Curl SSL Problems

See also Configure an own SSL certificate for a existing installation or vhost

With translate5 3.1.1 PHP must be installed with curl. Curl is needed to talk to several third party services, mainly openID connect, or also the language resource "google machine translation".

The communication is done encrypted with SSL therefore curl needs up to date ca.cert informations on the local machine. The CAs of the SSL certificate of the requested URLs are checked against this local CA list.

If the local CA list is not update or if the requested server does not provide all intermediate certificates, the following or similar errors can occur:

> *cURL error 60: SSL certificate problem: unable to get local issuer certificate*

Investigate the problem

Either use an online tool like https://globalsign.ssllabs.com/ or a local openssl to track down the problem:

```
openssl s_client -showcerts -connect DOMAINTOTEST:https
```

If openssl shows only one certificate with a error like that:

```
Verify return code: 21 (unable to verify the first certificate)
```

This indicates that the requested server only provides the server certificate but no intermediate certificate.

The problem about missing intermediates is, that browser solve that problem automatically by either fetching the missing intermediates or check an internal cache containing already the missing intermediate certificates.

Curl does not have such a cache / fetch mechanism.

Therefore a good server always provides the server cert and its cert chain / intermediate certs.

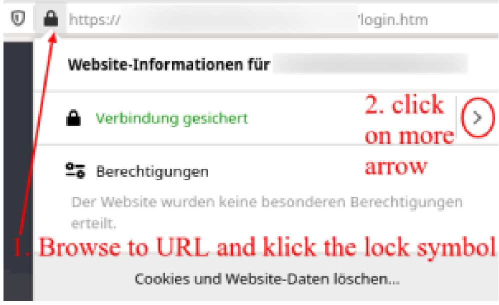
Solution if CA chain provided by the server is not complete

Contact the server administrator so that the missing intermediate certificates / the certificate chain is delivered too. For example in apache this must be done in configuration like that:

```
<VirtualHost *:443>
    ServerName notexistingexample.translate5.net
    DocumentRoot /pathtowebroot/notexistingexample.translate5.net/public
    SSLEngine on
    SSLCertificateFile /pathto/server-cert.crt
    SSLCertificateKeyFile /pathto/server-cert-key-file.key
    SSLCertificateChainFile /pathto/cert-chain-with-all-intermediate-certs.crt
</VirtualHost>
```

Provide missing chain as intermediate solution

Open the HTTPS URL in firefox, click on the lock symbol beneath the URL.



https:// 'login.htm

Website-Informationen für

Verbindung gesichert

Berechtigungen

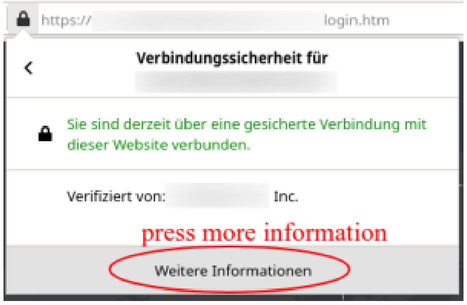
Der Website wurden keine besonderen Berechtigungen erteilt.

Cookies und Website-Daten löschen…

2. click on more arrow

1. Browse to URL and klick the lock symbol

Click on more information.



https:// login.htm

Verbindungssicherheit für

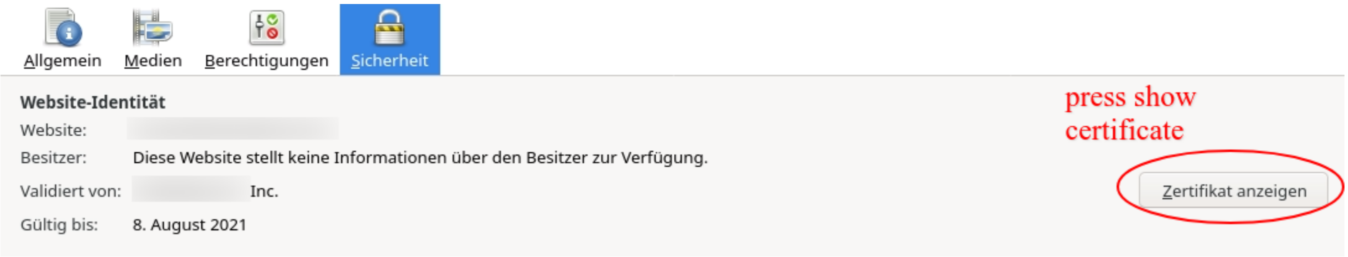
Sie sind derzeit über eine gesicherte Verbindung mit dieser Website verbunden.

Verifiziert von: Inc.

press more information

Weitere Informationen

Then a new window opens in firefox, press on show certificate.



Website-Identität

Website:

Besitzer: Diese Website stellt keine Informationen über den Besitzer zur Verfügung.

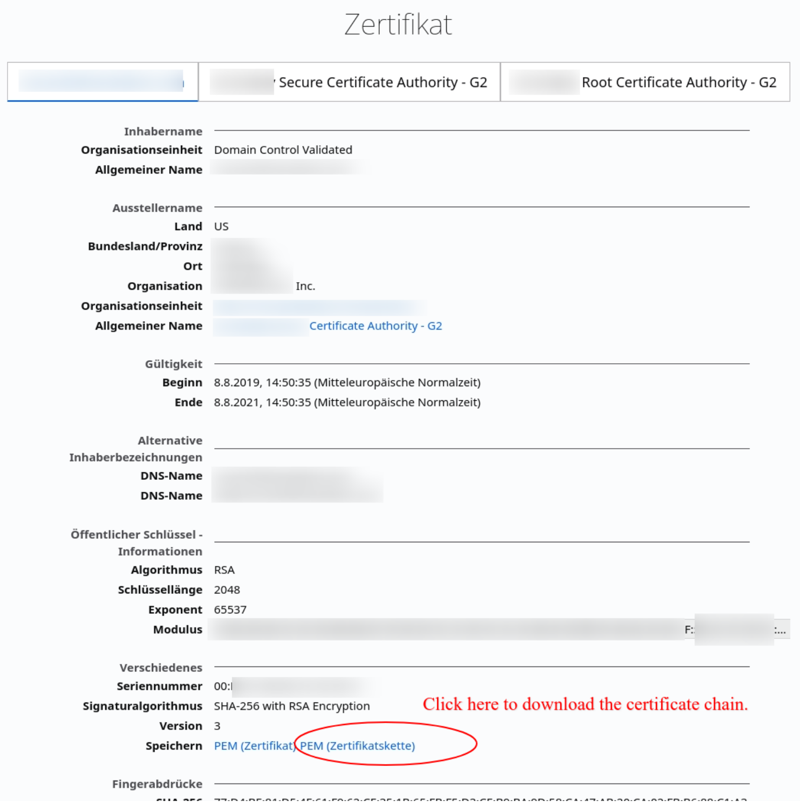
Validiert von: Inc.

Gültig bis: 8. August 2021

press show certificate

Zertifikat anzeigen

In a new tab more information about the certificate is shown. Each certificate in the chain gets an own tab in that window. In the first Tab - the server certificate - click on "Save PME (Certificatechain)"



Zertifikat

[redacted]
[redacted] Secure Certificate Authority - G2
[redacted] Root Certificate Authority - G2

Inhabername	
Organisationseinheit	Domain Control Validated
Allgemeiner Name	[redacted]
Ausstellername	
Land	US
Bundesland/Provinz	[redacted]
Ort	[redacted]
Organisation	[redacted] Inc.
Organisationseinheit	[redacted]
Allgemeiner Name	[redacted] Certificate Authority - G2
Gültigkeit	
Beginn	8.8.2019, 14:50:35 (Mitteleuropäische Normalzeit)
Ende	8.8.2021, 14:50:35 (Mitteleuropäische Normalzeit)
Alternative Inhaberbezeichnungen	
DNS-Name	[redacted]
DNS-Name	[redacted]
Öffentlicher Schlüssel - Informationen	
Algorithmus	RSA
Schlüssellänge	2048
Exponent	65537
Modulus	[redacted] F:[redacted]:...
Verschiedenes	
Seriennummer	00:[redacted]
Signaturalgorithmus	SHA-256 with RSA Encryption
Version	3
Speichern	PEM (Zertifikat) PEM (Zertifikatskette)
Fingerabdrücke	

Click here to download the certificate chain.

Save that file for later reuse with CURL.

```
openssl s_client -showcerts -CAfile /path/to/downloadedchainfile.pem -connect DOMAINTOTEST:https

# or with curl

curl --cacert /path/to/downloadedchainfile.pem -v https://DOMAINTOTEST
```

PHP Curl

In PHP curl the chain file must be provided with the following curl option:
`curl_setopt($ch, CURLOPT_CAINFO, "/path/to/downloadedchainfile.pem");`

> The server must provide valid certificate data, so consider above CAINFO setting only as temporary workaround!

Solution if local CA is completely not update

In this case either update the CA bundle of the operating system (updating ca-certificates package) , or download up-to-date CA bundle on your own, and configure curl to use it.

To use the downloaded file, use it at an suitable place on the disk and configure it in the used php.ini:

```
curl.cainfo = "/path/to/cacert.pem"
```

The cacert.pem can be downloaded from http://curl.haxx.se/ca/cacert.pem

See also https://daniel.haxx.se/blog/2018/11/07/get-the-ca-cert-for-curl/

Resources

- Explanation that browsers do fetching and caching of missing intermediates, curl does not do that.
  Also explanation how to check all single certificates:
  https://medium.com/@superseb/get-your-certificate-chain-right-4b117a9c0fce
- https://stackoverflow.com/questions/29822686/curl-error-60-ssl-certificate-unable-to-get-local-issuer-certificate
- Pointing into the direction of missing intermediate certificates:
  https://stackoverflow.com/a/35869560/1749200
- http://unitstep.net/blog/2009/05/05/using-curl-in-php-to-access-https-ssltls-protected-sites/
- Example of a PHP CURL request:
  https://stackoverflow.com/questions/4372710/php-curl-https
- Brief explanations why `CURLOPT_SSL_VERIFYPEER` is very dangerous:
  https://stackoverflow.com/a/14914398/1749200
  https://www.saotn.org/dont-turn-off-curlopt_ssl_verifypeer-fix-php-configuration/