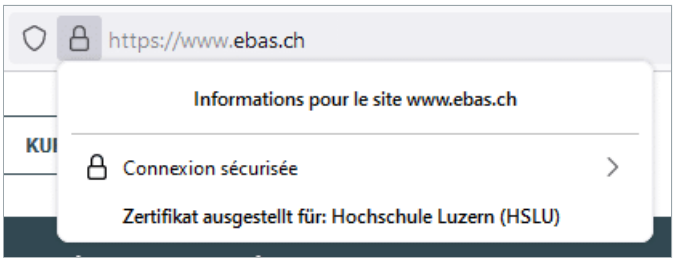
Contrôle du certificat du navigateur

Ce guide vous aidera à vérifier l'empreinte numérique de certificat d'un site web affiché dans le navigateur Mozilla Firefox.

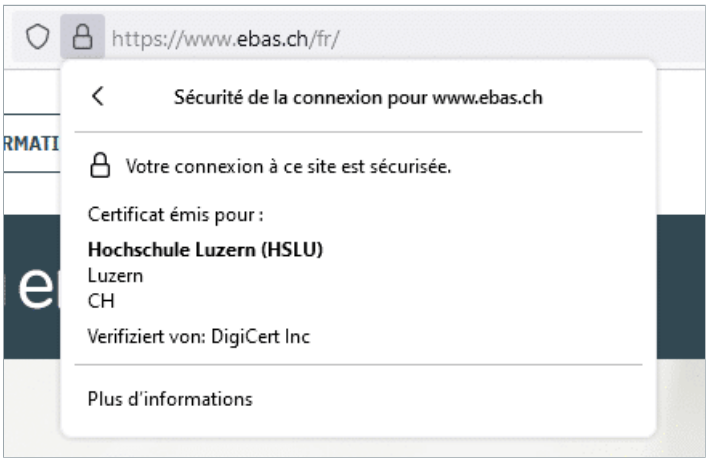
Cliquez ici (#OtherBrowsers) pour accéder au mode d'emploi d'un autre navigateur.

1. Cliquez sur le symbole du **cadenas** dans la barre d'adresse.

2. Cliquez sur la **flèche** pour afficher les détails de la connexion.

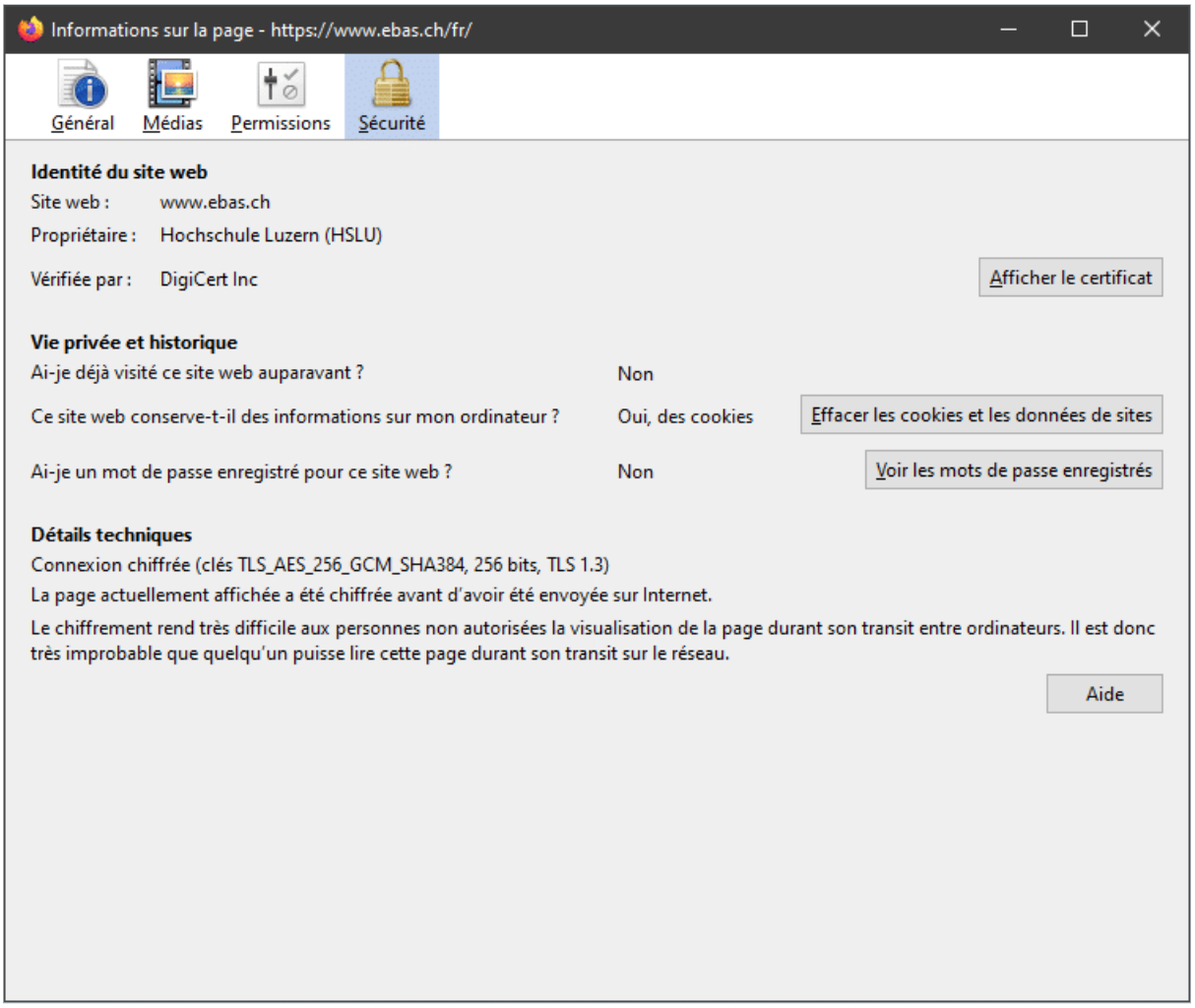


3. Cliquez sur **Plus d'informations**.



4. Cliquez sur **Afficher le certificat**.

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique



5. Pour vérifier l'empreinte numérique, vous devez comparer la suite de caractères qui s'affiche dans la fenêtre avec la suite de référence que vous aura fourni votre établissement financier. Si la suite de caractères de l'empreinte numérique de certificat est identique à celle communiquée par l'institut financier, le certificat est authentique. Lorsque vous comparez les deux suites de caractères, assurez-vous aussi qu'elles sont bien du même type (soit SHA-256 ou SHA-1). Vous trouverez les empreintes numériques de certificat de nos banques partenaires sur notre site Internet dans l'article Le contrôle du certificat (https://www.ebas.ch/fr/le-controle-du-certificat/) . (https://www.ebas.ch/zertifikatspruefung/)

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

www.ebas.ch | DigiCert EV RSA CA G2 | DigiCert Global Root G2

Nom du sujet

Pays d'enregistrement	CH
Catégorie d'affaires	Government Entity
Numéro de série	CHE-302.967.535
Pays	CH
Localité	Luzern
Organisation	Hochschule Luzern (HSLU)
Nom courant	www.ebas.ch

Nom de l'émetteur

Pays	US
Organisation	DigiCert Inc
Nom courant	DigiCert EV RSA CA G2

Validité

Pas avant	Fri, 28 Jun 2024 00:00:00 GMT
Pas après	Thu, 10 Jul 2025 23:59:59 GMT

Noms alternatifs du sujet

Nom DNS	www.ebas.ch
Nom DNS	ebas.ch
Nom DNS	www.ebankingabersicher.ch
Nom DNS	ebankingabersicher.ch
Nom DNS	www.ebankingmasicuro.ch
Nom DNS	ebankingmasicuro.ch
Nom DNS	www.ebankingentoutesecurite.ch
Nom DNS	ebankingentoutesecurite.ch
Nom DNS	www.ebankingbutsecure.ch
Nom DNS	ebankingbutsecure.ch

Informations sur la clé publique

Algorithme	RSA
Taille de la clé	2048
Exposant	65537
Module	D0:A3:DB:F4:4C:C4:D8:82:93:21:30:01:F1:CE:98:25:AE:21:01:12:46:04:68:2A:1D:88:...

Divers

Numéro de série	0F:D2:84:C9:06:55:2C:FD:99:DC:CB:BC:5B:2A:B6:F6
Algorithme de signature	SHA-256 with RSA Encryption
Version	3
Télécharger	PEM (cert) PEM (chain)

Empreintes numériques

SHA-256	FE:AC:6B:61:EA:47:CA:2A:BA:57:97:D1:50:D7:9B:9C:E8:CA:BA:BC:DC:46:E0:C0:58...
SHA-1	93:1B:29:E2:EB:F7:9F:2E:D0:45:45:06:A4:94:F1:02:AE:6C:BD:D2

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

Modes d'emploi pour d'autres navigateurs :

Google Chrome (https://www.ebas.ch/fr/le-controle-du-certificat-avec-chrome/)

Microsoft Edge (https://www.ebas.ch/fr/le-controle-du-certificat-avec-edge/)

Apple Safari (https://www.ebas.ch/fr/le-controle-du-certificat-avec-safari/)

Android Google Chrome (https://www.ebas.ch/zertifikatspruefung-android-google-chrome/)

L'empreinte numérique d'un certificat permet de vérifier l'authenticité du certificat sur lequel repose une connexion TLS/SSL. Une empreinte électronique se présente la plupart du temps comme une chaîne hexadécimale composée de chiffres de 0 à 9 et de lettres de A à F.

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique