

Zertifikate

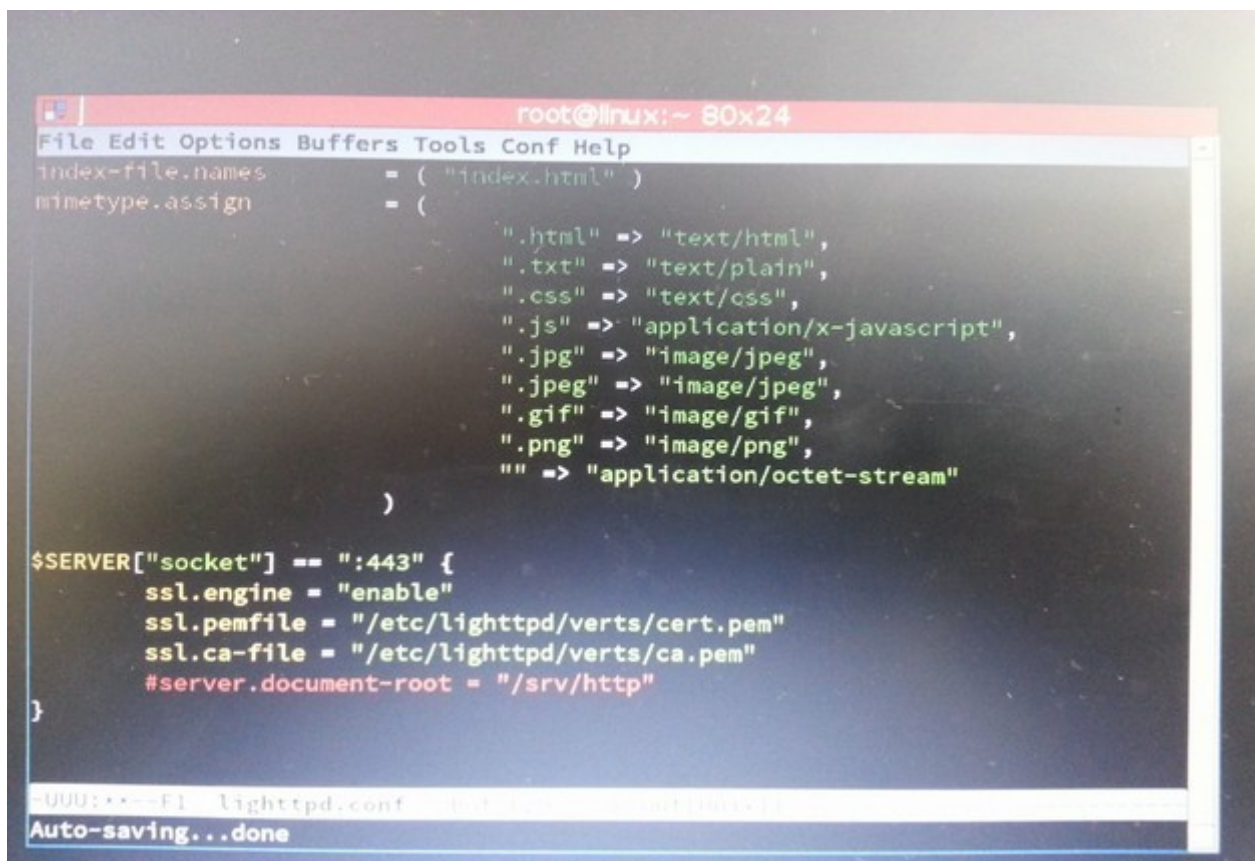
Aufgabenstellung:

- einen HTTPS-Webserver einrichten
- ein Zertifikat erstellen und von einem CA unterschreiben lassen
- die CA auf das Betriebssystem einbinden (oder bei Firefox)
- eine verschlüsselte Verbindung auf den Webserver aufbauen

1.) HTTPS-Webserver einrichten

Lighttpd (gesprochen Lighty) ist ein freier Webserver, der alle wichtigen Funktionen eines moderenen Webserver implementiert und diese (wie bei Apache) in Form von Modulen eingebindet.

Damit Lighty auf Port 443 auf HTTPS-Anfragen hört, muss erstmal die Konfigurationsdatei angepasst werden:



```
root@linux:~ 80x24
File Edit Options Buffers Tools Conf Help
index-file.names      = ( "index.html" )
mime.type.assign      = (
    ".html" => "text/html",
    ".txt"  => "text/plain",
    ".css"  => "text/css",
    ".js"   => "application/x-javascript",
    ".jpg"  => "image/jpeg",
    ".jpeg" => "image/jpeg",
    ".gif"  => "image/gif",
    ".png"  => "image/png",
    ""     => "application/octet-stream"
)

$SERVER["socket"] == ":443" {
    ssl.engine = "enable"
    ssl.pemfile = "/etc/lighttpd/verts/cert.pem"
    ssl.ca-file = "/etc/lighttpd/verts/ca.pem"
    #server.document-root = "/srv/http"
}

000:~--F1 lighttpd.conf 0.000:~--F1 lighttpd.conf 0.000:~--F1
Auto-saving...done
```

Mit dieser Konfiguration weißt Lighty genau auf welchen Port er hören soll und wo die Zertifikate liegen.

2.) Zertifikate erstellen

Wir benötigen zwei Zertifikate:

- cert.pem → das unterschriebene Zertifikat für "audio.com"
- ca.pem → die Zertifikate des CA (können mehrere Zertifikate sein; hierarchischer Aufbau)

Als aller Erstes muss ein Zertifikat erstellt werden:

```
openssl req -nodes -key -keynew rsa:2048 -o cert.pem
```

Mit diesem Befehl bekommen wir ein Zertifikat. Damit dieses Zertifikat gültig ist, muss ein vertrauenswürdiger CA das Zertifikat unterschreiben (die cert.pem Datei wurde Dominik Egretzberger gegeben, dieser hat das Zertifikat unterschrieben). Das unterschriebene Zertifikat wird vom Webserver mitgeschickt.

cert.pem: In dieser Datei enthält zwei Dinge, die der Webserver braucht → Privaten Schlüssel, damit er die Anfragen entschlüsseln kann → und das unterschriebene Zertifikat, welches der Webserver dem Client mitsendet (öffentlicher Schlüssel ist im Zertifikat enthalten)

```

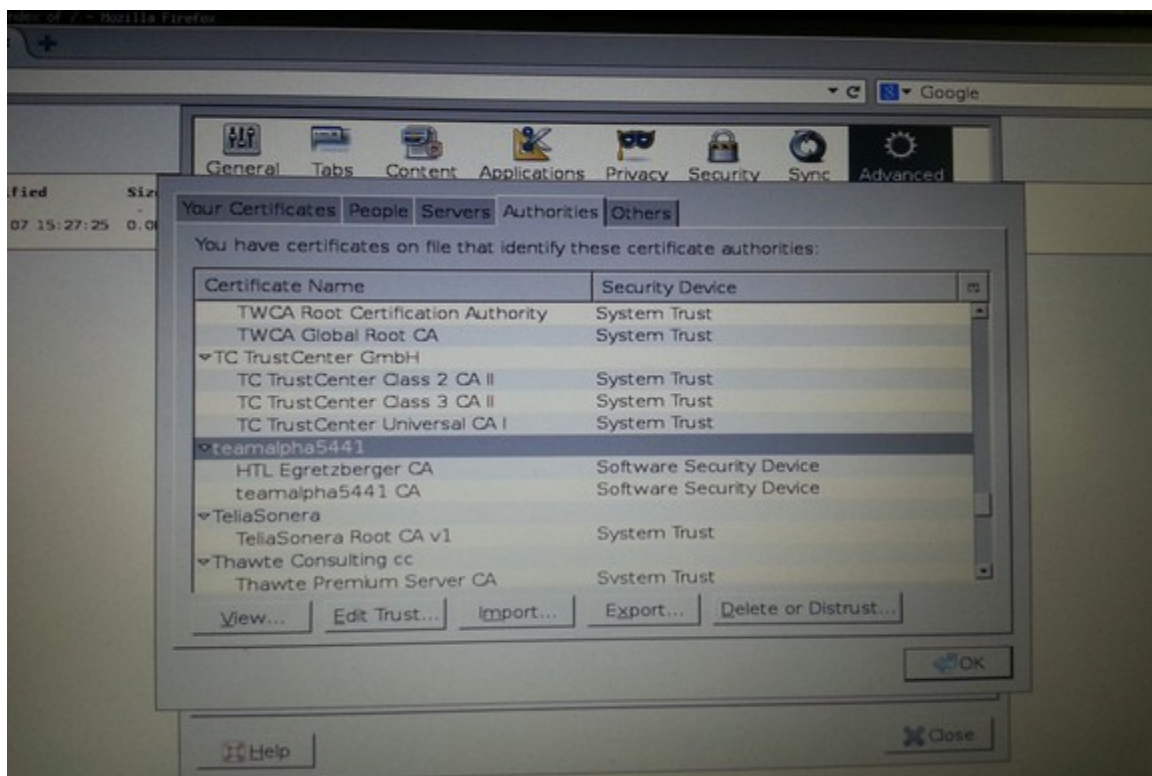
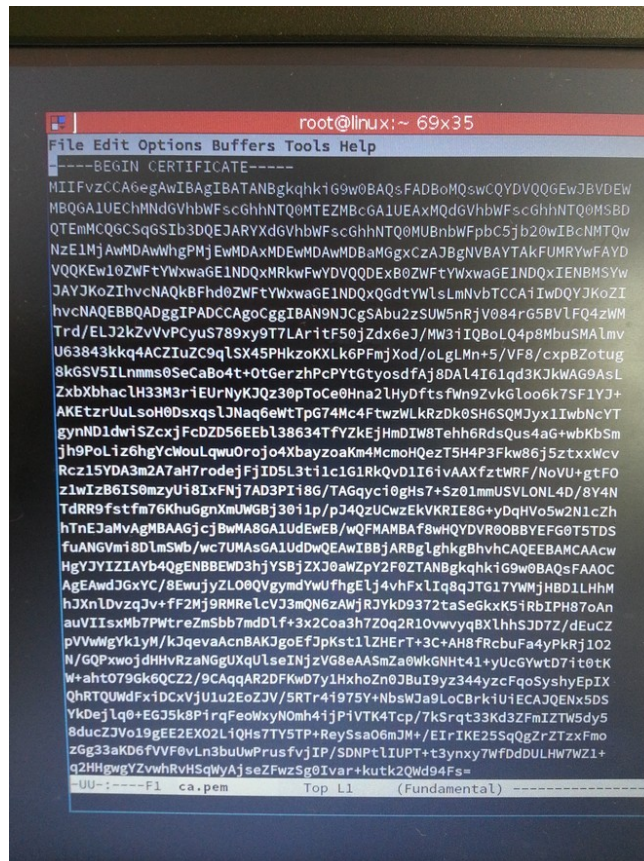
root@linux:~ 69x35
File Edit Options Buffers Tools Help
-----BEGIN PRIVATE KEY-----
MIIEVQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQQDwvjy+7p0bJ0GL
LG/ECdstvpYtgjyCwH02wHXVzV/B/jqNwr8AvIC16dJF8EdcPwsThS+St177xqta
EkKwHv2Tbpbk3TSWYIweRjtBSRnz/szF5XzIN+YvSrnUuyXFeaZ2Lrdg9ea0/3o0R
rIY2VNPWphuiEx++hygEsV3U0FsezWN6Y0ao8JZqPgNB1FEr/oVI8Hv2La4/497/
W/USA+mcL/ZL7EgWS0LfKz/6x6dGGKQp1fo3JuWC0LYvzPhjIsPhAFqgm4+j67YN
LW4EDMe6fATZdILPE/3X9Dj8PVMSB7aHAZgPaypnYkAI4a+6g49CG8zLNB1yNLq7
hnYJRKCzAgMBAACgEAGlnZxmwPLt32cYoKNwA6tkaQJdcqYbIELELnsuCywXFa
6g5dtc9r0+bPYLmtaAo5W3nabpyF8Ut9t13KQgK1MuQ9d0XInGVkBl6J/a6cpBvv
FD+00rbG16HQy174xGcdaAh7IoAN3FP0t5h+FBmurQZRGcBTauQ+6uSA6R5wMAU2
YpaemwpKXWdEL20ZuSAG2R0/Le0tTEL4AMwii/xqeaZvYKvkh01P3U0J5FgRJETa
rEn/oCxLeaDdMQBcGRuPjgdrkxCTw8KC2JN8ZT8oKRP1BEAAA4aRHLdytGxSm
DI/JITE0Z20Mu9yMtm66yPUXrhBA57FrTSLBmfCWQBgQ07esuIfzHaWe+itgg6
EieGpiIEbEaw7k/e3kRFdxRqyYtEq2wQdmubSUAp2eGPTIw5NLm47hK8Z2GUQB
R+zqVBshIkzHbx8JfDAQxhUEy54Vm+crwUWVYmDyzyHho2p8rHZDDt1jFebkfU/
+IVw0GH4mFPxU0a3CBIgp4R8YwKBgQDammVYX1K2eIhRbqaSSXhCyILE5z7geYw2
1kf+gJOEpYkUR537FLeJp2K/VvYx20/JX2z9a0be48ZiWcdpBpC7hmA0136lmt8
Krs8phhQunLT4kupag48Wf3yTLuPuUrf73xZby/IcdHIQ5UWEbhoPUoTWMbwqyt
B31r05YzcQKBgQDoL6cOHsoln5/43fLYkvx1gJw10yK/YG1AaWMNWE608LSZrT46
Y4JBXrpKTVFu8AHJ/3DWmc0zLvStA4TbXeorLH5J6ERVe06Adm32frzXUZXivTAC
IQ8Awy3lp1b7lkrj15VHhdkkhfChTXDPoIirNRCzswkF7mpwiJoaddjCHawKBgH7f
JPqJOGQWYgcapSo54cZAwUSUQVver3YUu2yi/Gt8ZTEms1w+mEm+d6j3KptB/a4u
gCo2iYhvybL5DuQxHdzCe6K9CcoqCu/hjRHC8GGQXehfELKejuyP/kbnG1Tq4W7H
c57/CMh45pxjRsffOQaPMWkMoPK3pag2tJ/L0XzBAoGAXXgKSLqH6UEJmrtYFOxP
x1YR9ws9njKLiOXfsjjuDF90w3nnio+Up8DFV/JBRrb2hstLG7WtdGK3vuTy4lQf
gkQch2ud3GaeAn4TmBsrXlHBowI4uqg3Kaggopwbv50u0m56ps0T47oHNC01xz
tPi0AzN0545uJ4TG4td/oe4=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEYjCCAkqgAwIBAgIBc3ANBgkqhkiG9w0BAQ0FADBTMwswCQYDVQQGEwJBVDEc
MIIEGA1UEAxMTSFRMIIEVncmV0emJlcmdlc1BDQTEuMkQwQ0Q0Q0Q0Q0Q0Q0Q0Q0
bWfscGhhNTQ0MUBnbWfPbC5jb20wHhcNMTEyMDk0OTAwHhcNMTEyMDk0OTAwHh
-UU-;-----F1 cert.pem Top L1 (Fundamental)

```

13.01.2015

Alin Porcic

ca.pem: Damit der Firefox das Zertifikat akzeptiert, muss das CA-Zertifikat in Firefox eingebunden werden:

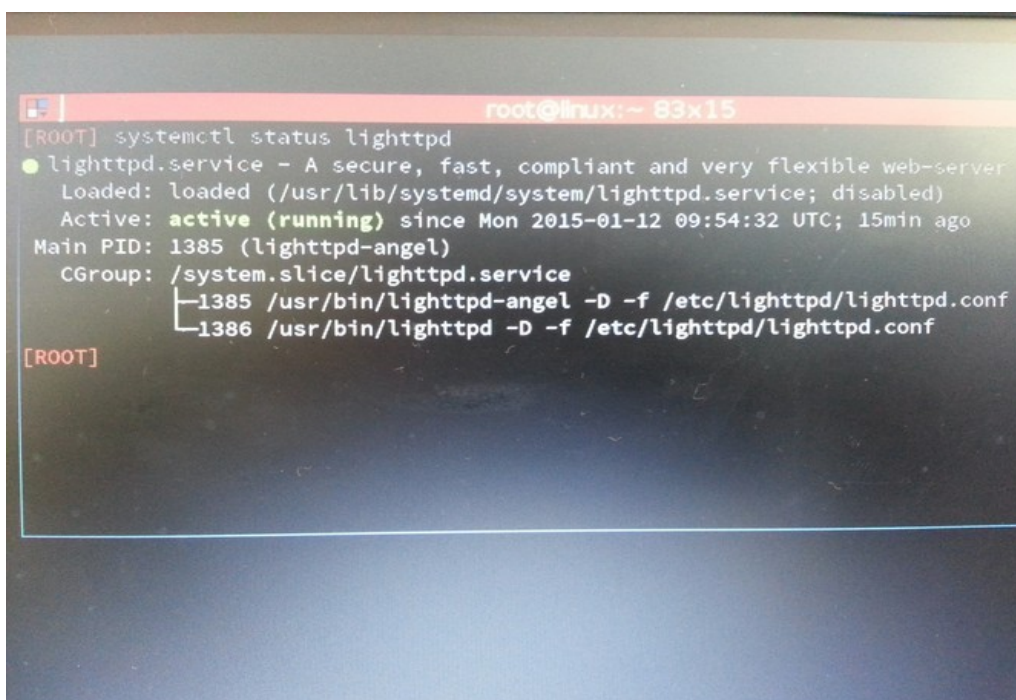


3.) Verbindung aufbauen

Im Feld “common name” muss eine vollständige Adresse angegeben werden, da ein Zertifikat nur für eine Adresse gültig ist. Unsere Adresse lautet “audio.com”.

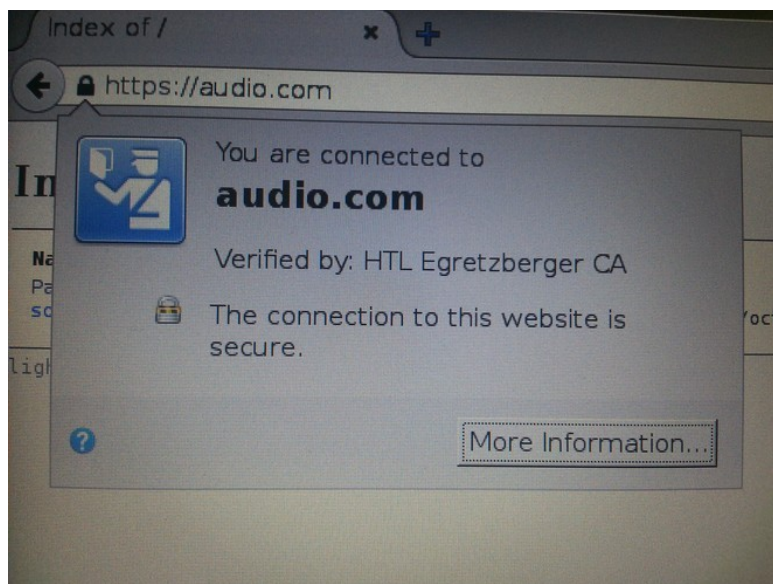
Wir haben einen Eintrag in der /etc/hosts angelegt damit der DNS “audio.com” auf localhost auflöst.

Webserver starten:



```
root@linux:~ 83x15
[ROOT] systemctl status lighttpd
● lighttpd.service - A secure, fast, compliant and very flexible web-server
   Loaded: loaded (/usr/lib/systemd/system/lighttpd.service; disabled)
   Active: active (running) since Mon 2015-01-12 09:54:32 UTC; 15min ago
 Main PID: 1385 (lighttpd-angel)
    CGroup: /system.slice/lighttpd.service
           └─1385 /usr/bin/lighttpd-angel -D -f /etc/lighttpd/lighttpd.conf
             1386 /usr/bin/lighttpd -D -f /etc/lighttpd/lighttpd.conf
[ROOT]
```

Nun “<https://audio.com>” aufrufen:



13.01.2015

Alin Porcic

Firefox akzeptiert die Verbindung, da das “audio.com”-Zertifikat von Egretzberger unterschrieben worden ist und dieser wurde in den vertrauenswürdigen Cas eingetragen.

