# Certificati digitali: come navigare sicuri

La sicurezza sul Web è una delle preoccupazioni che maggiormente assilla (o dovrebbe assillare) gli utenti, soprattutto quando si effettuano operazioni delicate come pagamenti online o trasferimento di dati sensibili dal punto di vista della privacy.

Esistono diverse soluzioni tecniche per garantire un livello soddisfacente di sicurezza, ma è importante che l'utente sia a conoscenza dei principi generali che gli garantiscono questa sicurezza.

Probabilmente molti utenti hanno sentito parlare di **protocolli sicuri**, come **HTTPS** o **SSL**, del fatto che questi protocolli codifichino i dati in modo che non possano essere decodificati da altri se non dai diretti interessati. Spesso questo concetto viene associato al famoso lucchetto che deve comparire sul browser a garanzia della sicurezza delle transazioni. Ma tutto ciò è sufficiente? È sufficiente sapere che i dati viaggiano crittografati tra un server ed un browser?

Vediamo se c'è altro da sapere.

# Sicurezza e identità

La trasmissione sicura dei dati tra un server Web ed un browser è normalmente garantita da **algoritmi di crittografia** e da protocolli che adottano tali algoritmi. Senza entrare nei dettagli tecnici, possiamo dire che le più recenti tecniche di crittografia offrono una elevata garanzia che i dati trasmessi, anche se intercettati da un malintenzionato, difficilmente potranno essere decodificati.

Quindi, se inviamo il numero della nostra carta di credito ad un sito di commercio elettronico che ha attivato il protocollo sicuro HTTPS siamo abbastanza sicuri che difficilmente qualcun altro potrà intercettarlo.

Ma proviamo ad insinuare un dubbio. Proviamo a farci una domanda che probabilmente in pochi si pongono: siamo sicuri che il destinatario a cui abbiamo inviato i dati della nostra carta di credito sia effettivamente quello che crediamo che sia? E se si trattasse di qualcuno che ha clonato un sito molto noto per raggirare gli utenti e farsi inviare i dati delle loro carte di credito?

La **sola riservatezza del trasferimento dei dati** non è garanzia di sicurezza dell'identità del destinatario. È opportuno assicurarsi che chi riceve i nostri dati sia effettivamente il destinatario con cui vogliamo interagire. A questa esigenza cerca di dare una risposta la tecnologia dei certificati digitali.

# Identità di un sito Web

Quando ci colleghiamo ad un sito Web, quindi, abbiamo la necessità di sapere se effettivamente stiamo inviando i dati al destinatario corretto. L'identificazione del destinatario è garantita dai certificati digitali associati alle connessioni sicure SSL. Per inciso, il protocollo HTTPS non è altro che protocollo HTTP integrato con SSL per gli aspetti relativi alla sicurezza.

Un certificato digitale è un file contenente informazioni sulle modalità di crittografia adottate dal sito Web e sul sito che riceve tali informazioni. Naturalmente, perché il contenuto del certificato sia affidabile è necessario che questo venga emesso da un ente autorizzato e che non possa essere falsificato. Gli enti autorizzati all'emissione di certificati digitali sono chiamati Autorità di Certificazione e i certificati da essi rilasciati sono automaticamente riconosciuti dai browser. Tali enti, al momento del rilascio di un certificato al gestore di un sito Web, appongono una firma digitale al certificato stesso validando le

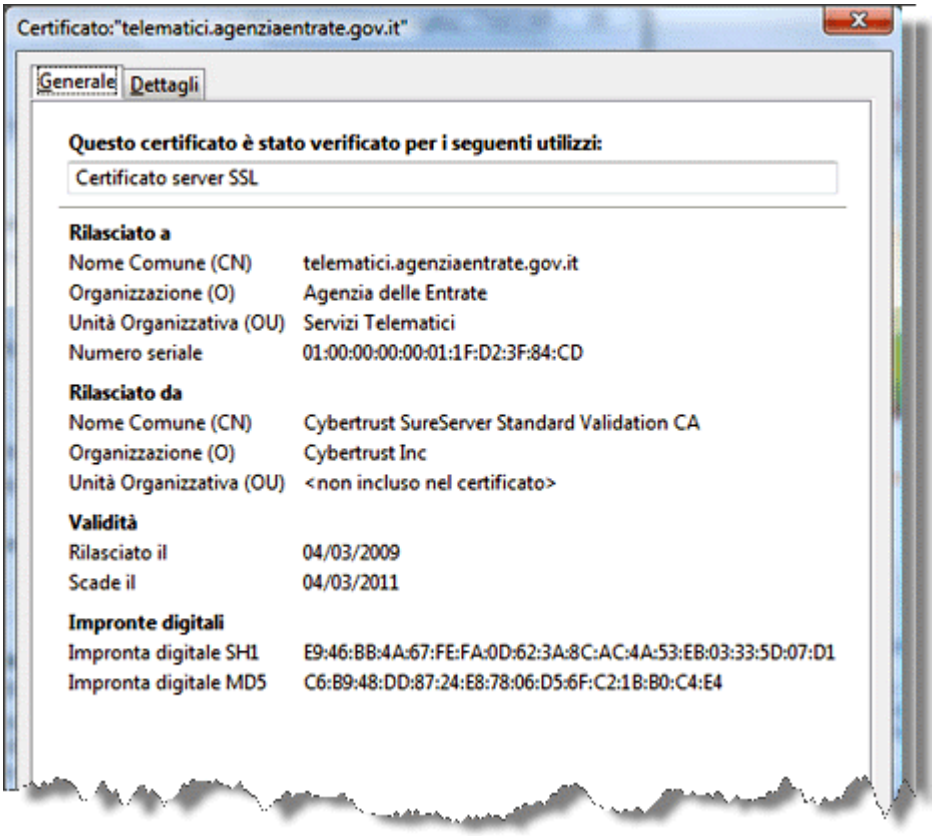
informazioni contenute in esso. Oltre a suggellare la validità delle informazioni contenute nel certificato, la firma dell'Autorità di certificazione garantisce che tali informazioni non possano essere modificate da terzi.

# Contenuto di un certificato

Ma vediamo più da vicino come possiamo accedere ad un certificato associato ad un sito Web e come visualizzare il suo contenuto. Come abbiamo detto, tutti i browser visualizzano un piccolo lucchetto che informa l'utente del fatto che si è connessi ad un server Web tramite connessione sicura. Ad esempio, su Firefox il lucchetto compare in basso sulla barra di stato, mentre su Internet Explorer appare sulla destra nella barra degli indirizzi.

Interagendo con l'icona del lucchetto (clic o doppio clic a seconda del browser) vengono visualizzate le informazioni relative alla sicurezza del sito ed è possibile visualizzare il contenuto del certificato. Ad esempio, la seguente figura mostra il certificato di un server dell'Agenzia delle Entrate:

Figura 1: Un certificato dell'agenzia delle entrate




I dati principali contenuti nel certificato indicano:

- **l'utilizzo a cui è destinato il certificato**. Nell'esempio è indicato che il certificato è utilizzato per l'identificazione di un server nell'ambito di una connessione protetta tramite protocollo SSL
- **a chi è stato rilasciato il certificato**. Dall'immagine dell'esempio ricaviamo che il certificato è associato al dominio *telematici.agenziaentrate.gov.it* in uso all'unità organizzativa Servizi telematici dell'Agenzia delle Entrate
- **l'Autorità di certificazione che lo ha rilasciato**. nel nostro caso si tratta di Cybertrust Inc.
- **il periodo di validità**. Individuato da una data di inizio e una di fine validità

Visualizzando il contenuto di un certificato abbiamo la possibilità di verificare che il sito a cui ci stiamo collegando è effettivamente quello che ci aspettiamo. La garanzia della validità dei dati contenuti nel certificato ci viene data dall'Autorità di certificazione che ha rilasciato il certificato.

In realtà non è necessario aprire il certificato associato ad una connessione sicura per verificare le informazioni fondamentali. Tutti i browser verificano automaticamente che il certificato sia stato rilasciato da un'Autorità di certificazione universalmente riconosciuta, che esso sia associato al dominio a cui si è collegati e che non sia scaduto.

Aprire un certificato può comunque essere utile per approfondire eventuali dettagli tecnici.

# Conclusioni

Abbiamo visto come la semplice crittografia dei dati trasmessi su una rete pubblica come Internet non offre una garanzia completa per una comunicazione sicura. I certificati digitali tendono a generare fiducia nell'utente garantendo l'identità di un sito Web.

Nella seconda parte di questo articolo vedremo come riconoscere i certificati ad alta affidabilità e cosa fare quando ci si imbatte in siti Web con certificati non validi.

Nella prima parte di questo articolo abbiamo visto come i certificati digitali hanno lo scopo di garantire l'identità di un sito Web. Continuiamo la nostra esplorazione analizzando il comportamento dei browser di fronte a determinati tipi di certificato e quando viene riscontrata qualche anomalia.

# Certificati... e garantiti

L'attendibilità del contenuto di un certificato dipende dall'Autorità di certificazione che lo ha rilasciato. Prima di rilasciare un certificato questi enti effettuano alcune verifiche sulle dichiarazioni fatte dal richiedente. Per i certificati standard normalmente la verifica si limita ad accertarsi dell'esistenza del dominio a cui è associato il certificato, che il dominio appartenga al richiedente ed in alcuni casi che effettivamente il richiedente possa essere contattato tramite e-mail o telefonicamente.

Tuttavia una tale verifica non esclude che il richiedente si faccia passare per un altro soggetto.

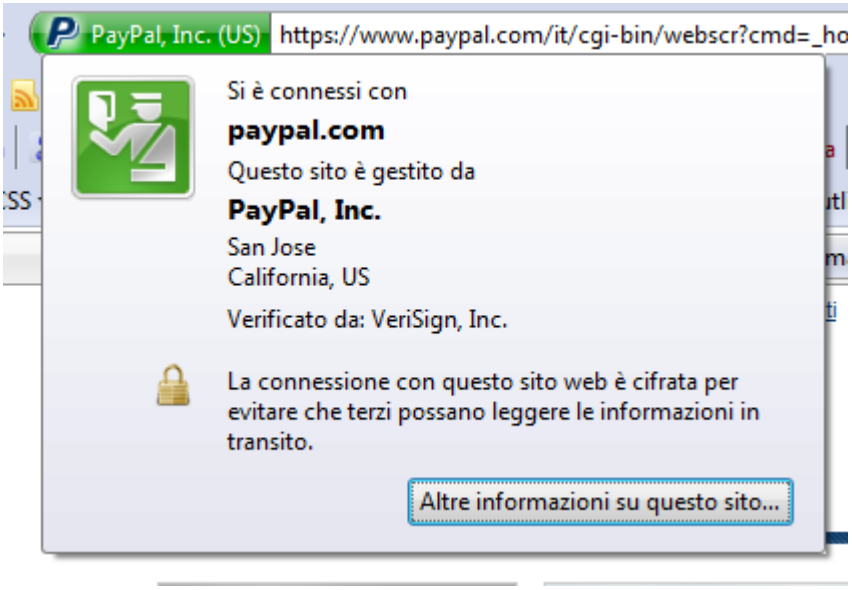
Per porre rimedio a questo potenziale pericolo è stato recentemente introdotto un tipo di certificato che offre maggiori garanzie sull'identità del possessore in quanto richiede una verifica più approfondita da parte dell'Autorità di certificazione. Si tratta dei certificati *Extended Validation* (EV).

Per il rilascio di questo tipo di certificato l'Autorità di certificazione non si limita a verificare l'esistenza del dominio e la relativa proprietà. Essa approfondisce l'identificazione del richiedente accedendo ad eventuali registri pubblici e richiedendo documentazione specifica per verificare legalmente e fisicamente l'identità del richiedente.

I browser più recenti, come ad esempio Internet Explorer 7 e Firefox 3, riconoscono questo tipo di certificati e lo evidenziano all'utente.

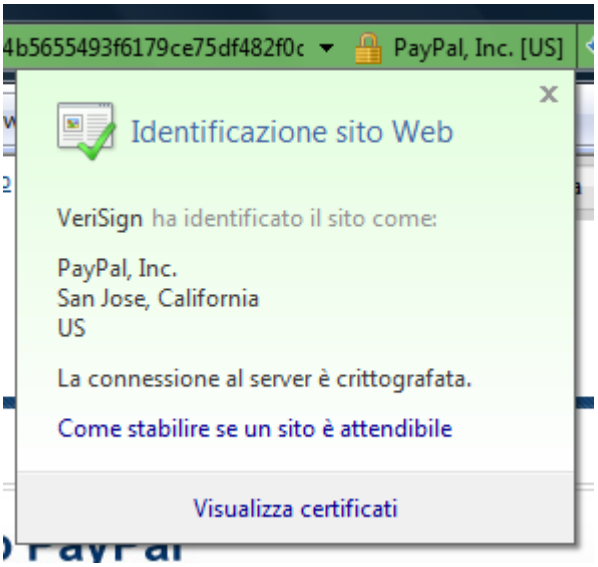
Ad esempio, Firefox mostra sulla sinistra della barra degli indirizzi il nome del possessore del certificato su uno sfondo verde; cliccando su questa area vengono visualizzati i dettagli identificativi del sito.

Figura 1: Certificato EV su Firefox




Internet Explorer, invece, mostra l'intera barra degli indirizzi in verde e sulla destra della stessa barra mostra il classico lucchetto con il nome del possessore del certificato; anche qui, cliccando sull'area vengono visualizzati i dettagli identificativi del sito.

Figura 2: Certificato EV su Internet Explorer




Grazie a queste segnalazioni visive, l'utente ha modo di rendersi conto dell'affidabilità del sito Web con cui sta interagendo. Quindi non solo le informazioni che trasmette al sito viaggeranno su un canale sicuro, ma ha anche una garanzia sull'identità del destinatario dei dati.

# Validità dei certificati

Durante la navigazione può capitare di visitare un sito con un certificato segnalato dal browser come non valido. Su Firefox potrebbe essere visualizzata una schermata simile alla seguente:

Figura 3: Certificato non valido su Firefox


Mentre su Internet Explorer verrebbe visualizzata una schermata del genere:

Figura 4: Certificato non valido su Explorer


Cosa fare in presenza di queste segnalazioni? Le azioni da compiere dipendono da diversi fattori dipendenti sia dal motivo della segnalazione di non validità sia dalle competenze tecniche dell'utente. Possiamo ricondurre i motivi di segnalazione di mancata validità di un certificato ai seguenti casi:

**L'Autorità di certificazione non è tra quelle riconosciute dal browser.** In questo caso è opportuno diffidare dal sito, a meno che non siamo sicuri dell'identità di chi ha emesso il certificato. Ad esempio, in determinate situazioni il certificato viene emesso dallo stesso possessore (una sorta di autocertificazione): si tratta di situazioni in cui i servizi proposti dal sito sono rivolti non al pubblico ma ad una ristretta cerchia di utenti. In questo caso la scelta di continuare l'interazione con il sito dipende dal nostro grado di confidenza con il sito stesso e con i suoi gestori

**Il dominio associato al certificato non corrisponde al dominio del sito a cui si è collegati**. Anche questa situazione è da affrontare con molta cautela. È opportuno in questi casi aprire il certificato e verificare il dominio a cui è associato. Può talvolta capitare che un sito sia accessibile con due domini,

supponiamo *www.dominio.com* e *www.dominio.it*, ma che il certificato sia associato soltanto al dominio *www.dominio.it*. Se accediamo al sito tramite *https://www.dominio.com* otterremo una segnalazione di questo tipo, anche se in realtà il sito con cui interagiamo è lo stesso.

**La data di validità del certificato è scaduta**. Come abbiamo visto prima, un certificato ha un periodo di validità fissato. Normalmente la durata è espressa in anni: uno, due e talvolta anche tre anni. Per garantire una maggiore sicurezza sarebbe buona norma che la validità del certificato durasse il minor tempo possibile. Questo per consentire un rinnovo più frequente delle chiavi necessarie per la crittografia. In linea di massima il fatto che un certificato sia scaduto non rappresenta di per sé una situazione particolarmente grave, soprattutto se è scaduto da poco tempo. Una segnalazione del genere può essere considerato un avvertimento che ci invita a verificare da quanto tempo il certificato è scaduto per stabilire se proseguire con la navigazione o meno. In ogni caso un sito con un certificato scaduto non offre un bel biglietto da visita...

**Il certificato è stato revocato**. Questa situazione rappresenta probabilmente la situazione più grave. Infatti un certificato viene revocato dall'Autorità di certificazione se, dopo l'emissione, viene rilevato qualche anomalia nella verifica dell'identità del richiedente o se si è verificato qualcosa che non rende più veritiere le informazioni presenti nel certificato. Ad esempio, nel caso di un certificato intestato ad un'azienda potrebbe essere cambiata la ragione sociale o l'azienda potrebbe non esistere più.

In queste situazioni è sempre meglio diffidare del sito su cui si sta navigando.

# Conclusioni

Come abbiamo avuto modo di vedere in questa breve panoramica, la sicurezza nella trasmissione dei dati sul Web non è data soltanto dalla loro codifica tramite algoritmi evoluti. È altrettanto importante identificare con certezza il destinatario dei dati. La tecnologia dei certificati digitali e l'infrastruttura di fiducia verso le Autorità di certificazione ci consentono di ottenere questa forma di identificazione. In ogni caso l'utente deve essere in grado di comprendere ed interpretare correttamente quello che strumenti come i browser ci segnalano sfruttando tali tecnologie.