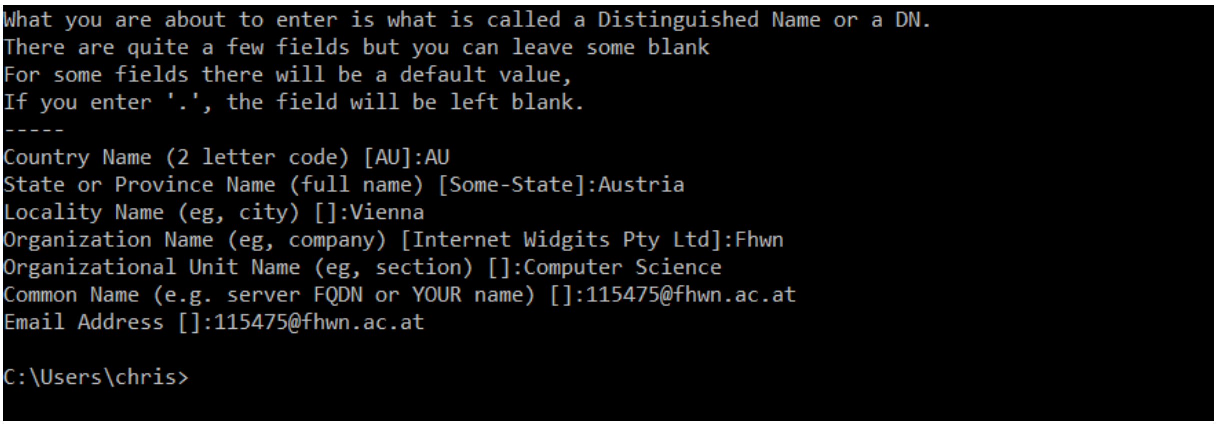
Create Root CA for X.509 certificates and a root certificate

openssl genrsa -out rootCA.key 4096

openssl req -new -key rootCA.key -out rootCA.csr -sha256

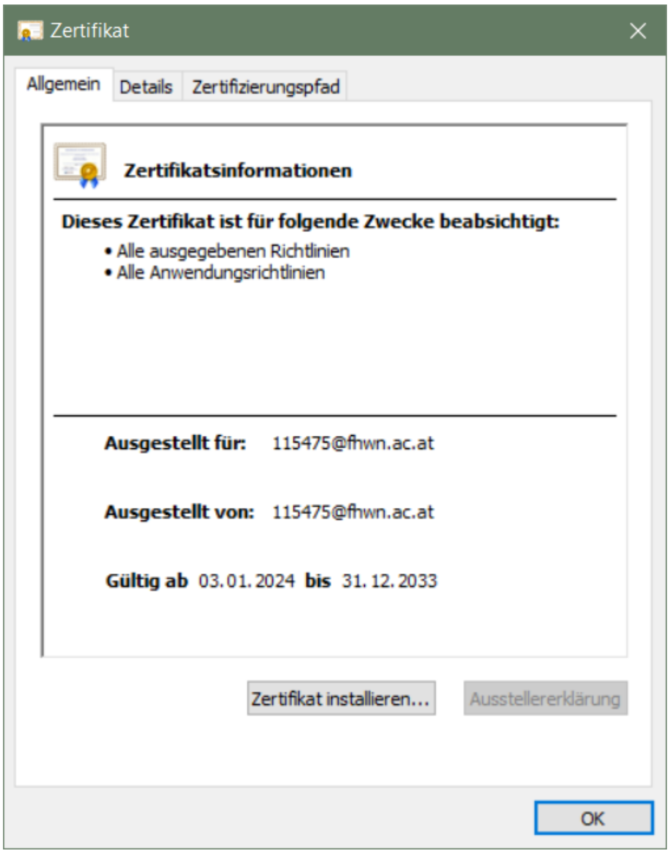
openssl x509 -req -days 3650 -in rootCA.csr -signkey rootCA.key -out rootCA.crt -sha256

Entering Subject (Same done for webserver certificate)



```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:Austria
Locality Name (eg, city) []:Vienna
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Fhwn
Organizational Unit Name (eg, section) []:Computer Science
Common Name (e.g. server FQDN or YOUR name) []:115475@fhwn.ac.at
Email Address []:115475@fhwn.ac.at

C:\Users\chris>
```

The created root certificate needs to be installed/imported into the list of trusted root Cas.



Zertifikatsinformationen

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Alle ausgegebenen Richtlinien
- Alle Anwendungsrichtlinien

Ausgestellt für: 115475@fhwn.ac.at

Ausgestellt von: 115475@fhwn.ac.at

Gültig ab 03.01.2024 **bis** 31.12.2033

Create Webserver certificate signed by the Root CA

```
openssl genrsa -out rootCA.key 4096
```

```
openssl req -new -key server.key -out server.csr -sha256
```

The default version (1) will be chosen for X509 if not specified, which leads to “Subject Atlernative Name Missing” and “ERR_CERT_COMMON_NAME_INVALID” errors, especially in Chrome. Thus, specifying it as version 3, will fix it. First following v3.ext file hast to be created and then added to the signing command as such:

```
authorityKeyIdentifier=keyid,issuer

basicConstraints=CA:FALSE

keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment

subjectAltName = @alt_names

[alt_names]

DNS.1 = localhost
```

Singing webserver certificate with root ca:

```
openssl x509 -req -days 365 -in server.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out server.crt -extfile v3.ext
```

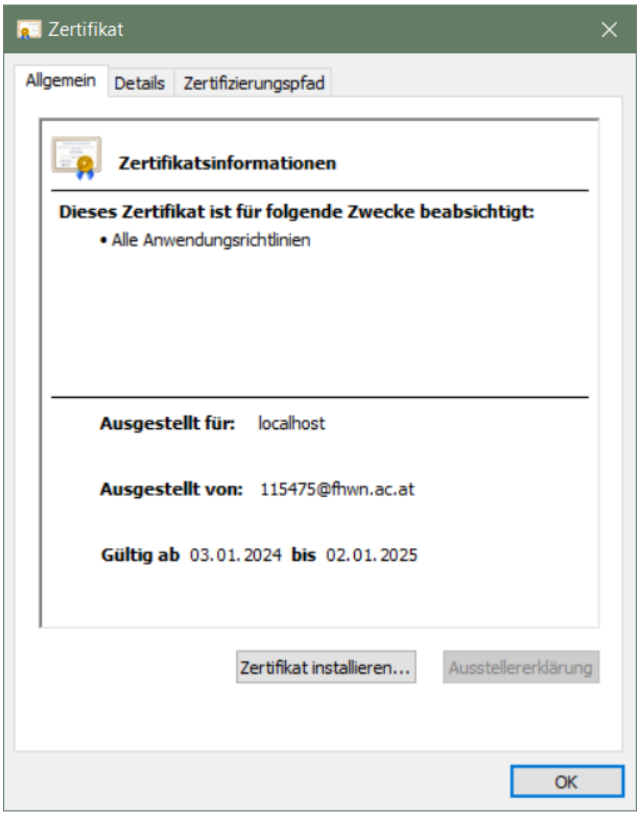
XAMPP install certificate:

Open XAMPP Control Panel

Go to Apache → Config → httpd-ssl.conf

Edit Virtual host as such:

```
<VirtualHost _default_:443>

   DocumentRoot "C:/xampp/htdocs/dashboard"

   ServerName localhost

   ServerAlias localhost

   SSLEngine on

   SSLCertificateFile "C:/Users/chris/Desktop/Fh/5.Semester/Fortgeschrittene-IT-Sicherheit/Übung3/certificates/server_certificate/server.crt"

   SSLCertificateKeyFile "C:/Users/chris/Desktop/Fh/5.Semester/Fortgeschrittene-IT-Sicherheit/Übung3/certificates/server_certificate/server.key"

</VirtualHost>
```



Zertifikatsinformationen

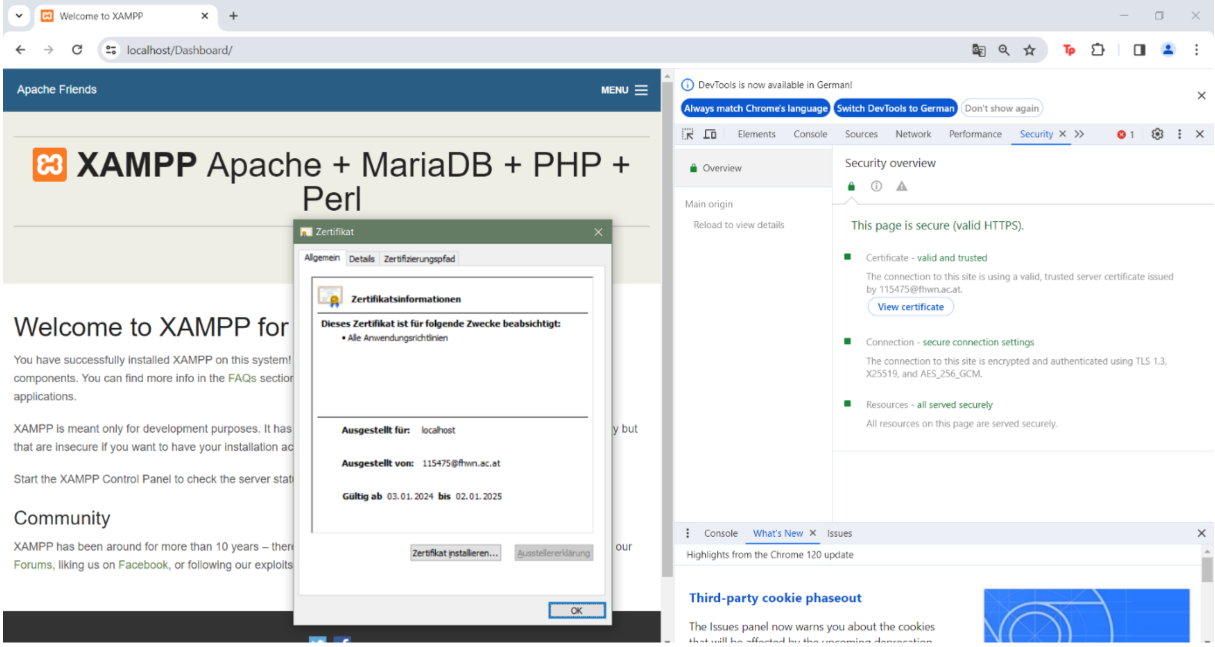
Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Alle Anwendungsrichtlinien

Ausgestellt für: localhost

Ausgestellt von: 115475@fhwn.ac.at

Gültig ab 03.01.2024 **bis** 02.01.2025



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for

You have successfully installed XAMPP on this system! components. You can find more info in the FAQs sectio applications.

XAMPP is meant only for development purposes. It has … y but that are insecure if you want to have your installation ac

Start the XAMPP Control Panel to check the server stat

Community

XAMPP has been around for more than 10 years – there … our Forums, liking us on Facebook, or following our exploits

Zertifikatsinformationen

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Alle Anwendungsrichtlinien

Ausgestellt für: localhost

Ausgestellt von: 115475@fhwn.ac.at

Gültig ab 03.01.2024 bis 02.01.2025

DevTools is now available in German!

Main origin

Reload to view details

Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by 115475@fhwn.ac.at.

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_256_GCM.

Resources - all served securely

All resources on this page are served securely.

Highlights from the Chrome 120 update

Third-party cookie phaseout

The Issues panel now warns you about the cookies