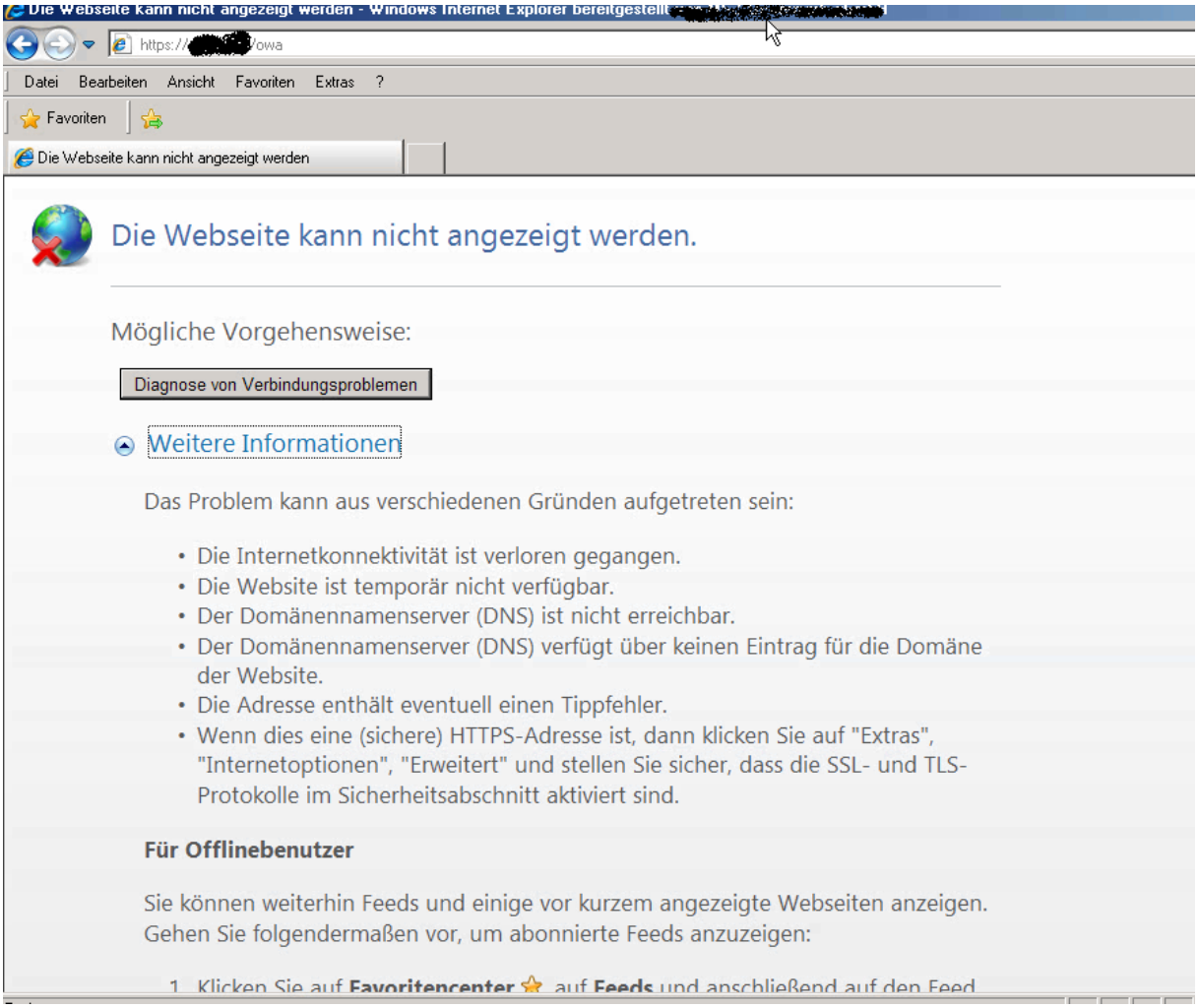
Fehlermeldung beim Aufruf einer SSL Webseite

Beim Aufruf von Outlook Web Access von einem Client erscheint folgende Fehlermeldung:



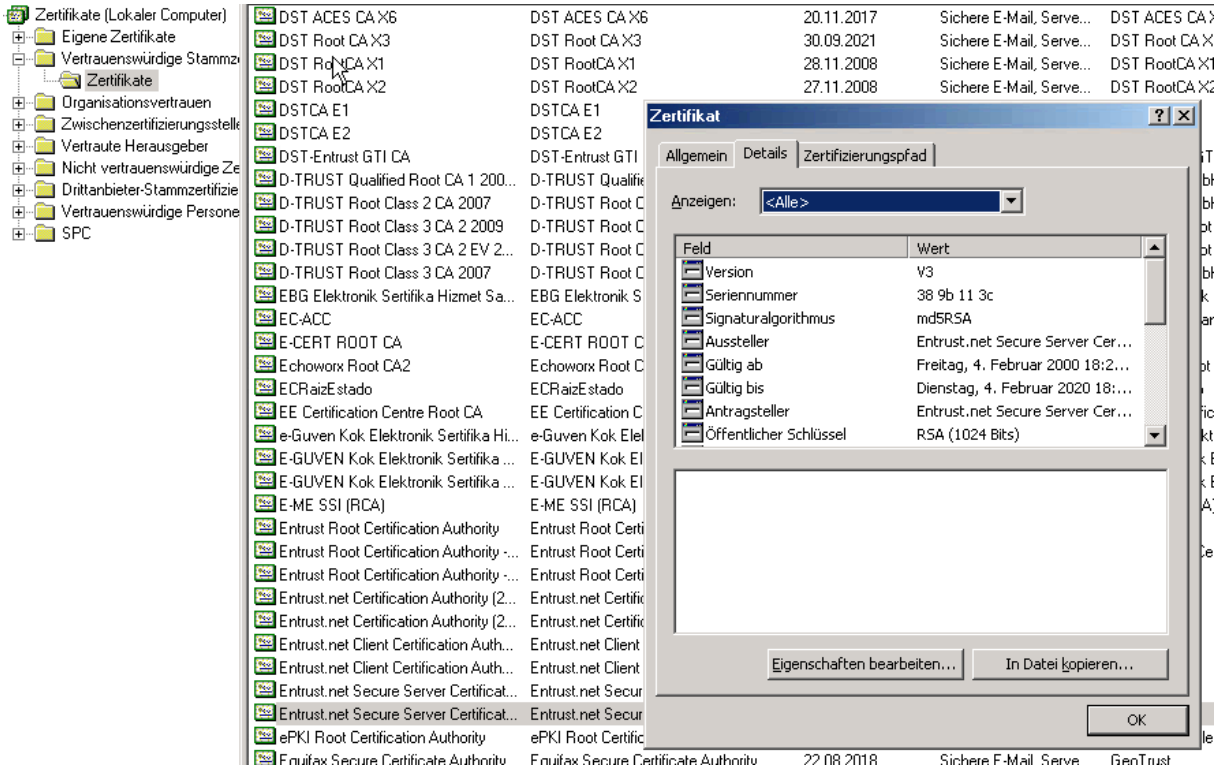
Auf einem Windows Vista / Windows 7 Client gibt das CAPI Logging weitere Hinweise, dass das Zertifikat nicht verwendet werden kann:
http://www.entrust.net/knowledge-base/technote.cfm?tn=8165

Eine kurze Recherche im Internet ergab:
https://support.comodo.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1427

Extrakt:

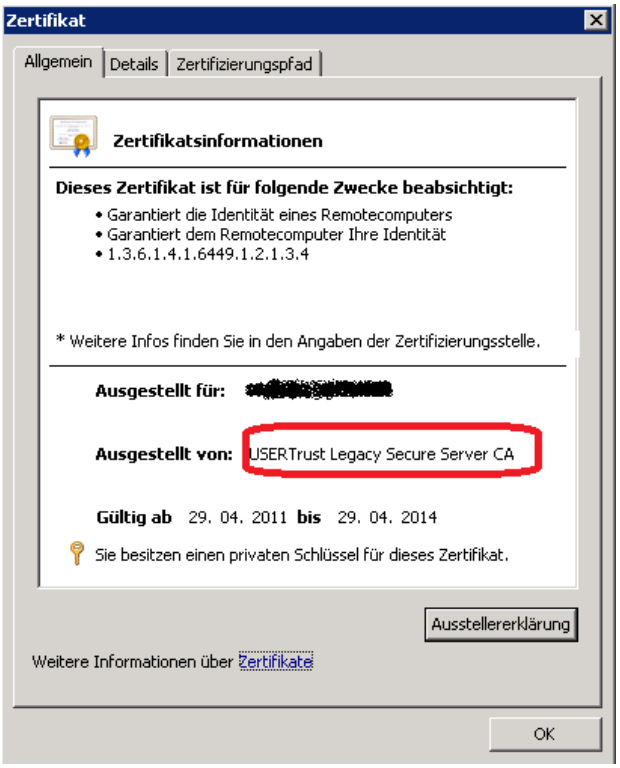
“Comodo have already stopped the issuance of certificates that use 'small' keys (generally defined as RSA keys of a size less than 2048-bit).
All of the root CA and issuing CA certificates directly controlled by Comodo are of at least 2048-bit size.
The industry deadline for the deprecation of these small keys has passed on 31-December-2013 and as of 11-March-2014 *Entrust.net Secure Server Certification Authority* has been removed from the Microsoft root program for Authenticating Servers”

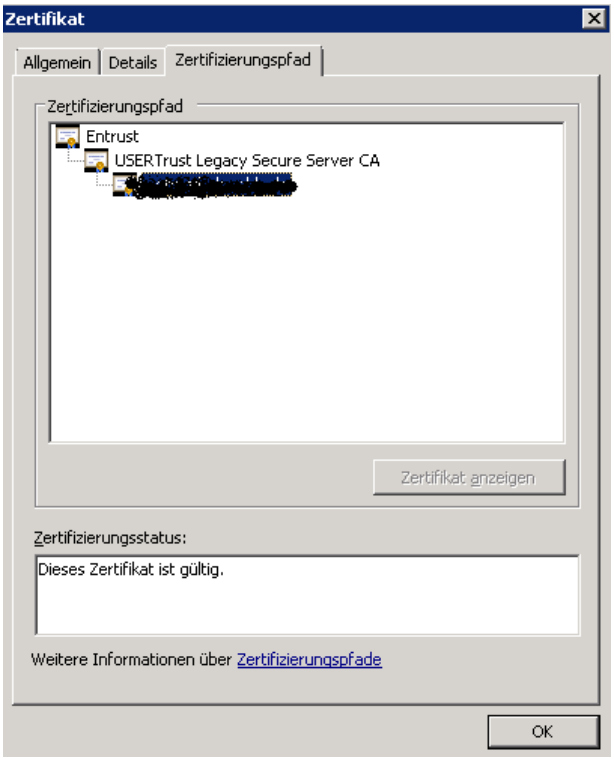
Eine Ueberpruefung des Zertifkatspeicher der vertrauenswuerdigen Stammzertifizierungsstellen auf den betroffenen Clients ergibt:



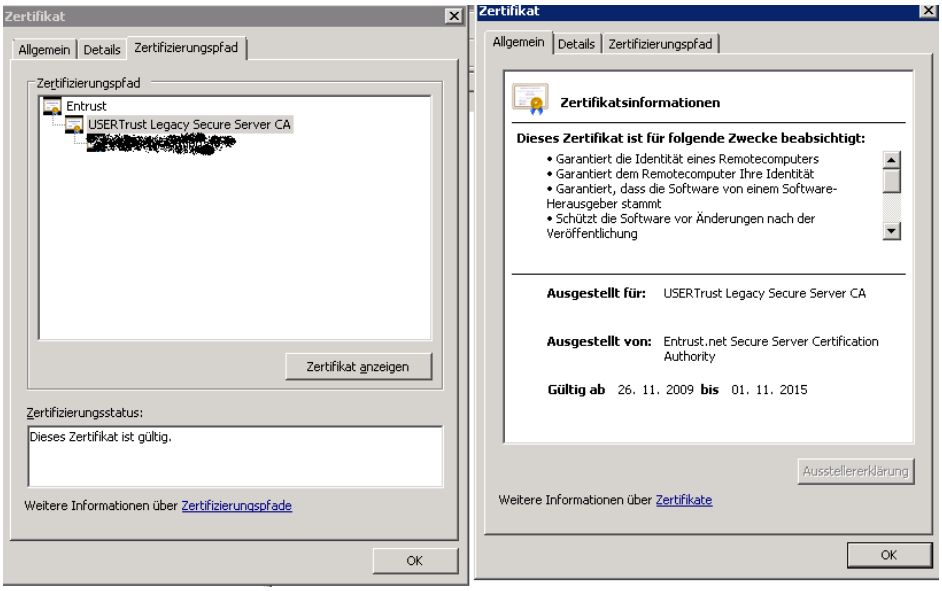
Die Webseite laesst sich mit Firefox problemlos oeffnen, da Firefox nicht den Zertifikatspeicher von Windows verwendet.

In den Eigenschaften des Zertifikats sieht man den Aussteller:

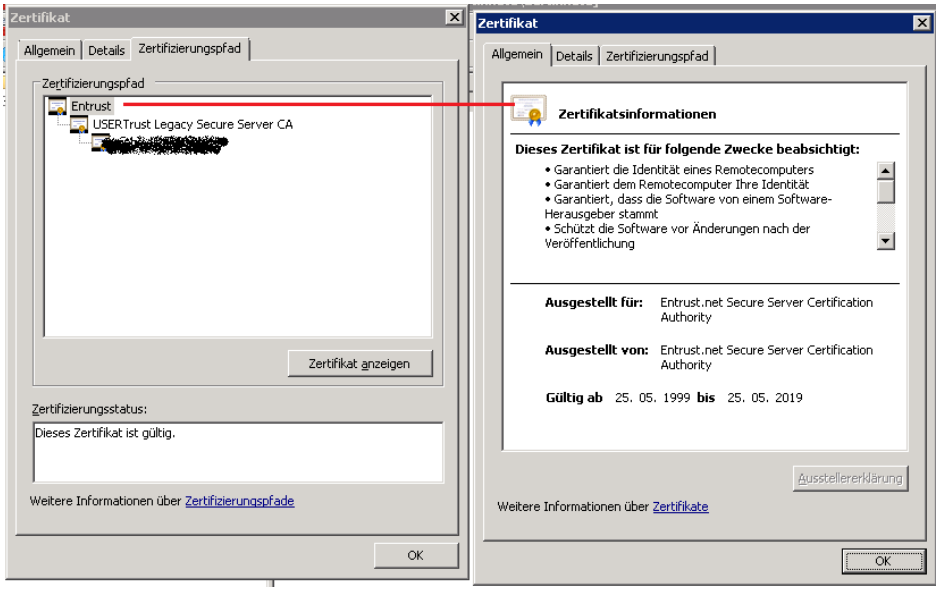




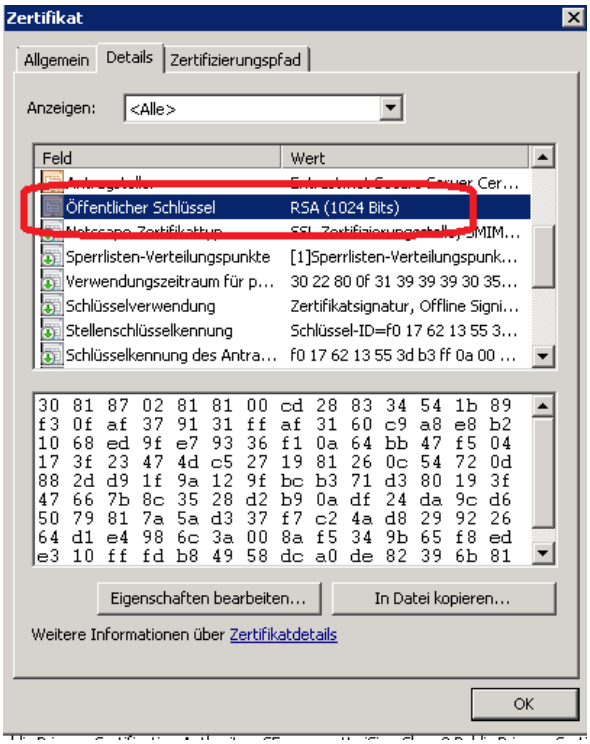
Intermediate CA ist USERTrust Legacy Secure Server CA



Root CA ist:



Das CA Zertifikat hat eine Schluessel Laenge von 1.024 Bit.

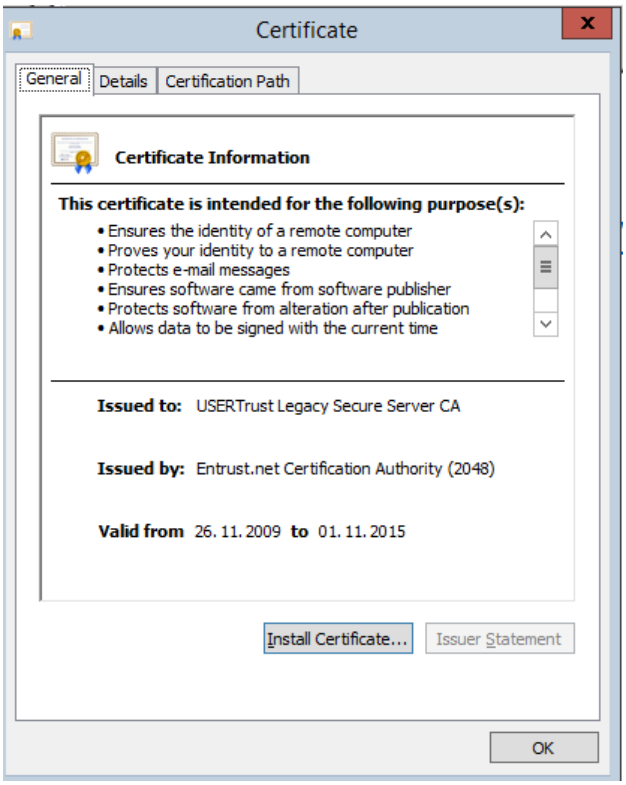


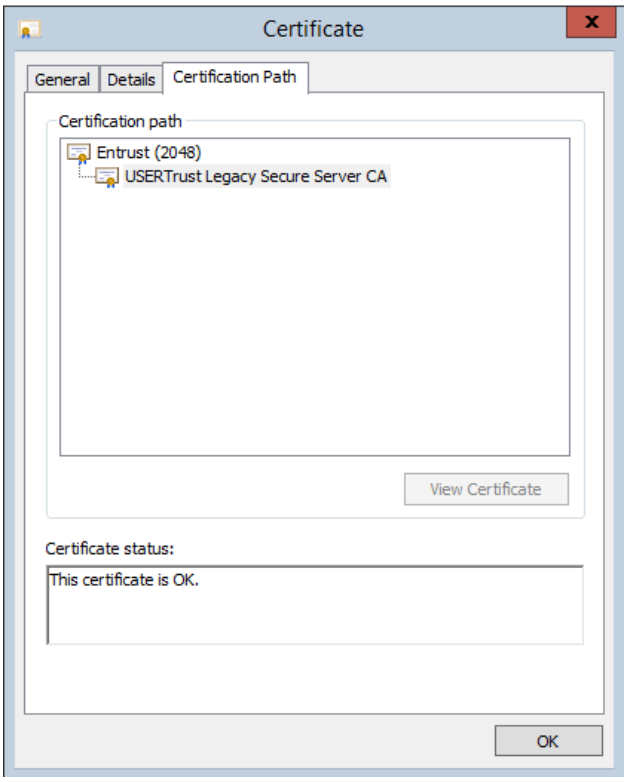
Comodo schreibt dazu in seiner Knowledge Base:

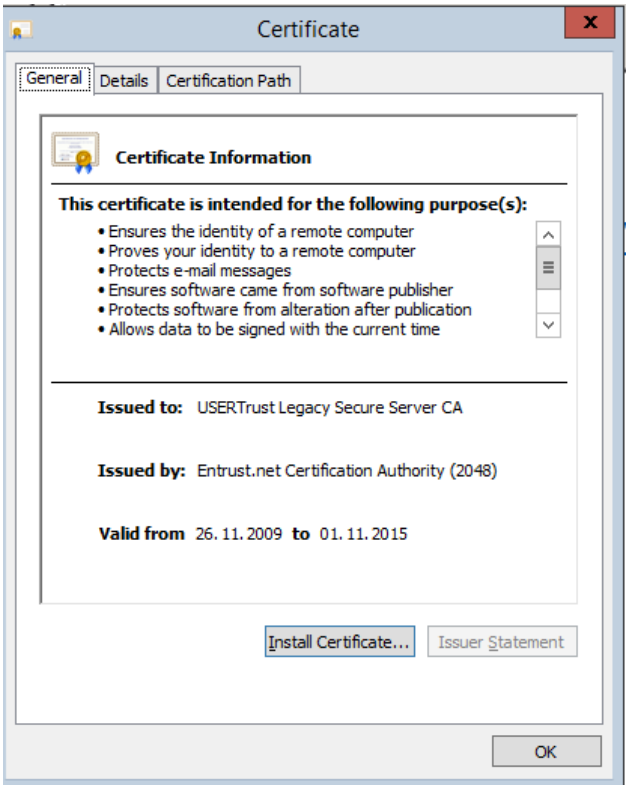
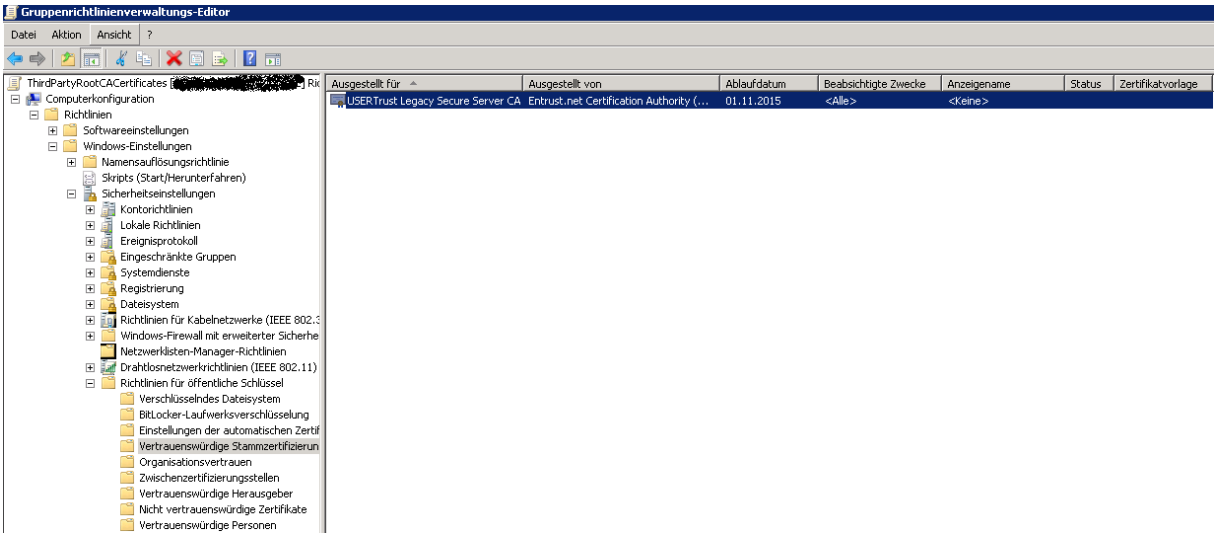
https://support.comodo.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1427

Das Problem betrifft alle Clients, welche ueber Windows Update ein Update des Microsoft Root CA Programm erhalten haben, da das *Entrust.net Secure Server Certification Authority* am 11.03.2014 aus dem Programm entfernt wurde.

Loesung: Neues Intermediate CA Zertifikat downloaden und auf den Exchange Servern bzw. den Firewalls / Reverse Proxy installieren und das alte Intermediate Certificate loeschen. Damit alle Clients das neue Intermediate Certificate haben, kann das neue Certificate auch auf allen Clients eingespielt werden, z. B. mit Hilfe von Gruppenrichtlinien.







Um fuer alle Computer welches Mitglied der Active Directory Gesamtstruktur sind das Zertifikat zu verteilen, kann eine Gruppenrichtlinie verwendet werden.