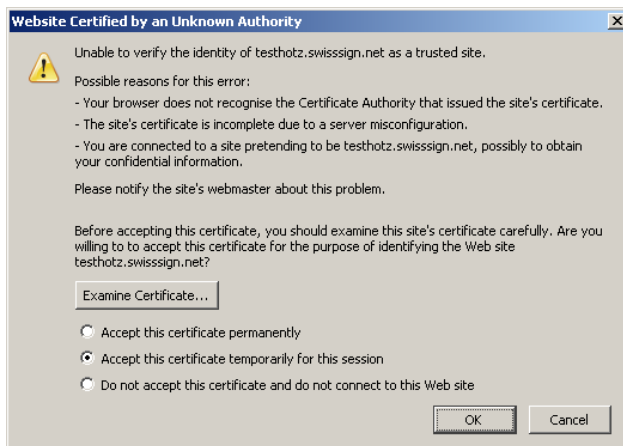


How to: Apache Konfiguration mit SSL Zertifikaten

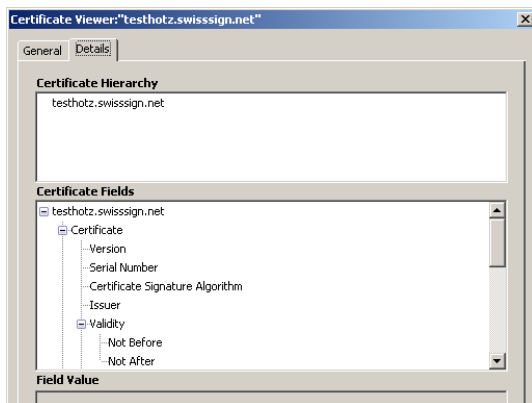
Einige Kunden haben SSL Zertifikate bezogen und fragten uns, warum diese Zertifikate von den Clients als nicht vertrauenswürdig eingestuft werden. Die Root Zertifikate (Platinum CA – G2, Gold CA – G2 und Silver CA – G2) sind ja in den gängigen Browsern installiert.

Folgende Fehlermeldung erscheint beim Client, wenn er auf eine SSL verschlüsselte Webseite verbinden möchte:



Dies ist so, da der Client nur den SwissSign Root Zertifikaten (zB. Silver CA – G2) und nicht der Issuing CA unseres Zertifikats (Server Silver CA –G2) vertraut.

Bei der Ansicht des Zertifikates sieht man, dass die Verbindung zum Root Zertifikat fehlt.



Damit der Client dem Server Zertifikat vertrauen kann, muss der Webserver dem Client die ganze Zertifikatskette bis zum vertrauenswürdigen Root Zertifikat mitteilen.

Dies kann unter Apache mit folgender Konfiguration gelöst werden:

Die Virtual Host Konfiguration

Beispiel eines Virtual Hosts unter Apache2: (/etc/apache2/sites-enabled/default)

```
NameVirtualHost *:443
<VirtualHost *:443>
...
SSLEngine on
SSLCertificateFile /etc/ssl/certs/test.crt
SSLCertificateKeyFile /etc/ssl/private/test.key
SSLCertificateChainFile /etc/ssl/certs/chain.crt
...
</VirtualHost>
```

Das Certificate Chain File

Das **SSLCertificateChainFile** muss die ganze Zertifikatskette enthalten (PEM codiert) beginnend mit dem lokalen Zertifikat bis zum Root Zertifikat.

Beispiel eines Chain File's: (/etc/ssl/certs/chain.crt)

```
Bag Attributes
  localKeyID: xx xx xx
subject=/C=CH/O=Test AG/CN=test.domain.ch
issuer=/C=CH/O=SwissSign AG/CN=SwissSign Server Silver CA - G2
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Bag Attributes
  localKeyID: xx xx xx
subject=/C=CH/O=SwissSign AG/CN=SwissSign Server Silver CA - G2
issuer=/C=CH/O=SwissSign AG/CN=SwissSign Silver CA - G2
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Bag Attributes
  localKeyID: xx xx xx
subject=/C=CH/O=SwissSign AG/CN=SwissSign Silver CA - G2
issuer=/C=CH/O=SwissSign AG/CN=SwissSign Silver CA - G2
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

Danach wird keine Fehlermeldung mehr erscheinen und bei der Ansicht des Zertifikates sieht man die ganze Zertifikatskette:

