Verifica del certificato

I certificati digitali vengono utilizzati per cifrare le connessioni e offrire agli utenti la sicurezza di essere connessi al sito Internet corretto. Dato che vengono utilizzati anche da siti Internet fraudolenti, è importante verificarne l'autenticità, soprattutto nell'e-banking.

Proteggetevi così:

- Nella barra degli indirizzi del browser digitate **sempre manualmente l'indirizzo Internet (URL) dell'istituto finanziario**.
- Prestate la dovuta attenzione ai **messaggi d'allarme e d'errore** che vengono visualizzati mentre si instaurano le connessioni, ed eventualmente interrompete l'operazione.
- Assicuratevi che la barra degli indirizzi sia contrassegnata da un'**icona a forma di lucchetto**.
- Controllate che il certificato sia stato rilasciato esplicitamente a **nome dell'istituto finanziario** (mostrato dopo aver fatto clic sul lucchetto nella riga «Rilasciato a:»).
- Verificate che l'indirizzo Internet (URL) contenga il **nome di dominio corretto** dell'istituto finanziario e che l'ortografia sia corretta. (Maggiori informazioni sulla struttura di un indirizzo Internet (URL) sono disponibili qui (https://www.ebas.ch/it/struttura-e-verifica-di-un-indirizzo-internet/) .)
- Inserite i vostri **dati d'accesso personali** solo dopo un esito positivo della verifica del certificato.

Protezione e rischi dei certificati

Ogni browser verifica automaticamente l'autenticità e la validità dei certificati TLS/SSL durante l'instaurazione della connessione, e visualizza il sito Internet correttamente e senza messaggi di errore solo se la verifica si è conclusa regolarmente.

Tuttavia, sempre più contraffazioni dei siti Internet degli istituti finanziari sono dotate di un certificato TLS/SSL valido a scopo di phishing, e per questo il semplice controllo del certificato da parte del browser non è più sufficiente per avere la certezza che il sito Internet visitato sia quello giusto.

Quindi, digitate sempre manualmente l'indirizzo Internet (URL) dell'istituto finanziario nella barra degli indirizzi del browser e controllate il certificato prima di ogni sessione di e-banking!

Verifica del certificato nel browser

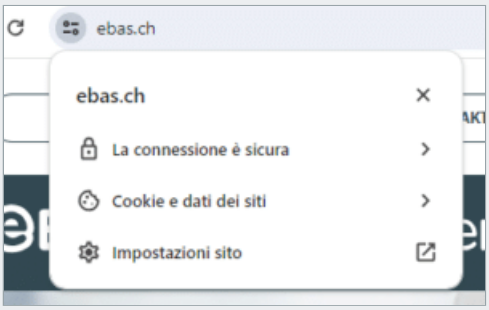
In estrema sintesi, quando si passa a una connessione protetta nel browser non devono comparire messaggi di errore, altrimenti ci sono dei problemi con il certificato o con la connessione, che va interrotta immediatamente.

Ciò significa che se compaiono messaggi d'allarme o d'errore non confermate mai manualmente il proseguimento della connessione!

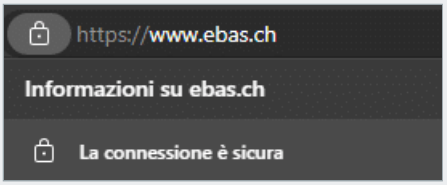
Una connessione TLS/SSL corretta – e quindi una connessione sicura – al sito Internet giusto, basata su un certificato autentico e valido, si riconosce da queste tre chiare indicazioni del browser:

1. **Icona a forma di lucchetto nella barra degli indirizzi**
   La connessione è stata criptata con un certificato TLS/SSL valido.
2. **Nome dell'istituto finanziario giusto (mostrato dopo aver fatto clic sul lucchetto nella riga «Rilasciato a:»)**
   L'identità del titolare del certificato (banca) è stata confermata.
3. **Nome di dominio corretto nell'indirizzo e ortografia corretta dell'indirizzo Internet (URL)**
   Vi trovate davvero sul sito dell'istituto finanziario.
   Qui (https://www.ebas.ch/it/struttura-e-verifica-di-un-indirizzo-internet/) potete leggere come è strutturato un indirizzo Internet (URL).

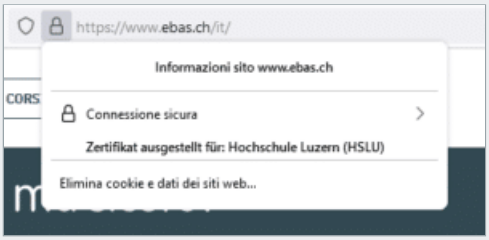
Google Chrome:



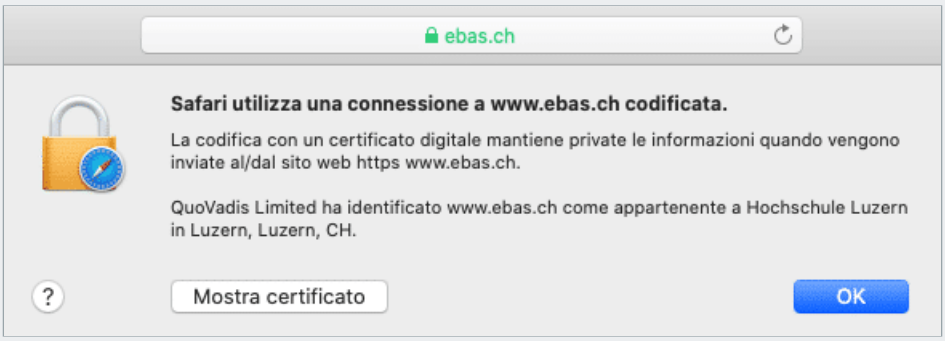
Microsoft Edge:



Mozilla Firefox:



Apple Safari:



La rappresentazione di queste caratteristiche differisce leggermente da un browser all'altro ed è riportata nelle istruzioni (https://www.ebas.ch/it/verifica-del-certificato-del-browser/) dei browser più comuni.

Verifica del certificato tramite impronta digitale

L'autenticità di un certificato può essere controllata manualmente: la procedura è un po' più elaborata ma proprio per questo motivo più sicura. L'«impronta digitale» (*fingerprint*) mostrata dal browser deve coincidere con quella pubblicata dall'istituto finanziario.

Se non è possibile verificare le impronte digitali, interrompete immediatamente la connessione!

Sul sito Internet «eBanking – ma sicuro!» trovate le impronte digitali delle pagine di login per l'e-banking (https://www.ebas.ch/it/impronta-digitale-del-certificato/) dei nostri banche partner e istruzioni (https://www.ebas.ch/it/verifica-del-certificato-del-browser/) dettagliate per verificare l'impronta digitale in diversi browser.

Nell'e-banking si utilizzano certificati digitali per garantire l'autenticità del server Web contattato e cifrare la connessione di comunicazione con il server. A tal fine viene utilizzato il protocollo TLS/SSL. Per questo si parla anche di certificati TLS/SSL e connessioni TLS/SSL.

Con poche operazioni è possibile verificare se la connessione è protetta come indicato.

Maggiori informazioni

Funzionamento di una connessione TLS/SSL

Quando si stabilisce una connessione protetta con un server Web, solitamente viene utilizzato il protocollo TLS/SSL. Si tratta di una tecnologia di telecomunicazione che cifra le informazioni da trasmettere in modo che non siano intercettabili e allo stesso tempo garantisce l'autenticità del server Web con cui viene stabilita la connessione.

Alla base della protezione implementata si trova un cosiddetto certificato digitale rilasciato per un server Web da un ente affidabile, noto anche come Autorità di certificazione.

Poiché l'impossibilità di intercettazione e l'autenticità del server Web sono garantite solo se il certificato su cui si basa la connessione TLS/SSL è autentico e valido, acquisisce un'importanza fondamentale la verifica del certificato.

Verifica del certificato con il supporto del browser

Quando instaura una connessione TLS/SSL, un browser verifica le proprietà del certificato seguenti:

- Affidabilità dell'emittente del certificato: il certificato è stato rilasciato (ossia fornito di firma digitale valida) da un'Autorità di certificazione affidabile. Questa verifica attesta l'autenticità del certificato.
- Validità del certificato: il certificato non è scaduto e non è stato dichiarato nullo (revocato) dall'Autorità di certificazione prima della scadenza del periodo di validità.
- Indirizzo del server Web: l'indirizzo del server Web inserito nel certificato corrisponde all'indirizzo effettivamente utilizzato nella barra degli indirizzi del browser.

Solo se queste tre verifiche hanno esito positivo il browser non visualizza nessun messaggio d'errore quando instaura la connessione TLS/SSL.

La verifica effettuata dal browser delle caratteristiche del certificato indicate offre un livello di sicurezza elevato, ma non è in grado di riconoscere in alcun modo i certificati rilasciati da un'Autorità di certificazione a un truffatore in seguito a un'analisi incorretta di chi lo ha richiesto. Alcune, poche truffe di questo tipo sono già note.

Dato che per il proprio certificato un truffatore sceglie, con enorme probabilità, un indirizzo diverso da quello dell'obiettivo dell'attacco (p. es. un istituto finanziario), questi certificati emessi in modo indebito si possono identificare controllando l'indirizzo Internet (URL) mostrato dal browser.

Oltre a questo l'utente deve verificare se il nome del dominio dell'indirizzo appartiene all'organizzazione contattata (cioè all'istituto finanziario). Per facilità, spesso molti browser evidenziano questa parte dell'indirizzo anche graficamente (p. es. in grassetto oppure in nero anziché in grigio).

Verifica del certificato tramite confronto dell'impronta digitale

Chiunque utilizzi una connessione TLS/SSL può verificare manualmente l'autenticità del certificato su cui si basa il collegamento. A tal fine, deve verificare l'impronta digitale del certificato.

L'impronta digitale si presenta come una sequenza di lettere dalla A alla F (senza distinzione tra lettere maiuscole e minuscole) e numeri dallo 0 al 9.

La verifica dell'impronta digitale viene eseguita confrontando tale sequenza con una sequenza di riferimento che l'utente ha ricevuto dall'istituto finanziario. Se la sequenza di caratteri riportata sul certificato e quella dell'istituto

finanziario coincidono, si ha la garanzia che il certificato sia autentico.

Se la sequenza di caratteri ricevuta dall'istituto finanziario è autentica, la verifica manuale dell'impronta digitale è il modo più sicuro per verificare il certificato.

Non è più necessario effettuare un controllo supplementare dell'indirizzo Internet (URL), come indicato sopra per la verifica con il supporto del browser.