Checking certificates

Digital certificates are used to encrypt connections and provide those using them with the certainty that they are connected to the correct website. However, they are also used by fraudulent websites, so it is important to check they are actually genuine, especially when e-banking.

Protect yourself by...

- always entering your **financial institution’s Internet address (URL) manually** into your browser address line.
- paying proper attention to any **warning messages and error alerts** appearing when establishing a connection, and cancelling the process if needs be.
- making sure that the address line is marked with a **lock symbol**.
- checking whether the certificate was explicitly issued for the **financial institution’s name** (this is displayed after you click the lock symbol, under “Issued for”).
- verifying that the Internet address (URL) contains the **correct domain name** of your financial institution and is spelled correctly (further information on the structure of Internet addresses (URLs) can be found here (https://www.ebas.ch/en/internet-address-structure-and-checking/)).
- only entering your **personal access data** once the certificate has successfully been checked.

Protection provided and risks inherent in certificates

Every browser automatically checks TLS/SSL certificates for authenticity and validity when establishing a connection, and only displays the target website once this check successfully verified the website as correct and as displaying without any error notifications.

Since an ever increasing number of faked financial institution websites however are also fitted with a valid TLS/SSL certificate for phishing purposes, it is not sufficient just for the browser to check a certificate to make absolutely sure you are on the correct website.

You should therefore always enter your financial institution’s Internet address (URL) manually into your browser’s address line, and check the certificate before starting any e-banking session!

Checking certificates in your browser

Generally, your browser must not display any error messages when changing over to a protected connection. Otherwise, there is something wrong with the certificate or the connection, and you should immediately terminate the connection.

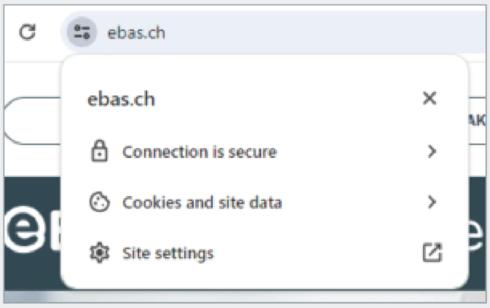
You should therefore never manually continue to establish a connection if any warning notices or error

messages are displayed!

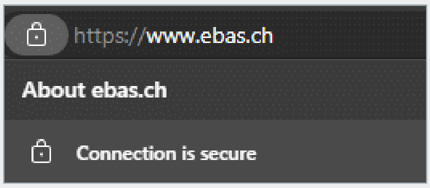
A TLS connection which has been correctly established with the proper website and which is based on an authentic and valid certificate – i.e. a secure connection – can be recognised by the following three clear browser characteristics:

1. **A lock symbol in the address line**
   This connection was encrypted using a valid TLS/SSL certificate.
2. **The correct financial institution’s name (this is displayed after clicking the lock symbol, under “Issued for”)**
   The identify of the certificate owner (the bank) has been confirmed.
3. **Correct domain name and correct spelling of the Internet address (URL)**
   You are actually on the financial institution’s website.
   You can read up on how an Internet address is structured here (https://www.ebas.ch/en/internet-address-structure-and-checking/) .

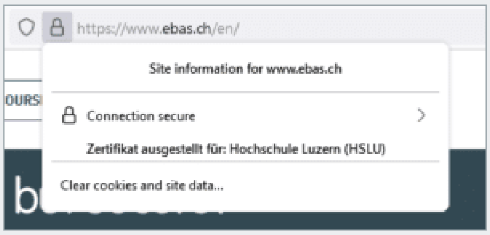
Google Chrome:



Microsoft Edge:



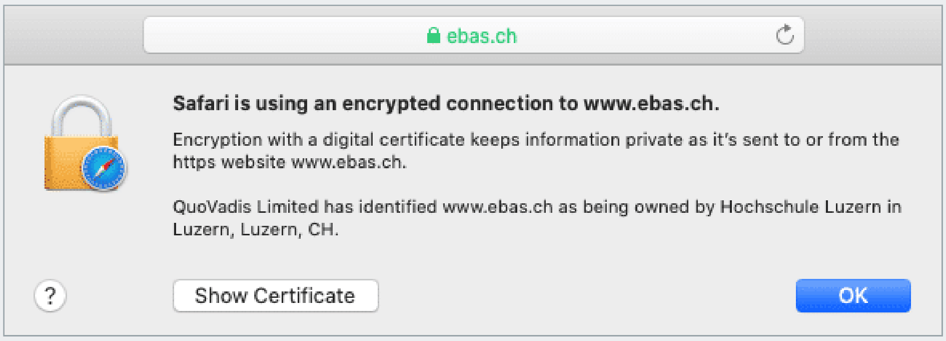
Mozilla Firefox:


https://www.ebas.ch/en/
Site information for www.ebas.ch
Connection secure

Zertifikat ausgestellt für: Hochschule Luzern (HSLU)

Clear cookies and site data...

Apple Safari:



Safari is using an encrypted connection to www.ebas.ch.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.ebas.ch.

QuoVadis Limited has identified www.ebas.ch as being owned by Hochschule Luzern in Luzern, Luzern, CH.

The specific display of these characteristics differs slightly from one browser to the next. You can read up on it under our instructions (https://www.ebas.ch/en/browser-certificate-checking/) for the most common browsers.

Checking certificates using finger prints

Manually checking the authenticity of a certificate provides even more security, even if it is a bit more laborious. In this case, the “finger print” displayed in the browser has to agree with the finger print published by the financial institution.

If a finger print cannot be identified, you must immediately terminate the connection!

The finger prints of the e-banking log-in pages (https://www.ebas.ch/en/certificate-finger-print/) of our partner banks plus detailed instructions (https://www.ebas.ch/en/browser-certificate-checking/) on how to check these finger prints with the help of various browsers can be found on our “eBanking – but secure!” website.

E-banking facilities use digital certificates to safeguard that the web server accessed is actually genuine, and to encrypt communication channels connecting to servers. They employ the TLS/SSL protocol to do so. They are therefore also called “TLS/SSL certificates” and “TLS/SSL connections” for short.

It only takes a few steps to check whether a connection is protected as it should be.

Further information for those interested

TLS/SSL connection operating principle

In general, the TLS/SSL protocol is the one most frequently used to establish a secure connection to a web server. This is communications technology which encrypts information to be transmitted so it cannot be captured. At the same time, it guarantees the authenticity of the web server to which you are connecting, i.e. that the web server is genuine.

The basis of the protection provided is a so-called digital certificate issued by a trustworthy body – a certification body – for a web server.

Since it can only be guaranteed that the web server is genuine and cannot be eavesdropped on for as long as the certificate underlying the TLS/SSL connection is authentic and valid, certificate checking plays a central role here.

Checking certificates with browser support

When browsers establish a TLS/SSL connection, they verify the following certificate properties:

- Trustworthiness of the certificate issuer: The certificate was issued by a trustworthy certification body (i.e. it was digitally signed by this body). These checks safeguard that the certificate is genuine.
- Certificate validity: The certificate has not expired and has not been declared invalid (has been revoked) before its expiry date.
- Web server address: The web server address provided in the certificate agrees with the address used in the actual browser address field.

Only once these three checks have been successfully concluded will there be no error messages displayed by the browser when establishing a TLS/SSL connection.

Verification of the above certificate properties by browsers offers a great degree of security, can however never identify certificates which were issued by a certificate body to a fraudster due to insufficient applicant checks. A few fraud cases of this kind did emerge.

Since fraudsters are highly likely to choose an address for their certificates which differs from the one of the actual target (financial institution), such improperly issued certificates can be identified by checking the Internet address (URL) displayed in the browser.

To this end, users will have to identify whether the domain name of the address actually belongs to the organisation they want to contact (e. g. a financial institution). Many browsers graphically underline this part of the address to make verification easier (for instance in bold or deep black letters).

Checking certificates by comparing finger prints

Every TLS/SSL connection user can check the authenticity of the certificate underlying a connection manually. To this end, they will have to verify the certificate finger print.

A finger print is usually displayed as a hexadecimal character string consisting of the letters A-F (although no differentiation is made between uppercase and lowercase letters) and the numbers 0-9.

Finger prints can be verified by manually comparing this character set with a reference set which users will have received from their financial institution. If the character sequence read from the certificate and the reference sequence received from a financial institution are identical, this is a genuine certificate.

Provided that the character set received from a financial institution is genuine, manually checking a finger print is therefore the most secure method of checking certificates.

There is then no need to additionally check the Internet address (URL) as described above for certificate checking with browser support.