



DOCUMENTO TECNICO

Sicurezza e affidabilità sono
indispensabili per qualsiasi attività
di commercio su Internet





SOMMARIO

+ Introduzione	3
+ Tecnologia di crittografia e certificati SSL	4
Livelli di crittografia e SGC	5
Livelli di autenticazione e affidabilità	5
+ EV: il nuovo standard di affidabilità	7
+ Certificati SSL di VeriSign per la massima sicurezza e affidabilità	9
+ Conclusioni	10



Sicurezza e affidabilità sono indispensabili per qualsiasi attività di commercio su Internet

+ Introduzione

Guadagnarsi la fiducia dei clienti online è indispensabile per il successo di qualsiasi società che trasferisce o trasmette dati riservati sul Web. Nell'effettuare acquisti online, i clienti temono il furto della propria identità e sono, pertanto, diffidenti nel fornire informazioni personali, in particolare i dettagli della carta di credito, a fonti non affidabili. Altri generi di attività online richiedono altri tipi di informazioni altrettanto riservate. Le persone sono restie a fornire numero di previdenza sociale, password o altri dati personali di carattere riservato, e in alcuni casi addirittura il nome, l'indirizzo o il numero di telefono, in quanto temono che tali informazioni vengano intercettate durante la trasmissione o che il sito di destinazione stesso sia gestito da impostori con cattive intenzioni.

Il risultato finale è la mancata finalizzazione della transazione commerciale. In base a una ricerca condotta da TNS nel 2006 risulta che il 70% degli acquirenti online non hanno portato a termine l'acquisto a causa di preoccupazioni relative alla sicurezza. Alcuni clienti riescono magari a mettere da parte i timori quando si tratta di acquisti di piccola entità, ma impongono un limite all'importo delle loro transazioni per paura che qualcuno intaschi i soldi senza fornire il prodotto o il servizio promesso.

Queste paure sono infatti ben fondate. A causa delle frodi online, nel solo 2007 sono state riportate delle perdite di profitto su transazioni online per un importo pari a 3,6 miliardi di dollari, con un incremento del 16% rispetto al 2006. Il numero di casi di phishing sottoposti all'attenzione dell'associazione Anti-Phishing Working Group (APWG) nel gennaio 2008 corrispondeva a 29.284, con un aumento di quasi il 9% rispetto al mese precedente.¹

È fondamentale che le aziende con attività online intervengano al fine di rassicurare i clienti, perché la paura di frodi su Internet costituisce un enorme deterrente per le vendite. In base a una ricerca svolta da TNS nell'agosto 2006 risulta che l'87% dei consumatori che effettuano acquisti online teme di diventare vittima di frodi relative alla propria carta di credito e che l'83% ha paura di fornire informazioni di carattere personale. Poiché la paura di truffe limita non solo il numero ma anche l'entità delle transazioni, l'aumento della fiducia dei clienti significherebbe un incremento del volume di affari.

Anche ai consumatori conviene che questa barriera di sfiducia venga abbattuta, in quanto niente è più conveniente ed economico che acquistare online. Non è raro che un cliente che desidera acquistare un particolare articolo lo trovi non solo su un sito Web affidabile, ma anche su un altro sito a un costo inferiore o con condizioni migliori. Sarebbe quindi meglio anche per il consumatore se esistesse un metodo semplice e rapido per potere fidarsi del sito meno accreditato. La paura di essere derubati della propria identità (timore condiviso dall'85% degli acquirenti online, secondo un sondaggio di TNS dell'agosto 2006) impedisce però a molte persone di sfruttare i vantaggi offerti dagli acquisti online. Infatti, come indicato da un sondaggio di Forrester Research condotto nel dicembre 2006, il 24% degli intervistati non effettua alcun acquisto online.

Fortunatamente oggi è disponibile la tecnologia necessaria per consentire alle aziende con attività online di proteggere i dati riservati dei clienti, gestire l'autenticazione e guadagnarsi la fiducia dei clienti, nonché consentire ai clienti di differenziare tra siti Web affidabili e copie create da truffatori a scopo di frode.

¹ APWG "Phishing Activity Trends", gennaio 2008

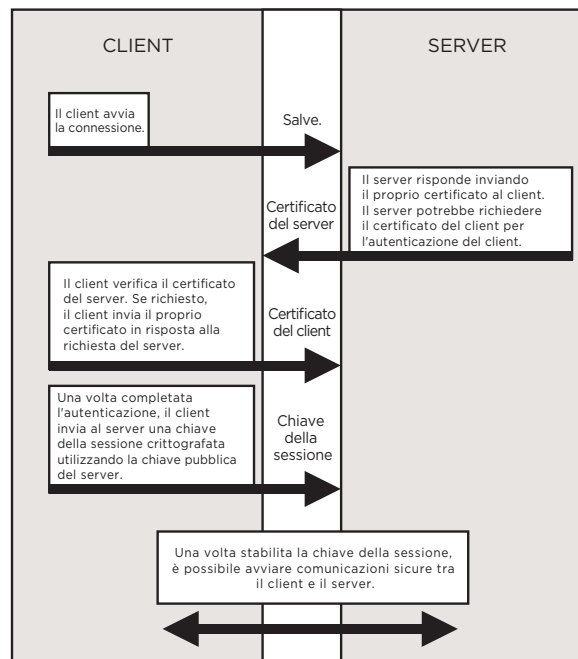
In questo documento viene analizzato lo stato attuale della tecnologia ed esaminati i contributi apportati da VeriSign per consentire alle organizzazioni di proteggere i dati critici e instillare maggiore fiducia nei clienti. Per prima cosa vengono descritte la crittografia e SSL (Secure Sockets Layer), ossia la tecnologia nata in risposta al problema più antico ed evidente delle attività commerciali online: l'intercettazione dei dati in transito da parte di criminali cibernetici. Tuttavia, con la sempre maggiore sofisticazione di questa generazione di criminali, la crittografia non è più sufficiente. In questo documento vengono perciò presentati i problemi di autenticazione e credibilità, che attualmente hanno raggiunto livelli critici, e viene illustrata la tecnologia SSL EV sviluppata in risposta a questi problemi. Infine vengono introdotte le soluzioni di VeriSign®, che offrono il meglio per tutte le tecnologie di sicurezza.

+ Tecnologia di crittografia e certificati SSL

È oramai risaputo l'alto rischio associato all'invio di informazioni a un sito Web non sicuro. Per sopravvivere in questo mercato le aziende con attività di commercio elettronico devono incorporare sui loro siti i certificati SSL e la tecnologia di crittografia da essi implementata.

La crittografia è un processo che trasforma le informazioni in modo da renderle incomprensibili a tutti eccetto il destinatario designato ed è fondamentale per garantire l'integrità dei dati e la privacy necessarie per le transazioni commerciali elettroniche. Clienti e partner commerciali inviano informazioni riservate ed effettuano transazioni su un sito Web solo se sono convinti che le informazioni riservate vengano protette. Le aziende che desiderano seriamente svolgere attività di commercio elettronico devono quindi implementare un'infrastruttura affidabile basata sulla tecnologia di crittografia.

SSL (Secure Sockets Layer), lo standard di sicurezza per il Web, è la tecnologia utilizzata per crittografare e proteggere le informazioni trasmesse sul Web mediante l'onnipresente protocollo HTTP. Durante il trasferimento, SSL protegge i dati che potrebbero altrimenti venire intercettati e alterati se fossero trasmessi senza essere crittografati. La maggior parte dei sistemi operativi, browser Web, applicazioni Internet e hardware server supporta SSL.



Un certificato SSL è un file elettronico che identifica in modo univoco persone e siti Web e consente l'esecuzione di comunicazioni crittografate. I certificati SSL vengono utilizzati come credenziali o come un passaporto digitale. In genere il firmatario di un certificato SSL è un'autorità di certificazione (CA). Con oltre un miliardo di server Web protetti in tutto il mondo, VeriSign è di gran lunga la principale autorità di certificazione.²

Nello schema a sinistra è illustrato il processo che garantisce la protezione delle comunicazioni tra un server Web e un client. Tutti gli scambi di certificati SSL vengono effettuati in pochi secondi e non richiedono alcun intervento da parte dell'utente.

² Include consociate, affiliate e rivenditori di VeriSign.

Livelli di crittografia e SGC

Sono disponibili vari livelli di complessità di crittografia, a seconda del numero di bit utilizzati nell'algoritmo di crittografia. Lo standard attuale è 128 bit, che è considerato appropriato per qualsiasi uso e scopo, in quanto non può essere compromesso con la capacità di elaborazione corrente dei computer. Versioni precedenti di alcuni sistemi operativi e browser, in determinate combinazioni, tra cui molti sistemi Windows 2000, non supportano una crittografia superiore a 40 o 56 bit. Poiché oggi è facile compromettere questi livelli di crittografia, gli utenti di queste combinazioni di sistemi operativi e browser risultano vulnerabili.

La tecnologia SGC (Server-Gated Cryptography), disponibile con certi certificati SSL di VeriSign, risolve questo problema per il 99,9% dei visitatori dei siti Web (alcune versioni obsolete di browser non supportano la crittografia a 128 bit indipendentemente dal certificato SSL utilizzato). Poiché i siti Web che utilizzano SGC utilizzano la crittografia a 128 bit per le comunicazioni con sistemi che in genere supportano solo la crittografia a 40 o 56 bit, le aziende che adottano i certificati SSL SGC possono garantire il livello di crittografia più elevato a tutti i clienti. Secure Site Pro e Secure Site Pro con EV di VeriSign supportano la crittografia a 128 bit SGC. Tutti i certificati SSL di VeriSign supportano la crittografia fino a 256 bit su tutte le connessioni, purché sia il client che il server supportino la crittografia a questo livello.

Livelli di autenticazione e affidabilità

Uno degli scopi principali dei certificati SSL è garantire ai consumatori che stanno effettivamente effettuando transazioni commerciali con il sito Web a cui intendono accedere. Per questo motivo le autorità di certificazione effettuano dei controlli di convalida prima di emettere i certificati. Esistono tre categorie di autenticazione SSL normalmente riconosciute: autenticazione del dominio, autenticazione dell'organizzazione ed EV. Le differenze nel livello di sicurezza fornito e nell'affidabilità associata sono di vitale importanza. Poiché gli specifici processi di autenticazione variano addirittura all'interno del livello a seconda dell'autorità di certificazione, è particolarmente importante scegliere un'autorità di certificazione nota, rispettata e affidabile. Nessun'altra autorità di certificazione è più affidabile o rinomata di VeriSign.

Autenticazione del dominio

I certificati con autenticazione del dominio sono quelli meno sicuri. L'autorità di certificazione infatti verifica che l'entità che richiede il certificato di autenticazione del dominio sia la proprietaria del dominio in questione o abbia diritto ad utilizzare il nome del dominio. L'autorità di certificazione potrebbe inoltre verificare che l'indirizzo di posta elettronica del contatto che richiede il certificato sia incluso nell'elenco WHOIS o soddisfi i requisiti di alias di posta elettronica stabiliti dall'autorità di certificazione. VeriSign non offre certificati SSL con autenticazione del dominio.

Autenticazione dell'organizzazione

L'autenticazione dell'organizzazione consiste nel processo di convalida effettuato da VeriSign e altre autorità di certificazione per i certificati SSL standard, ossia non EV. L'autorità di certificazione verifica l'esistenza dell'organizzazione cercando le credenziali emesse da enti governativi, in genere all'interno di database privati e pubblici. In alcuni casi possono essere richiesti documenti quali statuto societario, licenza o registrazione di nomi commerciali. Prima di emettere un certificato SSL, l'autorità di certificazione verifica l'identità della società e conferma che si tratta di un'entità legale, conferma che la società dispone del diritto a utilizzare il nome del dominio incluso nel certificato e verifica che la persona che ha richiesto il certificato SSL per conto della società sia stata autorizzata a tale fine.

Autenticazione EV

La tecnologia EV, che verrà descritta nella sezione successiva, garantisce il livello di autenticazione più elevato offerto dai certificati SSL. L'autenticazione EV fornisce una maggiore struttura e aggiunge ulteriori controlli al processo di autenticazione dell'organizzazione. Questo processo inizia con una verifica approfondita dell'autenticità dell'entità, a partire da una conferma firmata dal contatto aziendale che approva tale processo. Se l'autorità di certificazione non è in grado di confermare i dati dell'organizzazione accedendo ai database pubblici, potrebbe inoltre venire richiesto un documento che comprovi la registrazione della società. Talvolta potrebbe venire richiesta una lettera con valore legale che confermi le seguenti informazioni sull'organizzazione:

- Indirizzo fisico della sede operativa
- Numero di telefono
- Conferma del diritto esclusivo a utilizzare il dominio
- Conferma aggiuntiva dell'esistenza dell'organizzazione (se fondata da meno di 3 anni)
- Verifica dell'appartenenza del contatto aziendale all'organico

Questo processo non risulta oneroso per le organizzazioni legittime, ma rappresenta un ostacolo significativo per i malfattori.

Marchio di fiducia

Per guadagnare credibilità e massimizzare le attività online, è necessario non solo proteggere le trasmissioni online dei clienti, ma anche informare l'utente dell'implementazione di questo processo. Per questo motivo le autorità di certificazione mettono a disposizione simboli del loro marchio di fiducia che è possibile pubblicare sulle pagine del sito Web. Il simbolo VeriSign Secured® Seal, illustrato di seguito, è il simbolo di sicurezza più diffuso e riconosciuto al mondo. La selezione del simbolo visualizza una finestra contenente il nome del proprietario del certificato, il periodo di validità e informazioni sul livello di protezione fornito e sul processo di convalida a cui VeriSign ha sottoposto il proprietario prima di emettere il certificato. La ricerca condotta da TNS riporta inoltre un 70% di abbandoni delle transazioni online per incertezza in relazione alla sicurezza dei siti. Il 90% di queste transazioni sarebbe stato portato a termine positivamente con la presenza del simbolo VeriSign Secured® Seal.³



³ Ricerca TNS, agosto 2006

+ EV: il nuovo standard di affidabilità

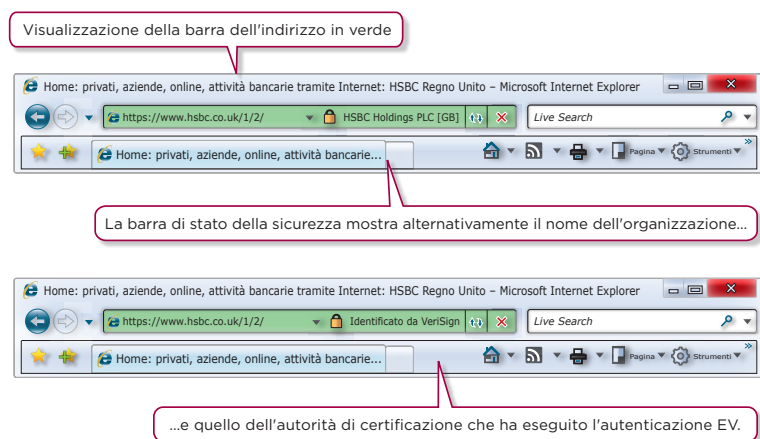
In passato indicatori della presenza di una sessione SSL, quali il prefisso https nell'URL o l'icona del lucchetto dorato, erano sufficienti per placare i timori della maggior parte dei consumatori, in quanto garantiscono la protezione della trasmissione dei dati riservati mediante livelli di crittografia adeguati. Oggigiorno però anche l'algoritmo di crittografia più avanzato non è più sufficiente a causa di un problema ben diverso. I ladri cibernetici hanno affinato le loro tecniche inducendo il cliente a credere che si tratti di attività legittime. Essi acquistano infatti certificati SSL, che sfortunatamente sono facilmente ottenibili da autorità di certificazione che eseguono verifiche superficiali, e li utilizzano per indurre i clienti a inviare dati riservati. Per questo motivo la crittografia non è più sufficiente, in quanto non offre alcuna protezione nel caso in cui il destinatario della trasmissione crittografata sia un'attività illegittima che ha intenzione di utilizzare i dati forniti a scopo di personificazione o altra forma di attività illecita. Il problema per gli utenti è quindi riconoscere se un sito Web che non hanno mai visitato sia legittimo o, addirittura, discernere se un'attività online nota e affidabile non sia in realtà stata duplicata da un impostore molto furbo a scopo di truffa. Il 90% degli utenti non sono in grado di distinguere i siti di phishing da quelli legittimi.⁴

Per guadagnarsi la fiducia dei clienti, è necessario disporre di un metodo semplice e affidabile in grado di dimostrare che le transazioni non solo sono sicure, ma che si tratta di un'attività legittima e non di un'entità che si presenta sotto false spoglie. Per soddisfare queste esigenze, i fornitori di soluzioni di sicurezza e di browser Internet hanno collaborato per definire lo standard EV, la più grande novità nel settore della sicurezza del commercio elettronico negli ultimi dieci anni. VeriSign supporta questo standard nei certificati SSL EV.

Quando un cliente che utilizza un browser che supporta EV visita una pagina Web protetta mediante un certificato SSL EV, la barra dell'indirizzo viene visualizzata in verde. Le versioni correnti e future di Microsoft Internet Explorer (a partire da Internet Explorer 7), Firefox (a partire da Firefox 3) e Opera (a partire da Opera 9.5) supportano questa funzionalità. Al momento il 50% dei browser, inclusi quelli sopra elencati, supporta lo standard EV.⁵

Oltre a visualizzare la barra in verde, il browser visualizza il nome dell'organizzazione riportato nel certificato. I dettagli di implementazione variano a seconda del browser. IE7, ad esempio, visualizza il nome del fornitore di soluzioni di sicurezza che ha emesso il certificato, ad esempio VeriSign, oltre a quello dell'organizzazione, alternandoli come illustrato di seguito.

Figura 2: visualizzazione della barra dell'indirizzo in verde ed EV



⁴ Rachna Dhamija, università di Harvard; J.D. Tygar e Marti Hearst, UC Berkeley

⁵ Net Applications, MarketShare Report, agosto 2008

I certificati SSL Secure Site Pro con EV di VeriSign offrono il livello di crittografia SSL più elevato a tutti i visitatori e garantiscono la più alta affidabilità. Mediante i certificati SSL Secure Site Pro con EV di VeriSign è possibile garantire la massima sicurezza ai propri clienti del sito Web e ai partner commerciali, indipendentemente dal sistema operativo o dal browser che utilizzano. Secure Site Pro con EV di VeriSign consente alle aziende di guadagnarsi la fiducia di cui hanno bisogno per espandere la loro attività di commercio elettronico.

Il browser e il fornitore di sicurezza controllano la visualizzazione per evitare che altre persone effettuino il phishing dei dati dei clienti o contraffacciano il marchio dell'organizzazione. Oggigiorno i truffatori possono imitare praticamente qualsiasi parte di un sito Web, ma se non dispongono del certificato SSL EV della società legittima, non possono in nessun modo visualizzarne il nome nella barra dell'indirizzo, perché la visualizzazione di queste informazioni non è sotto il loro controllo. Inoltre non possono ottenere il certificato SSL EV della società legittima a causa del rigoroso processo di autenticazione.

Quali sono i motivi per i quali EV offre rassicurazione al consumatore?

- I clienti online possono vedere il nome del proprietario del certificato sulla barra dell'indirizzo che garantisce che il sito è veramente gestito dall'organizzazione legittima e non da un impostore.
- Le autorità di certificazione portano a termine diversi livelli di verifica della legittimità e autenticità delle organizzazioni prima di emettere i certificati EV, come precedentemente descritto, per impedire che dei truffatori pretendano di essere attività commerciali legittime su Internet.
- Le autorità di certificazione stesse devono soddisfare criteri molto severi per potere emettere certificati SSL EV e vengono regolarmente sottoposte a controlli WebTrust di terze parti che ne verificano la conformità ai requisiti definiti negli standard del CA/Browser Forum, un consorzio di autorità di certificazione e fornitori di browser. In questo modo si evita che un'autorità di certificazione esegua controlli troppo superficiali che potrebbero consentire a un impostore di ottenere il riconoscimento EV. EV garantisce quindi ai clienti che l'organizzazione è stata sottoposta a tutti i controlli necessari.
- Il colore verde sembra avere un effetto psicologico calmante sui clienti. Infatti, anche i clienti che non conoscono i veri motivi per cui EV è sinonimo di migliore protezione, tendono ad effettuare acquisti e a spendere cifre più elevate se vedono la barra verde.

Il successo di EV è strepitoso. In base a una ricerca condotta da Tec-Ed nel gennaio 2007 sulle modalità di utilizzo e l'atteggiamento di 384 acquirenti online, risulta che:

- il 100% dei partecipanti nota se un sito mostra la barra verde EV;
- il 93% dei partecipanti preferisce effettuare acquisti su siti che mostrano la barra verde;
- il 97% dei partecipanti sono propensi a condividere i dati della carta di credito con siti che mostrano la barra verde, mentre solo il 63% fornirebbero tali dati su siti senza certificazione EV;
- il 77% dei partecipanti hanno dichiarato che esiterebbero ad effettuare acquisti presso un sito che in passato mostrava la barra verde EV ma su cui adesso non è più presente.

Dallo stesso studio di Tec-Ed risulta che l'88% dei partecipanti ha fiducia nel marchio VeriSign, mentre solo il 22% dei partecipanti si fida del successivo fornitore SSL più noto.

Ricerche di mercato come questa dissolvono ogni possibile dubbio sul valore e sull'importanza della certificazione EV e sul livello di riconoscimento, fiducia e apprezzamento di cui gode il marchio VeriSign. Quanto finora indicato si traduce inoltre in un incremento delle vendite, come è stato ampiamente dimostrato. Numerosi detentori di certificati SSL EV di VeriSign hanno effettuato degli studi per valutare come la visualizzazione della barra verde abbia influenzato il tasso di conversione delle vendite online. All'agosto 2008 14 clienti riportavano un aumento significativo delle vendite e da allora abbiamo continuato a ricevere simili risultati. Overstock.com, ad esempio, ha ottenuto una riduzione dell'8,6% del numero di acquirenti che escono dal carrello della spesa tra quelli che vedono la barra verde. Altri clienti hanno ottenuto miglioramenti ancora più significativi. Per informazioni dettagliate (in inglese) visitare il sito all'indirizzo www.Verisign.co.uk/success-stories/index.html.

I CONSUMATORI CONSIDERANO VERISIGN IL MARCHIO "NUMERO 1" QUANDO SI TRATTA DI SICUREZZA DI SITI WEB.

Il simbolo VeriSign Secured Seal incluso con tutti i certificati SSL di VeriSign consente di esporre sul proprio sito Web il marchio sinonimo di fiducia su Internet. È significativo che il 78% degli acquirenti online nel Regno Unito si accerti che siano presenti indicazioni visive, ad esempio il simbolo VeriSign Secured Seal, prima di completare una transazione. Il simbolo VeriSign Secured Seal consente ai visitatori di verificare le informazioni e lo stato del certificato SSL in tempo reale, aumentando la fiducia da loro riposta nella sicurezza delle transazioni elettroniche.

+ Certificati SSL di VeriSign per la massima sicurezza e affidabilità

VeriSign è il principale fornitore globale di certificati SSL. VeriSign è anche di gran lunga il principale fornitore di certificati SSL EV, con una quota di mercato del 75%, e include tra i clienti le più grandi aziende che operano nel settore del commercio elettronico e bancario.⁶ I primi 40 istituti bancari e oltre il 95% delle società che figurano nell'elenco Fortune 500 hanno scelto i certificati SSL di VeriSign⁷ e oltre 90.000 domini in 145 paesi visualizzano il simbolo VeriSign Secured Seal, il marchio di fiducia più riconosciuto su Internet. Gli utenti sono abituati a vedere il simbolo VeriSign Secured® Seal posizionato ben in evidenza sui siti Web che offrono commercio elettronico come segno di garanzia che l'attività è legittima e che il sito è in grado di proteggere le informazioni riservate degli utenti online mediante la crittografia SSL.

Per soddisfare tutte le esigenze, VeriSign offre quattro principali tipi di soluzioni SSL.

Secure Site di VeriSign

La soluzione più semplice di VeriSign include:

- Autenticazione dell'organizzazione
- Crittografia minima di 40 bit, fino a 256 bit
- Diritto a visualizzare il simbolo VeriSign Secured Seal
- Garanzia di 100.000 dollari
- Verifica dell'installazione

Secure Site Pro di VeriSign

Secure Site Pro di VeriSign® mette a disposizione il livello di crittografia più elevato a ogni visitatore del sito. Questa soluzione include tutti i servizi disponibili in Secure Site di VeriSign più la crittografia SGC, che garantisce la crittografia a 128 bit al 99,9% degli utenti Internet, e una garanzia di 250.000 dollari.

Secure Site con EV di VeriSign

Questa soluzione include tutti i servizi disponibili in Secure Site di VeriSign più EV. SSL EV offre ai visitatori dei siti Web un metodo semplice e affidabile per determinare la legittimità delle attività online. Infatti solo i certificati SSL con EV causano, nei browser Web con funzionalità di protezione avanzate, la visualizzazione della barra dell'indirizzo in verde contenente il nome dell'organizzazione proprietaria del certificato SSL e il nome dell'autorità di certificazione che lo ha emesso.

Secure Site Pro con EV di VeriSign

Secure Site Pro con EV di VeriSign rappresenta la migliore soluzione SSL per proteggere le trasmissioni riservate verso e da siti Web, per evitare che vengano lette o modificate da persone diverse da quelle tra cui avviene la comunicazione e per promuovere la fiducia dei clienti. Questa soluzione contiene tutte le tecnologie disponibili in altre soluzioni, inclusa la crittografia SGC e i certificati SSL EV, nonché una garanzia di 250.000 dollari.

VeriSign consiglia i certificati SSL Secure Site Pro con EV come migliore soluzione di crittografia e per la massima affidabilità. Questa soluzione causa la visualizzazione della barra verde EV in browser con funzionalità di protezione avanzate e consente a tutti i visitatori di connettersi utilizzando il livello di crittografia più alto possibile.

⁶ Netcraft, agosto 2008

⁷ Include consociate, affiliate e rivenditori di VeriSign.

VeriSign può aiutare le aziende a creare o aumentare la fiducia dei clienti proteggendo il sito Web dove si svolgono le attività commerciali. I certificati SSL di VeriSign proteggono lo scambio di informazioni tra i client e i server Web, tra i server e anche tra altri dispositivi di rete, come dispositivi per il bilanciamento del carico dei server o acceleratori SSL. Le soluzioni di VeriSign sono in grado di offrire la protezione completa su tutta la rete proteggendo i server che si interfacciano sia con Internet che con intranet private.



DOCUMENTO TECNICO

+ Conclusioni

Con l'aumentare del numero di frodi su Internet, la sicurezza delle trasmissioni di dati personali non è mai stata così importante e in futuro la situazione peggiorerà sicuramente. La diffusione, e le relative conseguenze, dei furti di identità sono fin troppo note e documentate. I potenziali clienti online sono molto più informati, scettici e, francamente, spaventati. I clienti vogliono essere protetti e al momento l'84% di essi ritengono che i siti Web non offrano la sicurezza necessaria.⁸

La fiducia è ciò che fa la differenza. Gli investimenti in tecnologie volte a proteggere i clienti e guadagnarne la fiducia sono irrisorie rispetto ai costi operativi totali e possono apportare un ritorno astronomico incrementando le vendite, nel caso di un cliente di VeriSign sino al 48.000% (questo caso di studio è disponibile, insieme a molti altri, sul sito di VeriSign).

In considerazione delle esorbitanti possibilità di guadagno e dei costi minimi, la scelta è ovvia: il nome più noto e affidabile, in quanto il riconoscimento del marchio e la fiducia sono esattamente TUTTO ciò che un fornitore SSL deve offrire. Il marchio VeriSign ha ottenuto un così alto riconoscimento e gode di molta fiducia perché garantisce la sicurezza e i clienti ne sono consapevoli. In definitiva, non ha senso scegliere mezze misure, quando con i certificati SSL Secure Site Pro con EV di VeriSign è possibile garantire che le informazioni riservate di TUTTI i clienti vengano trasmesse senza compromessi e che la destinazione sia veramente quella desiderata.

+ Ulteriori informazioni

VeriSign offre un'ampia gamma di servizi aggiuntivi per siti di commercio elettronico descritti sul sito www.Verisign.it in grado di soddisfare qualsiasi esigenza delle attività online. Per discutere con un esperto di VeriSign delle esigenze di sicurezza del sito Web della propria società, telefonare al numero gratuito 800-923-008 o al numero +39 0 269 430 579. È inoltre possibile contattare VeriSign tramite posta elettronica all'indirizzo vendite@Verisign.it.

+ Prova gratuita di un certificato SSL di VeriSign

È possibile proteggere il proprio sito Web per un periodo di prova gratuita della durata di due settimane. Per richiedere la prova gratuita di un certificato SSL Secure Site di VeriSign, visitare il sito all'indirizzo www.Verisign.co.uk/trial (in inglese). È possibile completare l'intero processo di registrazione online in circa 15 minuti e iniziare immediatamente a utilizzare il certificato di prova SSL di VeriSign.

+ Informazioni su VeriSign

VeriSign è il fornitore di servizi di infrastruttura Internet più affidabile per il mondo digitale. Miliardi di volte al giorno aziende e consumatori si affidano alla nostra infrastruttura Internet per comunicare e completare transazioni commerciali in piena tranquillità.

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

⁸ YouGov, gennaio 2008