Zertifikatsprüfung

Digitale Zertifikate werden genutzt, um Verbindungen zu verschlüsseln und den Anwendenden Sicherheit zu geben, mit der korrekten Website verbunden zu sein. Da sie auch von betrügerischen Websites verwendet werden, gilt es, ihre Echtheit, insbesondere beim E-Banking zu überprüfen.

Schützen Sie sich, indem Sie...

- im Adressfeld des Browsers die **Internetadresse (URL) des Finanzinstituts immer von Hand** eintippen.
- auftretenden **Warnhinweisen und Fehlermeldungen** beim Aufbau von Verbindungen die nötige Beachtung schenken und den Verbindungsaufbau allenfalls abbrechen.
- darauf achten, dass das **Schloss-Symbol** angezeigt wird (entweder neben der Internetadresse oder nach einem Klick auf den Schieberegler).
- verifizieren, dass die Internetadresse (URL) den **korrekten Domänen-Namen** des Finanzinstituts beinhaltet und die Schreibweise korrekt ist. (Weitere Informationen zum Aufbau einer Internetadresse (URL) finden Sie hier (https://www.ebas.ch/aufbau-und-ueberpruefung-einer-internetadresse/) .)
- Ihre **persönlichen Zugangsdaten** erst nach erfolgreicher Zertifikatsprüfung eingeben.

Schutz und Gefahr durch Zertifikate

Jeder Browser überprüft TLS/SSL-Zertifikate beim Verbindungsaufbau automatisch auf Echtheit und Gültigkeit und zeigt die Ziel-Website nur bei erfolgreicher Überprüfung korrekt und ohne Fehlermeldung an.

Da jedoch immer häufiger auch gefälschte Websites von Finanzinstituten zu Phishing-Zwecken mit einem gültigen TLS/SSL-Zertifikat ausgestattet werden, reicht die alleinige Zertifikatsprüfung durch den Browser nicht aus, um mit Sicherheit auf der korrekten Website zu sein.

Tippen Sie daher die Internetadresse (URL) des Finanzinstituts immer von Hand im Adressfeld des Browsers ein und überprüfen Sie vor jeder E-Banking-Sitzung das Zertifikat!

Zertifikatsprüfung im Browser

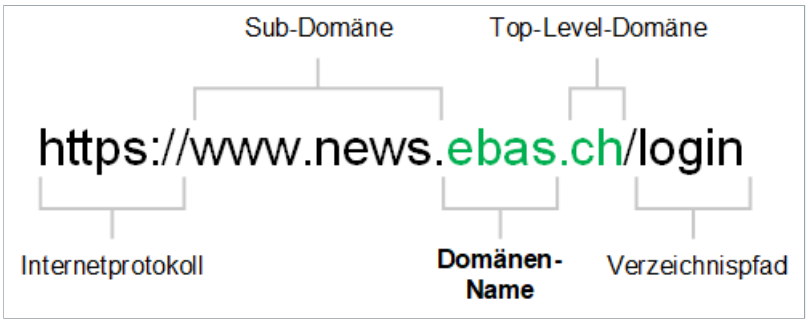
Grundsätzlich dürfen im Browser beim Wechsel zu einer geschützten Verbindung keine Fehlermeldungen auftreten. Andernfalls stimmt mit dem Zertifikat oder der Verbindung etwas nicht und die Verbindung sollte unverzüglich beendet werden.

Setzen Sie deshalb den Verbindungsaufbau bei Auftreten von Warnhinweisen oder Fehlermeldungen niemals manuell fort!

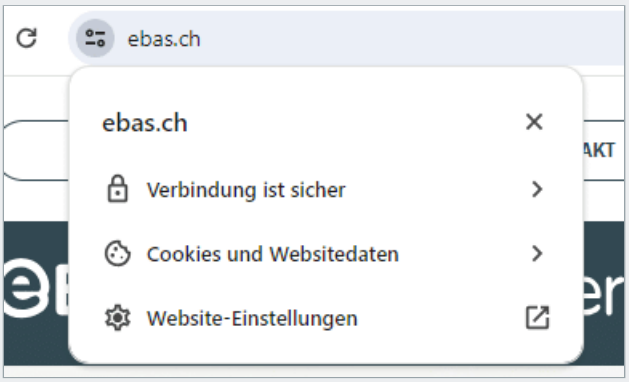
Eine korrekt aufgebaute TLS/SSL-Verbindung – also eine sichere Verbindung – zur richtigen Webseite, die auf einem echten und gültigen Zertifikat basiert, erkennen Sie anhand der folgenden zwei eindeutigen Browser-Merkmale:

1. **Schloss-Symbol (wird entweder neben der Internetadresse oder nach einem Klick auf den Schieberegler angezeigt)**
   Die Verbindung wurde mit gültigem TLS/SSL-Zertifikat verschlüsselt.
2. **Korrekter Domänen-Name in der Adresse**
   Sie befinden sich wirklich auf der Seite des Finanzinstituts.

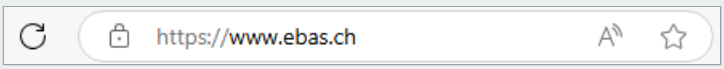
   Der **Domänen-Name** ist der eindeutige Name der Website, so wie z.B. hier auf dieser Website «ebas». Dies ist, zusammen mit der **Top-Level-Domäne** (letzter Teil rechts vom letzten Punkt einer Domäne), der wichtigste Teil der Internetadresse (https://www.ebas.ch/aufbau-und-ueberpruefung-einer-internetadresse/) .



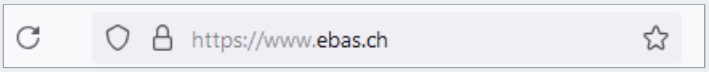
Google Chrome:



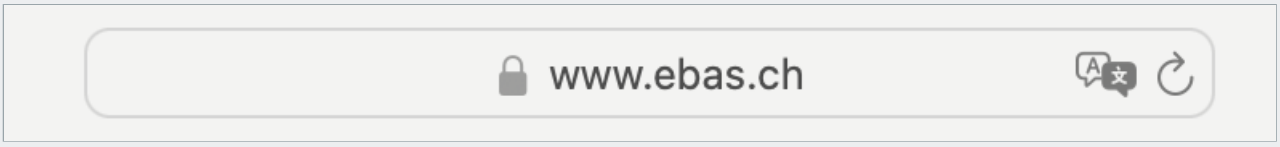
Microsoft Edge:



Mozilla Firefox:



Apple Safari:



Die konkrete Darstellung dieser Merkmale unterscheidet sich von Browser zu Browser geringfügig und kann unter Anleitungen (https://www.ebas.ch/browser-zertifikatspruefung/) für die verbreiteten Browser nachgelesen werden.

Zertifikatsprüfung mittels Fingerabdruck

Die Echtheit eines Zertifikats lässt sich etwas aufwendiger, dafür umso sicherer auch manuell überprüfen. Der vom Browser angezeigte «Fingerabdruck» (Fingerprint) muss dabei mit dem vom Finanzinstitut publizierten Fingerabdruck übereinstimmen.

Beenden Sie bei nicht verifizierbaren Fingerabrücken die Verbindung sofort!

Auf der «eBanking – aber sicher!» Website finden Sie die Fingerabdrücke der E-Banking Login-Seiten (https://www.ebas.ch/zertifikatsfingerabdruck/) unserer Partner-Banken sowie detaillierte Anleitungen (https://www.ebas.ch/browser-zertifikatspruefung/), wie Sie den Fingerabdruck mithilfe verschiedener Browser überprüfen können.

Beim E-Banking werden digitale Zertifikate verwendet, um die Echtheit des angesprochenen Webservers zu garantieren, und um die Kommunikationsverbindung zum Server zu verschlüsseln. Dabei kommt das TLS/SSL-Protokoll zur Anwendung. Man spricht daher auch kurz von TLS/SSL-Zertifikaten und TLS/SSL-Verbindungen.

In wenigen Schritten können Sie überprüfen, ob die Verbindung wie vorgegeben geschützt ist.

Weiterführende Informationen für Interessierte

Funktionsweise einer TLS/SSL-Verbindung

Wenn zu einem Webserver eine sichere Verbindung aufgebaut wird, kommt meist das TLS/SSL-Protokoll zum Einsatz. Es handelt sich dabei um eine Kommunikationstechnologie, welche zu übertragende Informationen abhörsicher verschlüsselt und gleichzeitig die Authentizität, also Echtheit des Webservers, zu dem eine Verbindung hergestellt wird, garantiert.

Basis für den implementierten Schutz ist ein so genanntes digitales Zertifikat, das von einer vertrauenswürdigen Instanz – auch Zertifizierungsstelle genannt – für einen Webserver ausgestellt wird.

Da die Abhörsicherheit und die Echtheit des Webservers nur garantiert sind, wenn das der TLS/SSL-Verbindung zugrundeliegende Zertifikat echt und gültig ist, kommt der Zertifikatsprüfung eine zentrale Rolle zu.

Zertifikatsprüfung mit Browser-Unterstützung

Ein Browser verifiziert beim Aufbau einer TLS/SSL-Verbindung die folgenden Zertifikatseigenschaften:

- Vertrauenswürdigkeit des Ausstellers des Zertifikats: Das Zertifikat wurde von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt (d.h. von dieser gültig digital signiert). Durch diese Überprüfung wird dem Zertifikat Echtheit attestiert.
- Gültigkeit des Zertifikats: Das Zertifikat ist nicht abgelaufen oder von der Zertifizierungsstelle vor Ablauf der Gültigkeitsdauer für ungültig erklärt (revoziert) worden.
- Adresse des Webservers: Die im Zertifikat eingetragene Adresse des Webservers stimmt mit der tatsächlich im Adressfeld des Browsers verwendeten Adresse überein.

Nur wenn diese drei Überprüfungen erfolgreich durchgeführt werden konnten, zeigt der Browser beim Aufbau der TLS/SSL-Verbindung keine Fehlermeldungen an.

Die Verifikation der obigen Zertifikatseigenschaften durch den Browser bietet ein hohes Mass an Sicherheit, kann aber in keinem Fall Zertifikate identifizieren, welche eine Zertifizierungsstelle nach mangelhafter Antragstellerprüfung für einen Betrüger ausgestellt hat. Einige wenige Betrugsfälle dieser Art sind bekannt geworden.

Da ein Betrüger für sein Zertifikat mit sehr hoher Wahrscheinlichkeit eine Adresse wählt, welche sich von derjenigen des Angriffsziels (z.B. ein Finanzinstitut) unterscheidet, lassen sich solche missbräuchlich ausgestellten Zertifikate durch eine Überprüfung der vom Browser angezeigten Internetadresse (URL) identifizieren.

Dazu muss durch den Benutzer verifiziert werden, ob der Domänen-Name der Adresse zur kontaktierten Organisation (z.B. ein Finanzinstitut) gehört. Viele Browser heben diesen Teil der Adresse zur Vereinfachung der Überprüfung oft graphisch (z.B. fett oder tiefschwarz) hervor.

Zertifikatsprüfung durch Vergleich des Fingerabdrucks

Jeder Benutzer einer TLS/SSL-Verbindung kann die Echtheit des der Verbindung zu Grunde liegenden Zertifikats manuell überprüfen. Dazu muss er den Fingerabdruck des Zertifikats verifizieren.

Der Fingerabdruck ist eine Zeichenfolge bestehend aus den Buchstaben A-F (wobei nicht zwischen Gross- und Kleinbuchstaben unterschieden wird) und den Ziffern 0-9.

Die Verifikation des Fingerabdrucks erfolgt durch manuellen Vergleich dieser Zeichenfolge mit einer Referenzfolge, die der Benutzer vom Finanzinstitut bekommen hat. Sind die aus dem Zertifikat herausgelesene Zeichenfolge und die vom Finanzinstitut erhaltene Zeichenfolge identisch, dann ist das Zertifikat garantiert echt.

Unter der Voraussetzung, dass die vom Finanzinstitut erhaltene Zeichenfolge echt ist, stellt die manuelle Überprüfung des Fingerabdrucks damit die sicherste Art der Zertifikatsprüfung dar.

Eine zusätzliche Überprüfung der Internetadresse (URL), wie oben bei der Zertifikatsprüfung mit Browser-Unterstützung beschrieben, erübrigt sich dabei.