



DOCUMENTO TECNICO

---

Come rafforzare la fiducia dei visitatori  
del sito tramite i certificati SSL  
Extended Validation





**SOMMARIO**

+ L'erosione della garanzia di identità	3
+ Certificazione di identità affidabile	4
Internet Explorer 7: Verde per il "via libera"	4
+ Come funziona l'architettura Extended Validation	7
+ EV Upgrader estende la protezione ai client Windows XP	8



Le aziende operanti sul Web stanno sperimentando una crisi di fiducia da parte degli acquirenti. Si registra un calo della fiducia nella sicurezza dei siti e un numero sempre crescente di consumatori tende a ridurre le transazioni online, se non addirittura a evitarle. Da una ricerca condotta l'8 dicembre 2005 da Forrester Research è emerso che un sorprendente 24% degli utenti di Internet ha dichiarato che non avrebbe effettuato transazioni online durante le festività natalizie a causa della sensazione di scarsa sicurezza. Addirittura il 61% ha dichiarato di aver almeno ridotto gli acquisti online per la stessa ragione. Se da un lato questo fenomeno è stato mascherato dall'aumento complessivo delle attività online (quali, ad esempio, operazioni bancarie, trading e versamento delle imposte), di fatto le aziende che si occupano di vendita online ottengono per la maggior parte risultati inferiori, anche dal punto di vista economico, a quelli che potrebbero ottenere.

A partire dai primi mesi del 2007 le aziende che operano online hanno l'opportunità di dimostrare ai clienti la propria identità al di là di ogni dubbio e i clienti possono verificarla prima di concludere transazioni di acquisto sui siti. Questa opportunità è il risultato del maggiore sviluppo nel campo della sicurezza sul Web compiuto negli ultimi 10 anni: l'introduzione di un nuovo tipo di certificato SSL, il primo dalla nascita della tecnologia oltre un decennio fa.

Si tratta del certificato SSL Extended Validation (EV), il frutto di oltre un anno di lavoro del CA/Browser Forum, un consorzio del quale fanno parte i maggiori produttori di browser Web e le principali autorità di certificazione SSL come VeriSign. Dai primi mesi del 2006 i membri del CA/Browser Forum hanno reso disponibili questi nuovi certificati, di grande utilità tanto per le aziende operanti sul Web quanto per i visitatori dei siti. I certificati possono aumentare la propensione a concludere transazioni commerciali online in tutte le forme rafforzando la fiducia dei visitatori nella legittimità dei siti e riducendo in modo consistente l'efficacia degli attacchi di phishing.

## L'erosione della garanzia di identità

Immaginiamo di chiedere all'acquirente online tipico cosa significhi il piccolo simbolo del lucchetto visualizzato nel browser Internet: con ogni probabilità la risposta sarà che le trasmissioni sono crittografate e pertanto protette da occhi indiscreti. Pur essendo tecnicamente corretta, quest'affermazione non comprende tutti i significati che i pionieri dell'e-commerce intendevano attribuire al piccolo simbolo.

L'obiettivo originario dei certificati SSL era convalidare l'identità di un sito nel momento in cui un utente vi si collegava. Tale convalida è un'esigenza: se è difficile imitare fisicamente l'identità di un'azienda, è tuttavia alquanto semplice imitarla online. Fu proprio questo principio, compreso dagli operatori del settore già nel lontano 1995, a portare alla creazione dei certificati SSL. Nelle intenzioni dei suoi creatori, il certificato avrebbe dovuto certificare l'identità del sito, proteggendo quindi gli acquirenti online dalle truffe. Agli inizi era sufficiente la garanzia di identità fornita da un certificato SSL standard. Oggi, però, non lo è più. L'uso diffuso del Web da parte di utenti profani senza particolari competenze in campo informatico, in combinazione con la scarsa visibilità del simbolo del lucchetto nei browser più comunemente utilizzati, ha consentito al phishing di diventare il fenomeno che si registra oggi.

Nonostante le intenzioni iniziali, i certificati SSL di tipo tradizionale non sono la soluzione. Alcune autorità di certificazione riescono con successo ad autenticare l'identità, altre però fanno molto poco oppure utilizzano pratiche che possono essere facilmente aggirate. Un sito può addirittura generare un certificato SSL con firma senza alcuna autenticazione. Nella seconda metà del 2005 gli utenti online iniziarono a registrare attacchi di phishing su larga scala che utilizzavano certificati SSL "soft target" a basso livello di autenticazione, al fine di alimentare l'illusione della legittimità.

## Certificazione di identità affidabile

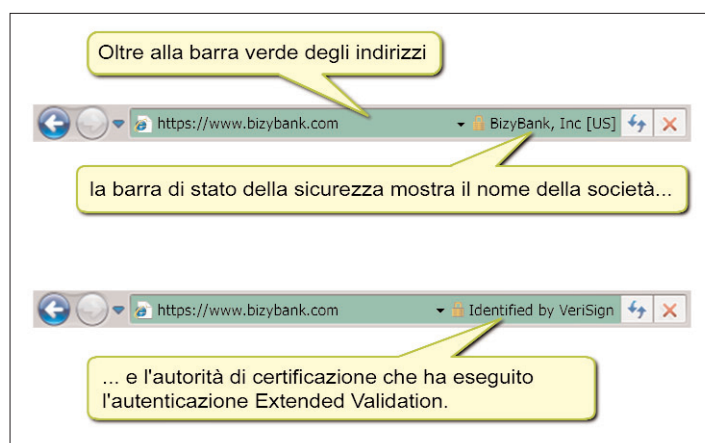
Per far sì che i certificati SSL potessero imporre la propria autorità come fonte di informazioni di identità dei siti per i visitatori, le aziende leader del settore dovevano risolvere due punti deboli del sistema esistente. In primo luogo, si avvertiva l'esigenza di una nuova categoria di certificati SSL in grado di fornire un certo livello di garanzia in merito all'identità del proprietario del sito. In secondo luogo, era necessario creare un'interfaccia browser che consentisse agli utenti di distinguere immediatamente un'identità nota da una sconosciuta. Vennero così introdotti i nuovi certificati SSL EV precedentemente menzionati. Alcuni utenti si riferiscono ad essi anche utilizzando il nome di lavoro: certificati SSL High Assurance (HA); si tratta di certificati differenti da quelli High Assurance generici, che non implicano lo stato EV.

Il CA/Browser Forum, composto di oltre 20 tra i maggiori produttori di browser Web, fornitori di certificati SSL e auditor di WebTrust, ha lavorato per oltre un anno in collaborazione con l'Information Security Committee dell'American Bar Association per creare un processo di autenticazione standardizzato che deve essere seguito dalle autorità di certificazione che intendano rilasciare certificati EV. Tali autorità di certificazione devono sottoporsi a verifiche indipendenti che attestino la conformità con il processo specificato. Il CA/Browser Forum sviluppò questo processo sulla base delle pratiche di verifica aziendale esistenti che erano state utilizzate diffusamente con successo per anni con l'autenticazione di milioni di certificati SSL.

Una volta completata l'autenticazione in base a questo processo, l'autorità di certificazione può rilasciare un certificato con stato EV. Tale certificato funziona esattamente come un certificato SSL di tipo tradizionale, infatti i browser non in grado di riconoscere automaticamente i certificati EV (es. Windows Internet Explorer e Mozilla Firefox 2.0 e versioni precedenti) si comportano esattamente come farebbero con un certificato non EV. Tuttavia nei nuovi browser EV compatibili i certificati vengono visualizzati in modo molto più evidente e con maggiori informazioni. Il primo di questi browser è Internet Explorer 7 (IE7).

### + Internet Explorer 7: Verde per il "via libera"

Con IE7 vengono introdotte diverse convenzioni di interfaccia che consentono di migliorare l'identificazione della proprietà di un sito. La più evidente è la "barra verde degli indirizzi": quando un browser IE7 accede ad una pagina con un certificato EV valido, lo sfondo della barra degli indirizzi diventa verde. Questo semplice cambiamento nell'interfaccia indica in modo molto visibile che il sito ha superato un alto livello di autenticazione dell'identità. Anche la scelta del colore utilizza convenzioni di interfaccia consolidate: il colore verde infatti viene associato al "via libera", proprio come il rosso rappresenta.



Alcune ricerche condotte presso gli utenti indicano che queste convenzioni interfaccia risultano estremamente efficaci. Nell'autunno del 2006 VeriSign ha condotto una ricerca sull'utilizzo e sulle attitudini degli acquirenti online negli Stati Uniti. Ecco alcune delle conclusioni rilevate da VeriSign:

- Il 100% dei partecipanti ha notato la presenza o meno su un sito della barra verde degli indirizzi dell'Extended Validation.
- Il 100% dei partecipanti era più propenso a fornire i dati della carta di credito nei siti sui quali era visualizzata la barra verde degli indirizzi.
- Il 98% dei partecipanti ha espresso la preferenza ad effettuare acquisti presso i siti sui quali è visualizzata la barra verde degli indirizzi dell'Extended Validation.
- L'80% dei partecipanti ha dichiarato che avrebbe esitato ad effettuare acquisti presso un sito sul quale non è più disponibile la barra verde degli indirizzi dell'Extended Validation precedentemente visualizzata.

IE7 contiene inoltre un campo aggiuntivo a destra della barra degli indirizzi denominato "barra di stato della sicurezza". Questo campo viene visualizzato quando il browser è in grado di offrire informazioni che potrebbero risultare utili ai visitatori del sito per valutarne l'affidabilità. Se una pagina contiene certificati SSL EV, nella barra di stato della sicurezza viene visualizzato il nome dell'organizzazione. Questa stringa di testo viene estratta direttamente dal certificato, dove è stata inserita dall'autorità di certificazione. Dal momento che l'autorità di certificazione ha verificato questo nome che viene anche visualizzato nell'interfaccia del browser, il visitatore può fidarsi dell'accuratezza di tale stringa.

Poniamo l'esempio di un'ipotetica banca online chiamata BizyBank: il nome dell'istituto viene visualizzato direttamente nell'interfaccia del browser. Gli utenti finali possono verificare l'identità del sito cercando la barra verde degli indirizzi e il nome BizyBank, che insieme rappresentano un nuovo e significativo ostacolo per i phisher che vogliono impadronirsi dei conti BizyBank. Per poter sferrare un attacco di phishing oggi è sufficiente duplicare il sito originale e trovare un URL convincente. Se i clienti di BizyBank imparano a cercare il nome della società e la barra del indirizzi verde prima di fornire informazioni riservate, gli autori di potenziali attacchi di phishing non saranno in grado di imitare quest'interfaccia. Se anche i phisher si servissero di un'azienda esistente per acquistare certificati EV per il proprio sito di phishing, l'interfaccia del browser non conterrebbe comunque il nome BizyBank.

Nella barra di stato della sicurezza viene visualizzato anche il nome dell'autorità di certificazione che ha rilasciato l'autenticazione, consentendo ai clienti di valutare la sicurezza utilizzata dai siti prima di decidere di effettuare transazioni. Se i visitatori del sito non si fidano dello specifico fornitore di certificati SSL, possono scegliere di fare i propri acquisti altrove. Analogamente, se un'autorità di certificazione rilascia certificati EV non validi, il pubblico imparerà a non fidarsi dei siti che utilizzano certificati SSL con questo marchio.

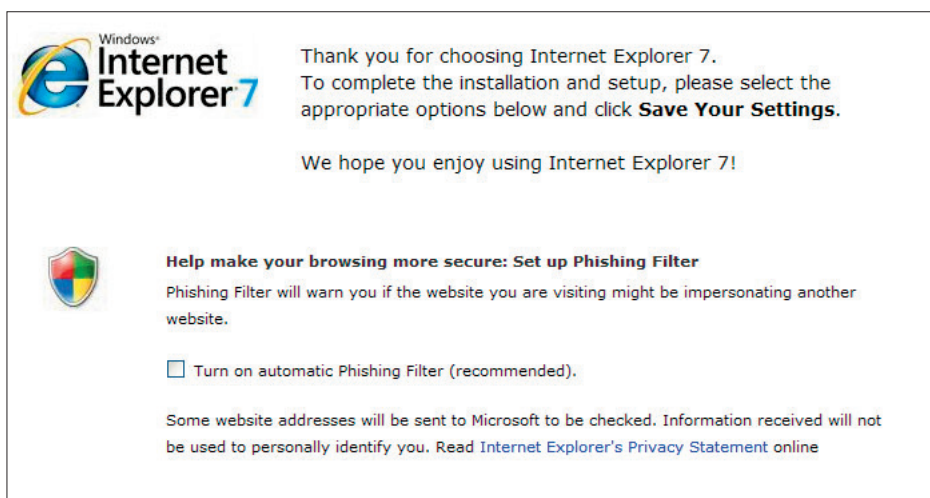
Alcune ricerche hanno dimostrato che la scelta del marchio del certificato SSL può influire sulla propensione del visitatore di un sito a effettuare transazioni. Ad esempio Opodo, società leader in Europa nel settore viaggi, ha testato un set di pagine di ordinazione online identiche con e senza il simbolo VeriSign Secured Seal: sulle pagine che riportavano il simbolo sono state concluse vendite superiori del 10% rispetto alle pagine che non presentavano simbolo. "Abbiamo immediatamente compreso l'impatto del fattore fiducia sulla percentuale di abbandono durante le transazioni di acquisto e da allora abbiamo inserito il simbolo VeriSign Seal sulle pagine dei pagamenti sull'intera rete dei nostri siti europei", ha detto Warren Jonas, responsabile della gestione servizi di Opodo.

Nell'estate del 2006 TNS, la nota azienda di ricerche di mercato, ha analizzato le reazioni degli acquirenti online ad una serie di sigilli di sicurezza online, giungendo alla conclusione che il simbolo VeriSign Secured Seal è di gran lunga il marchio di affidabilità online più riconosciuto al mondo. Dalla ricerca è infatti emerso che il simbolo VeriSign Secured Seal viene riconosciuto dal 56% degli acquirenti online a livello mondiale, una percentuale 8 volte superiore al marchio di certificati SSL che occupa la posizione immediatamente successiva.

Questi risultati sottolineano l'importanza del marchio di sicurezza dei certificati SSL che i venditori online scelgono di pubblicare sui propri siti: scegliendo di visualizzare il marchio di sicurezza più conosciuto sul Web è quindi possibile incrementare il numero di transazioni (e di conseguenza le potenzialità complessive di un sito di e-commerce) del 10% o anche più.

Alcune impostazioni in IE7 possono influire sulla visualizzazione di queste convenzioni di interfaccia. In particolare, è necessario abilitare la funzione Protocollo di stato del certificato in linea (OCSP) affinché vengano visualizzate tali caratteristiche. Il protocollo OCSP consente al browser di verificare i certificati SSL in tempo reale per garantire che non siano stati revocati. Il protocollo OCSP è supportato nella maggior parte delle versioni più recenti del browser, che offrono anche un controllo nell'interfaccia che consente la disattivazione di tale funzionalità. A causa dell'elevata garanzia di affidabilità offerta dai certificati EV, per la visualizzazione della barra verde degli indirizzi e di altre convenzioni di interfaccia EV per qualsiasi certificato EV il browser IE7 richiede l'abilitazione del protocollo OCSP. Ciò consente all'utente di sapere non solo che il sito ha superato un alto livello di autenticazione dell'identità, ma anche che successivamente non si sono verificati incidenti che abbiano comportato la revoca del certificato.

Oltre a consentirne l'abilitazione diretta, IE7 è in grado di abilitare automaticamente il protocollo OCSP quando l'utente attiva un'altra funzione del prodotto che richieda la funzionalità OCSP. Questa funzione, definita "filtro phishing", aggiunge alle funzionalità EV la visualizzazione di barre degli indirizzi di colore rosso o giallo sui siti che rispondono a determinate condizioni che comportano la classificazione come siti sospetti. IE7 consente (e raccomanda) di applicare questa funzione durante l'installazione. Insieme al filtro phishing viene abilitata anche l'interfaccia EV.



*Insieme al filtro phishing (la cui abilitazione è consigliata durante l'installazione), viene automaticamente abilitata anche la visualizzazione dei certificati SSL EV.*

Il sistema operativo Windows Vista si spinge ancora più avanti: in IE7 per Windows Vista, infatti, la funzionalità OCSP e il filtro phishing sono abilitati per impostazione predefinita e l'utente del browser deve attivamente disabilitarli se desidera impedirne il funzionamento.

È impossibile misurare su quale percentuale di sistemi client con IE7 la funzionalità OCSP sia abilitata. Considerando l'importanza per gli utenti finali della barra verde degli indirizzi e del filtro phishing, la visibilità di queste funzioni nell'interfaccia e la raccomandazione visualizzata nel corso dell'installazione di abilitare il filtro phishing, VeriSign ritiene che questa percentuale sia considerevolmente elevata. Gli amministratori dei siti che valutano i certificati SSL EV devono accertarsi che queste funzioni siano abilitate sui propri sistemi. La barra verde gli indirizzi non viene infatti visualizzata in un browser IE7 nel quale tali impostazioni siano disabilitate.

## Come funziona l'architettura Extended Validation

L'architettura EV è stata progettata per offrire informazioni attendibili sull'identità dei siti Web agli utenti finali in modo che questi possano decidere consapevolmente di quali siti fidarsi. Il raggiungimento di questo obiettivo ha richiesto la modifica di ogni componente dell'architettura di affidabilità del Web. Oltre alle nuove convenzioni di interfaccia molto intuitive, i certificati EV devono la loro affidabilità 1) alle modifiche delle procedure di autenticazione e 2) alle verifiche dei certificati in tempo reale.

- 1) Il primo passaggio è l'autenticazione. Il CA/Browser Forum ha dedicato oltre un anno a preparare con grande cura delle linee guida sull'autenticazione in grado di garantire risultati di autenticazione affidabili. Tali linee guida richiedono l'utilizzo da parte delle autorità di certificazione qualificate di informazioni primarie o autenticate, piuttosto che di informazioni fornite dalle stesse organizzazioni che richiedono il certificato. Utilizzano tecniche consolidate impiegate con successo per l'autenticazione di milioni di certificati in decenni di utilizzo. Questa procedura consente di verificare che tutte le informazioni contenute nel certificato siano corrette e che il richiedente abbia l'autorità di richiedere tale certificato per la propria organizzazione. Tali procedure di autenticazione sono disponibili al pubblico per la consultazione all'indirizzo [www.cabforum.org](http://www.cabforum.org). Ciascuna autorità di certificazione deve sottoporsi ogni anno a una verifica (eseguita da un'azienda di verifica WebTrust registrata) che attesti il rispetto delle linee guida EV.
- 2) Una volta rilasciato un certificato, il passaggio successivo è garantire che il certificato presentato al cliente rifletta in modo accurato le informazioni acquisite dall'autorità di certificazione e che i certificati siano effettivamente conformi allo standard di autenticazione EV come dichiarano. L'integrità del certificato è garantita perché ciascun certificato SSL contiene funzioni hash sicure e non funzionerà correttamente se manomesso in qualsiasi modo. L'infrastruttura EV garantisce lo stato di validità corrente del certificato tramite un controllo in tempo reale. Questo tipo di controllo dipende da due infrastrutture parallele: la prima è il protocollo OCSP, precedentemente menzionato; tale funzionalità OCSP esegue un controllo delle revocche in tempo reale in modo tale che un certificato EV compromesso o revocato per qualche altra ragione non venga visualizzato come valido sui browser EV compatibili.

Il secondo servizio in tempo reale è l'archivio dei root di Microsoft. Lo stato di certificato EV è indicato da un contrassegno di metadati molto semplice. Per impedire che un'autorità di certificazione senza scrupoli o incompetente possa rilasciare in modo non corretto certificati contrassegnati come EV pur non avendo superato la corretta autenticazione EV, il browser IE7 esegue un controllo in tempo reale nell'archivio dei root di Microsoft per verificare che lo specifico root SSL sia approvato per i certificati EV. Grazie a questo controllo, negli eventuali certificati contrassegnati come EV ma rilasciati da un'autorità di certificazione non approvata per il rilascio di certificati EV non sarebbero comunque visualizzate la barra degli indirizzi verde e le altre caratteristiche di interfaccia EV. Allo stesso modo, nel caso un'autorità di certificazione non superi la verifica annuale o rilasci ripetutamente certificati non corretti con il banner EV, Microsoft ha la facoltà di rimuovere lo specifico root dall'elenco dei root EV approvati contenuto nell'archivio dei root di Microsoft. Con questa operazione viene disabilitata la visualizzazione della barra verde degli indirizzi e degli altri elementi di interfaccia EV per tutti i certificati contenenti il root sospetto.

## EV Upgrader estende la protezione ai client Windows XP

Gli elementi di interfaccia EV vengono visualizzati automaticamente nei client Windows Vista che visitano un sito; per il browser IE7 su Windows XP, invece, è richiesto un aggiornamento del root SSL perché i certificati EV possano essere visualizzati correttamente. VeriSign ha creato la soluzione VeriSign EV Upgrader per consentire a tutti i browser IE7 di rilevare i certificati SSL EV e visualizzarli correttamente. EV Upgrader sfrutta le funzionalità di aggiornamento root esistenti del sistema operativo Windows per scaricare e aggiornare in modo automatico e invisibile il nuovo root EV sul sistema client. Per semplificare il più possibile l'uso di EV Upgrader da parte degli amministratori dei siti, VeriSign ha incorporato la soluzione direttamente nel simbolo VeriSign Secured Seal, ed è pertanto disponibile anche nel caso in cui il simbolo sia già stato installato sul sito.

Per una descrizione dettagliata di EV Upgrader e del suo funzionamento come parte del simbolo VeriSign Secured Seal, consultare il documento tecnico di VeriSign *Abilitazione dei client Windows XP per l'Extended Validation tramite EV Upgrader*. Per ulteriori informazioni sui certificati EV di VeriSign o per acquistarli per il proprio sito Web, visitare la pagina <http://www.verisign.it/ssl/index.html>.