificato disponibili scende sotto un certo valore, l'amministratore riceve un avviso che lo informa che è necessario acquistarne di aggiuntive. Gli avvisi di richieste in sospeso invece segnalano agli amministratori che devono accedere al conto per esaminare tali richieste. Le e-mail di conferma comunicano agli amministratori quando vengono emessi dei certificati automaticamente.

Risultato: un processo amministrativo chiaramente articolato, integrato nel sistema di gestione.

5. **Generare periodicamente report sui rinnovi e sulle unità disponibili.**

L'accesso in tempo reale alle informazioni sui certificati SSL dell'intera azienda consente agli amministratori di sistema di ottimizzare tempo e risorse. Infatti, invece di tenere traccia dei certificati in fogli di calcolo, consuntivi e report dettagliati mostrano l'inventario corrente delle unità per tutta l'azienda in base allo stato dei certificati, ossia tutte le richieste e i certificati in sospeso, approvati, rifiutati, validi, revocati, disattivati, scaduti o prossimi alla scadenza. Un report sui rinnovi, che include certificati in scadenza a 90, 60 e 30 giorni, consente agli amministratori di pianificare il budget trimestrale per il rinnovo dei certificati SSL. Gli amministratori possono personalizzare i report con dettagli sull'uso dei certificati in base all'organizzazione o all'amministratore. Nei log vengono registrate informazioni cronologiche dettagliate su tutte le operazioni eseguite dagli amministratori per tutti i certificati emessi.



Risultato: migliore supervisione e allocazione delle risorse.

6. **Revocare e sostituire i certificati quando necessario.**

Gli strumenti di gestione e inventario consolidati semplificano le operazioni di revoca e sostituzione dei certificati. Se una chiave privata viene persa o risulta compromessa, o se un server si arresta in modo anomalo e un certificato viene eliminato, l'amministratore può revocare il certificato ed emetterne uno sostitutivo.

Risultato: maggiore controllo sui certificati persi o mancanti.

+ SSL per le aziende

Il costo e la complessità di gestire singoli certificati SSL aumentano rapidamente con la crescita dell'organizzazione e l'espansione dei servizi online. Installare e gestire la propria autorità di certificazione (CA) per l'emissione di certificati SSL risulta inefficiente e richiede molte risorse. Managed PKI per SSL di VeriSign è un'applicazione basata su Web di semplice utilizzo che consente di emettere, rinnovare, revocare e gestire certificati SSL. Un amministratore può personalizzare le pagine di registrazione dell'organizzazione, mentre VeriSign gestisce i servizi back-end all'interno della propria infrastruttura all'avanguardia.

Caratteristiche di Managed PKI per SSL di VeriSign

Acquisto	Possibilità di acquistare tutti i tipi di certificati di VeriSign per più organizzazioni dallo stesso conto
Registrazione	Pagine di registrazione personalizzabili con il proprio logo e possibilità di emissione immediata
Avvisi	Avvisi di reintegro, notifiche di rinnovo
Emissione	Emissione immediata dei certificati
Sostituzione illimitata	Sostituzione dei certificati illimitata e revoca gratuita per 30 giorni
Gestione mediante interfaccia Web	Possibilità di gestire tutti i tipi di certificati di VeriSign per più organizzazioni dallo stesso portale
Panoramica dei certificati	Verifica dello stato dei certificati per tutte le organizzazioni, i domini e gli amministratori
Generazione di report	Report riepilogativi e dettagliati sui certificati in base al tipo, allo stato, all'organizzazione, alla data di scadenza e all'utilizzo
Registrazioni	Log contenenti tutte le azioni effettuate sui certificati e dagli amministratori, per tutte le organizzazioni e i tipi di certificati
Amministrazione delegata	Delega delle responsabilità e dei privilegi degli amministratori per organizzazione e unità organizzativa
Sicurezza	Autenticazione a due fattori per gli amministratori, controllo degli accessi basato sui ruoli e blocco dell'acquisto di certificati singoli
Periodo di validità	Periodi di validità di uno, due o tre anni
Domini	Emissione di certificati per più domini, aggiunta di nomi di dominio e assegnazione di domini alle organizzazioni
Supporto	Assistenza telefonica, via Web, e-mail e interattiva online inclusa per 60 giorni e disponibilità di piani di supporto estesi
Utilizzo	Siti Web, intranet, extranet, siti di commercio elettronico, più server logici
Compatibilità browser	Compatibilità con praticamente tutti i browser

Managed PKI per SSL di VeriSign offre accesso a tutti i certificati SSL di VeriSign, mettendo a disposizione una forte crittografia, un rigoroso processo di autenticazione, il simbolo VeriSign Secured™ Seal e un piano di protezione NetSure® con una garanzia estesa fino a \$ 250.000. VeriSign è uno dei principali fornitori di certificati SSL con funzionalità SGC, che permettono di offrire una protezione con crittografia a 128 o 256 bit a oltre il 99,9% degli utenti Internet.

Certificati Managed PKI per SSL di VeriSign

Certificati SSL Extended Validation	Crittografia SSL a 128 o 256 bit reali con il processo di autenticazione più severo, che supporta la barra degli indirizzi verde e il simbolo VeriSign Secured Seal
Certificati SSL Premium	Crittografia SSL a 128 o 256 bit reali e il simbolo VeriSign Secured Seal
Certificati SSL Standard	Crittografia di alta qualità e il simbolo VeriSign Secured Seal
Certificati SSL Intranet Premium	Crittografia SSL a 128 o 256 bit reali per la sicurezza interna
Certificati SSL Intranet Standard	Crittografia di alta qualità per la sicurezza interna
Certificati Code Signing	Garanzia di integrità e proprietà di codice e contenuto
Certificati SSL per istituti finanziari che utilizzano OFX	Autenticazione e protezione delle transazioni su Internet per istituti finanziari scelti

+ Conclusioni

La fiducia e la sicurezza delle applicazioni Web critiche si basano sui certificati SSL, in quanto offrono una forte crittografia dei dati e un'autenticazione affidabile del sito e della società con cui il cliente interagisce. Managed PKI per SSL di VeriSign offre alle aziende e ai fornitori di servizi certificati SSL emessi dal fornitore di sicurezza più riconosciuto sul Web e gli strumenti per gestirli nell'intera organizzazione.

Per ulteriori informazioni, visitare il sito Web www.VeriSign.it.