

Installare e utilizzare i certificati SSL

La tua guida essenziale





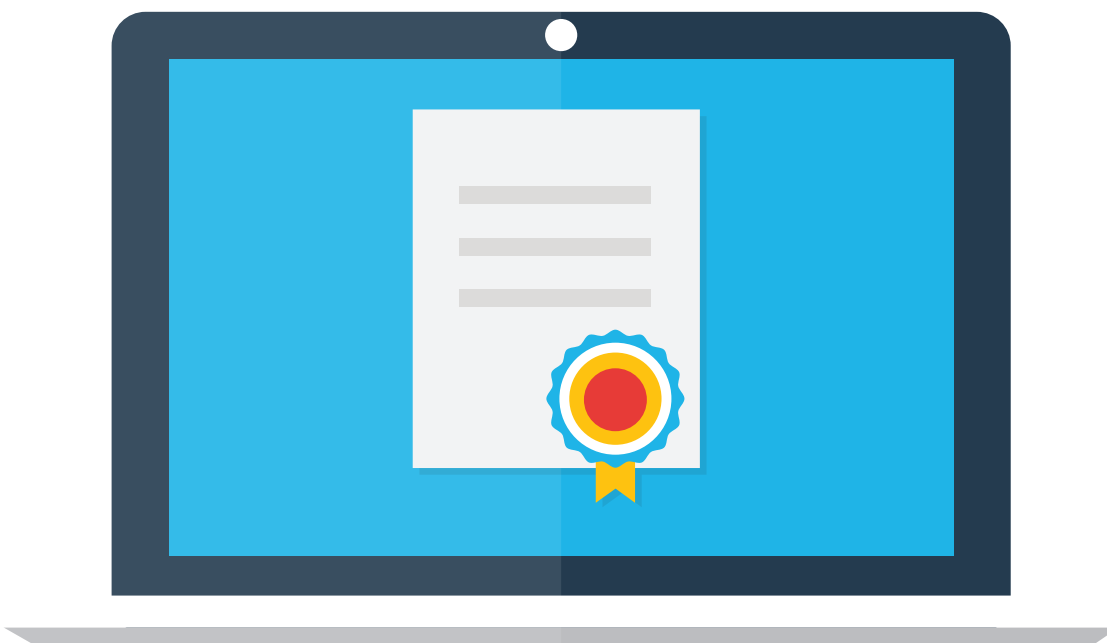
Cosa fare una volta acquistato un certificato SSL.

L'acquisto del certificato è solo uno dei numerosi passaggi necessari per proteggere il tuo sito Web. Troppo spesso si verifica che i certificati non vengano installati nel modo appropriato, che pagine riservate rimangano esposte e che i dati dei moduli vengano inviati senza essere crittografati, lasciando molti siti Web in balia di possibili attacchi.

Symantec ha raccolto in questa guida una serie di suggerimenti strategici per affrontare al meglio il processo di messa in sicurezza del sito. Aiutandoti a evitare le minacce del Web e le pratiche meno raccomandabili per l'efficacia della protezione del sito, il tuo certificato SSL potrà essere il tuo passaporto verso un mondo di interazioni più sicuro per te, per i tuoi collaboratori e per i tuoi clienti.

C'è un solo modo per installare un certificato SSL. Installarlo correttamente.

Come molte altre organizzazioni, anche la tua ha riconosciuto l'esigenza di compiere un passo fondamentale, acquistando un certificato SSL. Adesso è il momento di installarlo nel modo appropriato. L'approssimazione non è ammessa: i visitatori che non si sentano completamente al sicuro nel sito lo abbandoneranno al più presto possibile.





SUGGERIMENTO 1 - Prepara la chiave privata e la CSR



Per installare un certificato digitale, è innanzitutto necessario generare la chiave privata e, da questa, la richiesta di firma del certificato (CSR, Certificate Signing Request) per il server in cui si intende installarlo. Quindi si invia la richiesta CSR per la registrazione del certificato. Ecco come procedere.

Se disponi di server IIS 6 o versione successiva o di server Redhat Linux, puoi scaricare lo strumento [Symantec SSL Assistant](#) e seguire l'intuitiva procedura guidata. Per un elenco di istruzioni per la generazione della richiesta CSR su altri server, visita la pagina [Symantec CSR Generation](#). Per richiedere un servizio relativo ai certificati SSL di Symantec, sono necessarie le seguenti informazioni:

- Durata o periodo di validità del certificato: 1, 2 o 3 anni
- Numero di server che ospitano un unico dominio (fino a 5 server)
- Piattaforma server
- Organizzazione, unità organizzativa, indirizzo
- Informazioni per il pagamento e un contatto per la fatturazione
- Nome comune: questo corrisponde al nome host + nome dominio, ad esempio "www.miodominio.com" o "webmail.miodominio.com"
- Indirizzo e-mail per la verifica delle informazioni da parte di Symantec
- Una richiesta di firma del certificato (CSR) generata dal server che deve essere protetto

Una volta ottenuto il certificato, attieniti alla procedura indicata al Suggerimento 3.

Se il tuo server non è tra quelli elencati o se desideri ulteriori informazioni, consulta la documentazione del server o contatta il relativo produttore. Se non conosci il software utilizzato dal tuo server, contatta i tuoi amministratori IT.

Per la registrazione, racchiudi la richiesta CSR da inviare tra le seguenti stringhe:

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



SUGGERIMENTO 2 - Installa correttamente il certificato SSL



È la prima volta che installi un certificato SSL? Nessun problema: è più semplice di quanto pensi. Segui la procedura per installare il certificato Symantec sul server.

La procedura è la stessa per tutti i tipi di server:

Passaggio 1 - Salva il certificato

Segui le istruzioni fornite nell'e-mail di conferma per salvare il certificato SSL sul desktop dall'URL indicato. Ti verranno forniti sia il certificato in questione che i certificati delle CA intermedie necessari.

Passaggio 2 - Installa o sposta il certificato in una cartella appropriata

Passaggio 3 - Configura il certificato sul sito Web

Passaggio 4 - Fai riferimento al certificato

[Fai clic qui](#) per informazioni dettagliate e per la procedura completa per ciascun tipo di server.

Per sfruttare appieno la protezione offerta dal certificato SSL, aggiungi il Norton Secured Seal al tuo sito Web. La presenza di questo simbolo comunicherà maggiore fiducia ai visitatori che si accingono a completare transazioni nel sito.

Copia e incolla le righe appropriate delle pagine Symantec dedicate al Norton Secured Seal per aggiungere il simbolo al tuo sito. A questo scopo, segui la semplice procedura fornita al link indicato alla fine del presente suggerimento. In questa viene anche spiegato come testare il certificato mediante lo strumento Certificate Installation Checker immettendo il dominio quando richiesto.

A questo punto il certificato SSL è installato e pronto per l'implementazione.

In caso di problemi

Symantec mette a disposizione un'ampia gamma di esercitazioni video per vari tipi di server: [accedi alle esercitazioni](#)

Verifica dell'installazione

Immetti l'URL del server che desideri controllare: [verifica l'installazione](#)

Generazione del Site Seal

Segui le istruzioni per installare il Norton Secured Seal: [genera il Site Seal](#)

Risoluzione dei problemi

Visita il sito del Supporto Symantec: [accedi al supporto](#)



SUGGERIMENTO 3 - Proteggi le chiavi private e scegli il meglio



Le chiavi pubbliche e private sono una componente fondamentale del meccanismo SSL. La chiave privata viene mantenuta segreta nel server e utilizzata per crittografare tutti i dati del sito Web. La chiave pubblica contenuta all'interno del certificato è un altro elemento costitutivo dell'identità del sito Web, come il nome del dominio e le informazioni dell'organizzazione.

Tratta le tue chiavi private come una risorsa preziosa, condivisa tra un numero ristretto di colleghi o collaboratori di fiducia. Immagina di essere un direttore di banca: consegneresti le chiavi del caveau a chiunque? Ovviamente no. Ecco perciò alcune prassi che sarà opportuno osservare:

- **Genera le chiavi private su un server affidabile.** Non affidare questo compito a terzi.
- **Proteggi le chiavi private con password** per impedirne la violazione quando sono archiviate nei sistemi di backup.
- **Rinnova i certificati ogni anno** e, in quella occasione, introduci sempre nuove chiavi private.

La dimensione della chiave privata ha un significativo impatto sull'handshake crittografico necessario per stabilire connessioni sicure. L'utilizzo di una chiave troppo breve è poco affidabile, ma una chiave troppo lunga può rallentare notevolmente le prestazioni.

Nel panorama dei metodi di crittografia correnti si sta affermando la crittografia su curve ellittiche (ECC, Elliptic Curve Cryptography), che fornisce protezione avanzata pur utilizzando chiavi di lunghezza inferiore. Symantec offre ECC con chiavi le cui dimensioni in bit sono un sottomultiplo di quelle richieste da RSA e DSA, nonostante siano oltre 10.000 volte più difficili da violare (i 256 bit di una chiave ECC hanno la forza crittografica di 3072 bit RSA). ECC offre una sicurezza più rigorosa a condizioni di carico inferiori per il server e contribuisce a ridurre i cicli di CPU richiesti per le operazioni crittografiche sul server.

Ulteriori informazioni su ECC sono disponibili a pagina 7.



SUGGERIMENTO 4 - Elimina gli anelli deboli della catena



Nella maggior parte delle distribuzioni SSL, il solo certificato del server non è sufficiente: per stabilire una catena di fiducia completa sono necessari almeno tre o più certificati. Una catena di certificati è costituita da tutti i certificati necessari per confermare l'affidabilità del soggetto identificato dal certificato finale.

In pratica, la catena include il certificato dell'entità finale, i certificati delle CA intermedie e il certificato della CA radice.

La procedura di verifica dell'autenticità e della validità di un nuovo certificato implica il controllo di tutti i certificati, dalla CA radice universalmente attendibile alle CA intermedie fino al certificato appena ricevuto: il certificato dell'entità finale. Un certificato può essere considerato attendibile solo se ciascun certificato nella relativa catena è stato correttamente rilasciato e convalidato.

Un problema frequente consiste nella mancata inclusione dei certificati delle CA intermedie nella catena, nonostante la corretta configurazione del certificato dell'entità finale. Puoi verificare se i certificati intermedi sono stati installati in modo corretto utilizzando il nostro [strumento di controllo certificati](#).



SUGGERIMENTO 5 - RSA, ECC e importanza della lunghezza delle chiavi



La crittografia su curve ellittiche (ECC) fornisce il livello di protezione più avanzato e più performante nel panorama dei metodi di crittografia correnti.

Metodo di crittografia approvato dal governo degli Stati Uniti e dall'US National Security Agency (NSA), ECC crea le chiavi di crittografia sulla base dei punti di una curva ellittica che definiscono una coppia di chiavi pubblica/privata. Estremamente resistente agli attacchi di forza bruta spesso utilizzati dagli hacker, offre una soluzione più rapida e meno esigente in termini di risorse di elaborazione rispetto alla crittografia basata su RSA.

Come algoritmo di crittografia e di firma digitale, RSA ha svolto un ruolo fondamentale nella sicurezza Internet degli ultimi vent'anni. Il suo impiego rimane tuttora valido, ma l'aumento delle dimensioni di chiave minime accettabili per offrire protezione dagli attacchi crittografici di ultima generazione ne sta mettendo in discussione l'efficienza. ECC garantisce migliori prestazioni, in quanto richiede chiavi di lunghezza inferiore pur fornendo un livello superiore di sicurezza. Una chiave ECC a 256 bit, ad esempio, offre infatti il medesimo grado di sicurezza di una chiave RSA a 3072 bit. Il risultato è una sicurezza rigorosa che non pregiudica le prestazioni.

La minore lunghezza delle chiavi ECC comporta inoltre certificati di dimensioni inferiori, con un consumo minore di larghezza di banda. Caratteristica preziosa, tenuto conto del diffondersi presso i consumatori dell'uso dei dispositivi mobili anche per le transazioni online, con l'opportunità di offrire con ECC un'esperienza più gratificante al cliente.

Supportati per i tre browser più diffusi fin dal 2007, i certificati ECC radice di Symantec sono compatibili con la tua infrastruttura esistente, purché utilizzati con i browser di ultima generazione, e disponibili senza costi aggiuntivi.

Per ulteriori informazioni su ECC e sull'agilità dell'algoritmo, [fai clic qui](#).



SUGGERIMENTO 6 - Sicurezza integrale con Always On SSL



Implementare la crittografia SSL è un'ottima misura. Ma vuoi fare un passo in più? Estendila all'intero sito con Always On SSL. Si tratta di una soluzione conveniente per proteggere l'esperienza degli utenti del sito Web, dall'accesso fino all'ultimo momento della loro visita, rendendo più sicure attività come la ricerca, la condivisione e l'acquisto online.

Per le aziende che attribuiscono grande importanza alla protezione dei clienti e alla propria reputazione è consigliabile implementare Always On SSL e i certificati SSL emessi da una CA attendibile, come Symantec. Facile da implementare, questa misura di sicurezza permette di autenticare l'identità del sito Web e di crittografare tutte le informazioni condivise tra il sito e l'utente, cookie inclusi, proteggendo i dati dall'accesso non autorizzato, dalla contraffazione o dall'abuso.

Non è un caso che la Online Trust Alliance esorti tutti i siti Web ad adottare l'approccio Always On SSL, definendolo "una misura di sicurezza pratica e di provata efficacia che dovrebbe essere implementata su tutti i siti Web in cui gli utenti accedono a informazioni riservate o le condividono".

Molti dei siti più rinomati del Web hanno riconosciuto il valore di Always On SSL e, implementandolo, si sono garantiti la protezione dai pericoli del sidejacking e delle altre violazioni che minacce come Firesheep e l'inoculazione di malware possono comportare.

Always On SSL può aiutarti a proteggere la fiducia che gli utenti tributano al tuo sito, dimostrando che la loro privacy e la loro sicurezza ti stanno a cuore e che fai tutto quanto è nelle tue possibilità per tutelarle.



SUGGERIMENTO 7 - Pinning della chiave pubblica: una questione di fiducia



Il pinning della chiave pubblica (più propriamente noto come Public Key Pinning Extension for HTTP o HPKP) è progettato per offrire agli operatori dei siti Web un mezzo per specificare in modo tassativo le CA autorizzate a rilasciare i certificati i propri server.

In sostanza, il pinning della chiave pubblica crea un'associazione tra un host e il relativo certificato o chiave pubblica prevista. Una volta che una chiave pubblica viene rilevata per un determinato host, essa viene associata o, letteralmente, “fissata” a tale host.

Secondo il CA Security Council, il pinning della chiave pubblica consente al proprietario del sito Web di dichiarare che il relativo certificato SSL deve possedere uno o più dei seguenti elementi:

- Una chiave pubblica specificata
- La firma con la chiave pubblica specificata da parte di una CA
- Una gerarchia di trust con una CA tramite la chiave pubblica specificata

Se un certificato per il dominio del proprietario del sito Web viene rilasciato da una CA non elencata (ossia, non “fissata”), un browser che supporti il pinning della chiave pubblica mostrerà un avviso di attendibilità. I proprietari dei siti Web possono inoltre eseguire il pinning di più chiavi rilasciate da CA differenti, che verranno considerate come valide dai browser.

Il proprietario del sito Web può contare sul fatto che le CA prescelte non rilasceranno erroneamente un certificato per il proprio dominio. Spesso queste CA pongono restrizioni su chi può richiedere il rilascio di un certificato per i domini specifici del proprietario, fornendo così un livello aggiuntivo di sicurezza contro il rischio che i certificati vengano erroneamente rilasciati a soggetti non autorizzati.

Il CA Security Council ha dichiarato la non scalabilità del pinning della chiave pubblica implementato nel 2011 da Google, in quanto richiede l'aggiunta al browser delle chiavi pubbliche per ciascun dominio. Tuttavia, una nuova soluzione di pinning della chiave pubblica scalabile è stata documentata attraverso una RFC (Request for Comments) proposta dall'IETF (Internet Engineering Task Force).

In tale proposta, i pin della chiave pubblica verranno definiti tramite un'intestazione HTTP dal server al browser. L'opzione di intestazione può contenere, ad esempio, un algoritmo a chiave SHA-1 e/o SHA-256, la durata massima del pin, il supporto o meno dei sottodomini e la rigorosità del pinning.



SUGGERIMENTO 8 - Dissuadi i curiosi con la Perfect Forward Secrecy



Come ti sentiresti al pensiero che qualcuno, oltre a intercettare abusivamente il tuo traffico dati, riesca un giorno a decifrarlo? Non proprio tranquillo, ovviamente. Eppure è questa la situazione in cui molte organizzazioni si trovano, spesso a loro completa insaputa.

Prendiamo il caso della protezione RSA: questa genera una chiave pubblica e una privata per crittografare e decifrare i messaggi. Eppure l'utilizzo continuo di chiavi riutilizzabili rende i dati archiviati accessibili in caso di futura violazione delle chiavi. In molti casi, un hacker in possesso della tua chiave privata e del traffico SSL abusivamente acquisito potrà utilizzare la prima per decifrare tutte le chiavi di sessione negoziate nel corso degli handshake SSL salvati e quindi utilizzare queste ultime per decifrare tutti i dati di sessione salvati. Scenari come questi non ispirano sonni tranquilli. Ma esiste una soluzione migliore, denominata "Perfect Forward Secrecy" (PFS).

Essa prevede la generazione di chiavi di sessione temporanee e non recuperabili, che una volta utilizzate verranno definitivamente eliminate. Inoltre, quando integrata appropriatamente con la crittografia a curva ellittica (ECC), la tecnologia PFS offre maggiore sicurezza ed efficienza rispetto agli algoritmi RSA.

PFS non prevede alcun collegamento tra la chiave privata del server e ciascuna chiave di sessione. Se sia il client che il server la supportano, utilizzeranno una variante di un protocollo denominato, dal nome dei suoi inventori, Diffie-Hellman, in base a cui entrambe le parti si scambiano numeri casuali per giungere allo stesso segreto condiviso. Si tratta di un algoritmo intelligente, in grado di impedire a soggetti non autorizzati di ricavare il segreto, anche qualora fossero in grado di intercettare tutto il traffico.

Per ulteriori informazioni guarda l'infografica Symantec:

[Guarda l'infografica](#)



SUGGERIMENTO 9 - HTTP Strict Transport Security (HSTS): la tua rete di sicurezza



Quando si parla di scenari online, la sicurezza non è mai troppa. E per potersi di dire ragionevolmente tranquilli è spesso necessario quel passo in più, oltre la sicurezza standard.

Gli hacker possono utilizzare attacchi man-in-the-middle attraverso le reti wireless, come gli attacchi SSLstrip, per intercettare le richieste inviate dal browser ai siti HTTPS e restituire le pagine richieste su HTTP. In questo modo, rimuovendo la protezione crittografica per la connessione, gli hacker possono intercettare le informazioni immesse dalle vittime nel sito Web che suppongono sicuro. E l'eventualità che le vittime si accorgano della violazione è remota, in quanto è piuttosto improbabile che prestino attenzione alla barra degli indirizzi del browser mentre passano da una pagina all'altra del sito. Inoltre, poiché i browser non sono in grado di determinare se le pagine del sito Web devono essere restituite in modo sicuro, difficilmente mostreranno un avviso quando un sito viene caricato tramite una connessione non crittografata.

HTTP Strict Transport Security (HSTS) impedisce questo tipo di violazione consentendo ai server di inviare un messaggio al browser per richiedere che tutte le connessioni specificate siano crittografate. Il browser quindi applica l'istruzione, crittografando ogni pagina Web visitata dagli utenti come richiesto e proteggendo le aziende proprietarie dei siti e i loro clienti dagli attacchi.

Per attivare la protezione HSTS è sufficiente impostare una singola intestazione di risposta nei siti Web da proteggere. Quindi, i browser che supportano HSTS (ad esempio Chromium, Google Chrome, Firefox, Opera e Safari) rispetteranno le relative istruzioni. Una volta attivata, HSTS non consentirà comunicazioni non sicure con il sito Web: un risultato ottenuto convertendo automaticamente tutti i link in testo normale in link sicuri.

Internet Explorer non supporta ancora HSTS, ma Microsoft ne ha preannunciato l'introduzione a partire da Internet Explorer 12.

© 2015, Symantec Corporation.
Tutti i diritti riservati. Symantec, il logo Symantec,
il logo Checkmark e il logo Norton Secured sono
marchi o marchi registrati di Symantec Corporation o
delle sue consociate negli Stati Uniti e in altri paesi.
Altri nomi possono essere marchi commerciali dei
rispettivi proprietari.