

Zertifikate verteilen

1. Stammzertifikat

“

Das Stammzertifikat muss auf alle Geräte installiert werden, von denen ihr auf euren Web Server zugreifen / browsen wollt! Es wäre deshalb ratsam euer "Zertifikatsverzeichnis" auf den jeweiligen Geräten als Laufwerk verbunden zu haben!

1.1 MAC

Kommando: "sudo security add-trusted-cert -d -r trustRoot -k
"/Library/Keychains/System.keychain" <Verzeichnis><SLD>.pem

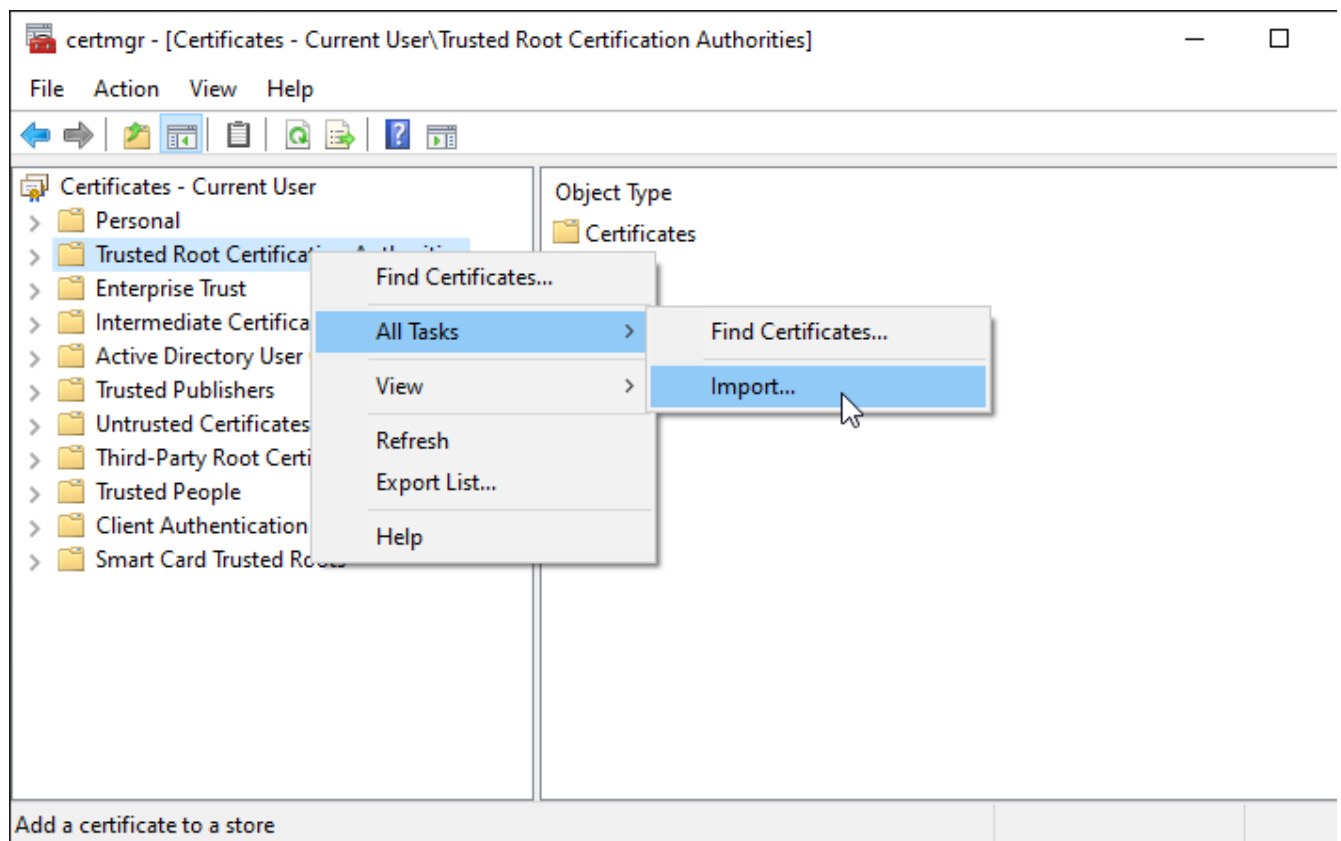
1.2 Linux

Kommando: "sudo cp <Verzeichnis><SLD>.pem /usr/local/share/ca-certificates/<SLD>.crt"

Kommando: "sudo update-ca-certificates"


1.3 Windows

Kommando: "WIN + R - Eingabe: certmgr.msc" - OK



NEXT

×

←  Certificate Import Wizard

File to Import
Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)

↖

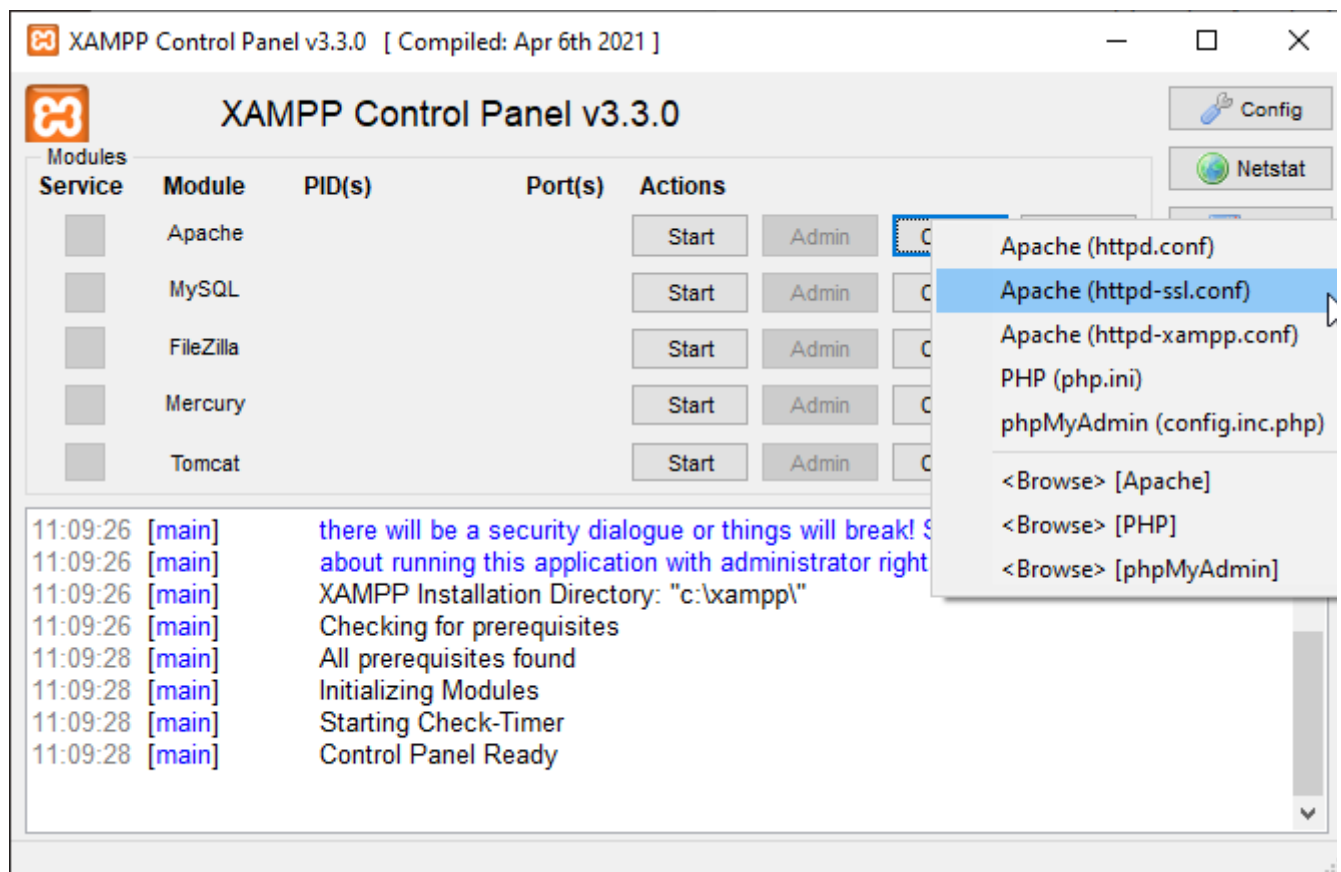
hoffe, den Rest bekommt ihr selber "zusammen geklickt" ! ☐☐

2. Web Server Zertifikat

2.1 Apache

“ Stellt bitte sicher, das ihr "a2enmod ssl" angeschaltet habt!

- geht in das Apache Verzeichnis "sites-available" und erstellt eine .conf Datei (geht natürlich auch mit der default-ssl.conf). Solltet ihr mit XAMPP den Web Server betreiben, dann:



- ändert die VirtualHost Direktive

```
<VirtualHost *:443>
    ServerName <>
    DocumentRoot <>

    SSLEngine on
    SSLCertificateFile <Verzeichnis>/<subdomäne.SLD.TLD>.crt
    SSLCertificateKeyFile <Verzeichnis>/<subdomäne.SLD.TLD>.key
</VirtualHost>
```

- Kommando: "a2ensite <der Dateiname>.conf"
- Kommando: "service apache2 restart"

“ im Fall von XAMPP Apache stoppen und wieder starten!

2.1 NGINX

```
server {
    listen          443 ssl;
    server_name     <subdomäne.SLD.TLS>;
```

```
ssl_certificate      <Verzeichnis><subdomäne.SLD.TLS>.crt;  
ssl_certificate_key  <Verzeichnis><subdomäne.SLD.TLS>.key;  
ssl_protocols        TLSv1.2 TLSv1.3;  
ssl_ciphers          HIGH:!aNULL:!MD5;  
...  
}
```

“ Jetzt habt es ihr aber geschafft!!!! ☐ Versteht bitte, das es hier um lokale Zertifikate gegangen ist und nicht wie man eine PI generiert oder wie man einen Webserver aufsetzt oder, oder, oder... Es bliebe nur noch die eigentliche Randthematik DNS Resolver übrig um das Bild abzurunden. Selbst wenn alles richtig gemacht wurde, kann es euch passieren, das eure Domäne nicht ansprechbar in euren Browsern ist.... ☐ Deshalb noch ein Abschlusskapitel DNS Resolver! Hey, und natürlich auch ein "Gutzi" fürs durchhalten. Schaut doch mal unter "Gutzi"!!!! ☐

Revision #6

Created 17 June 2025 10:31:30 by tomek

Updated 17 June 2025 12:10:29 by tomek