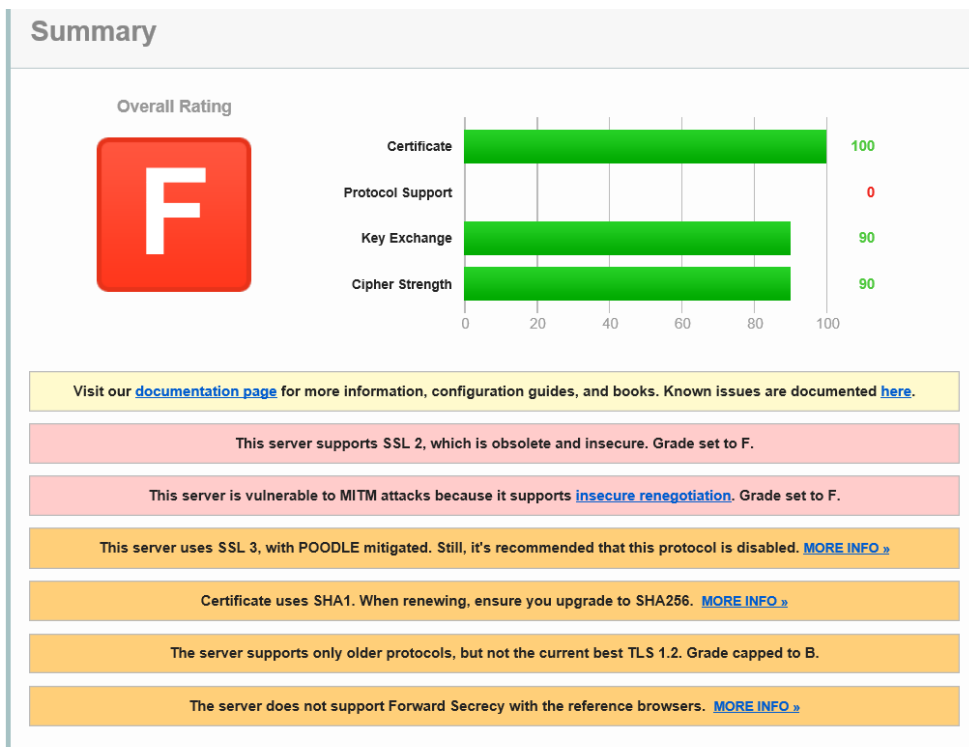
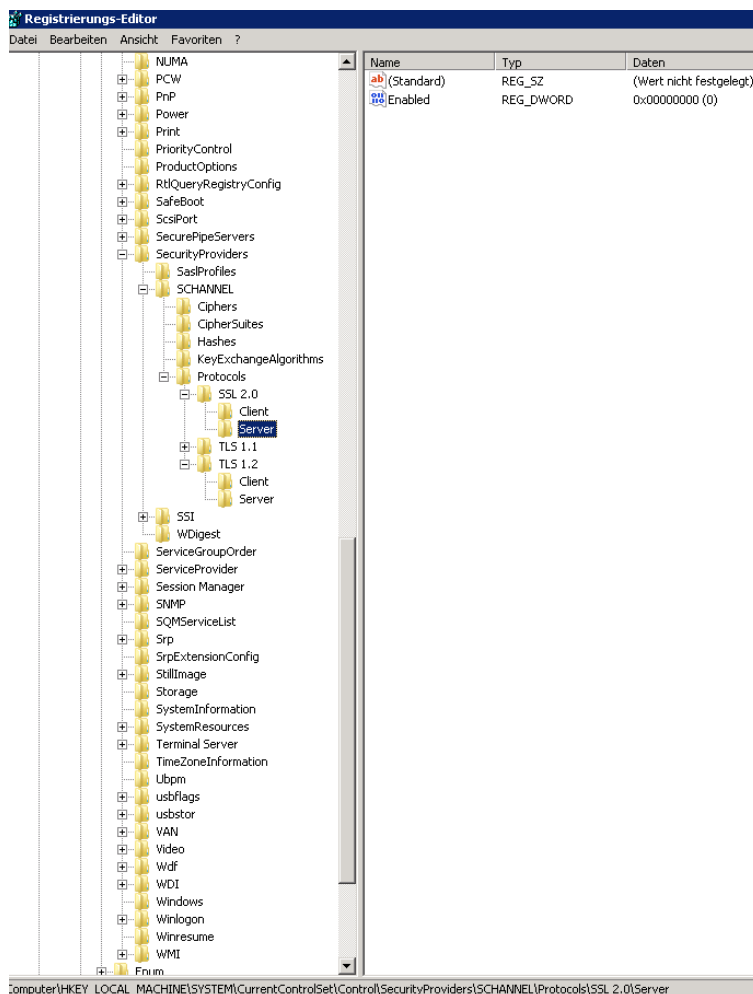


SSL Test Forefront TMG



SSL 2.0 fuer den Server deaktivieren

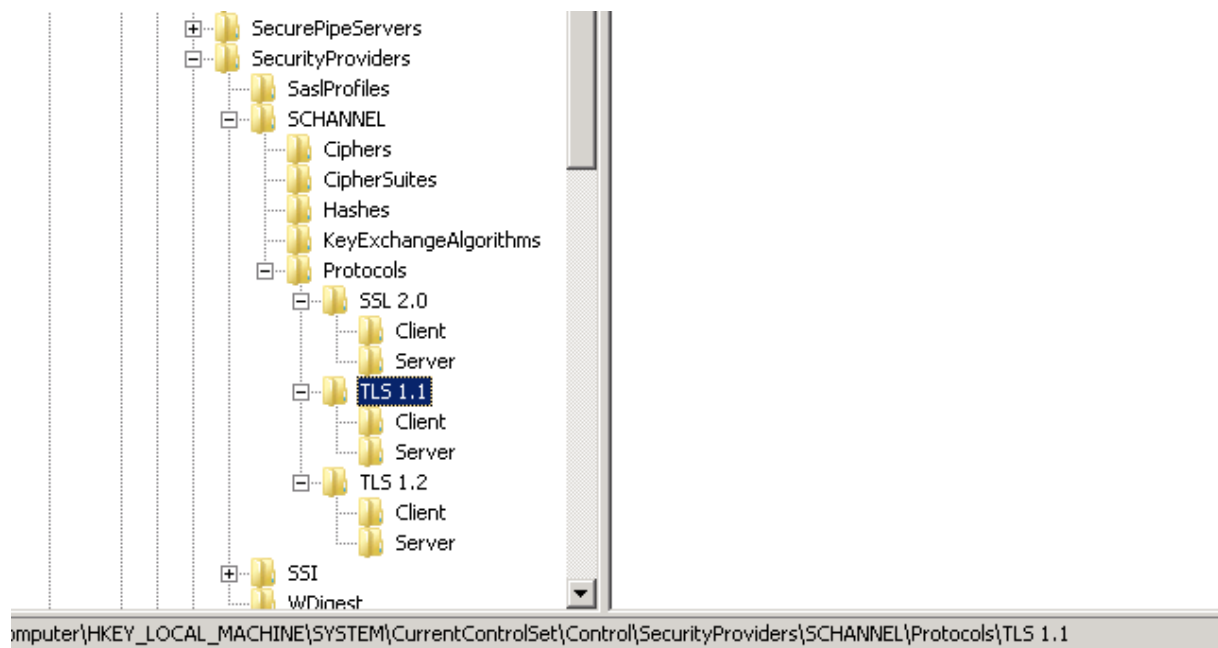


Weak Negotiation deaktivieren

Weak Negotiation fuer Server deaktivieren



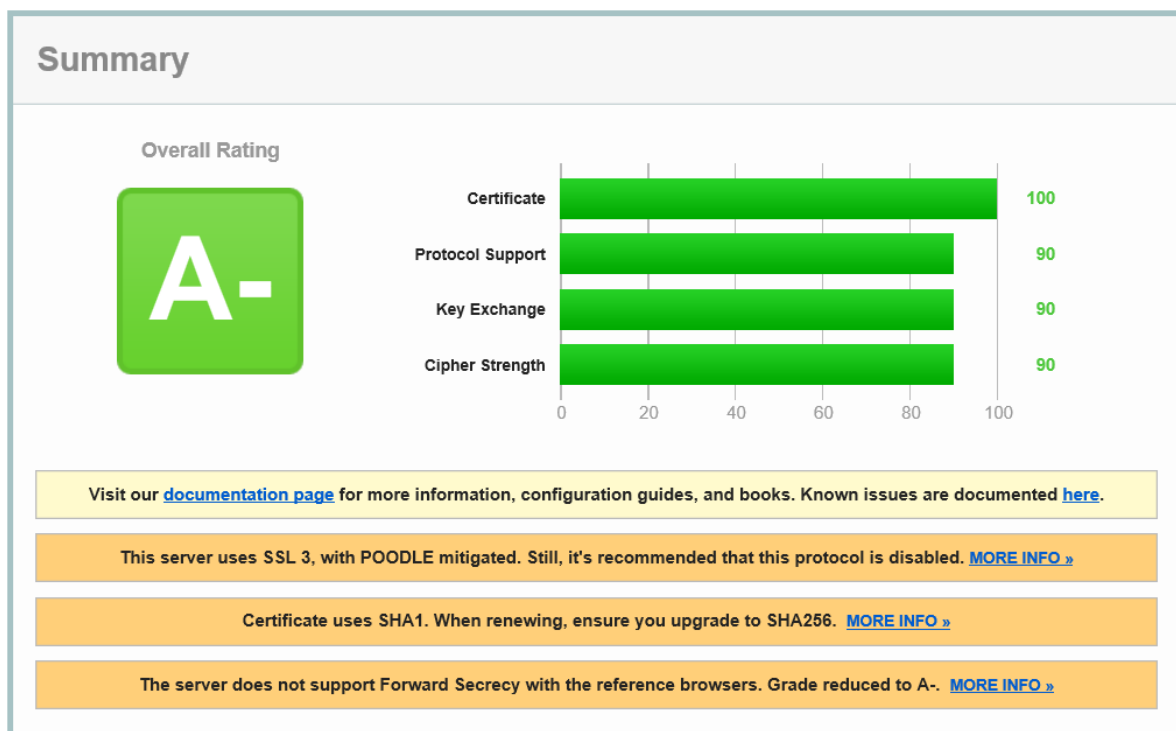
TLS 1.1 und TLS 1.2 aktivieren



Eintraege

Name	Type	Data
ab(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)

Server booten



Details

Issuer	VeriSign Class 3 Secure Server CA - G3
Signature algorithm	SHA1withRSA WEAK

Das werden wir nicht aendern koennen. TMG bzw. Windows Server 2008 R2 unterstuetzt kein SHA2 (CNG)

TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2	No

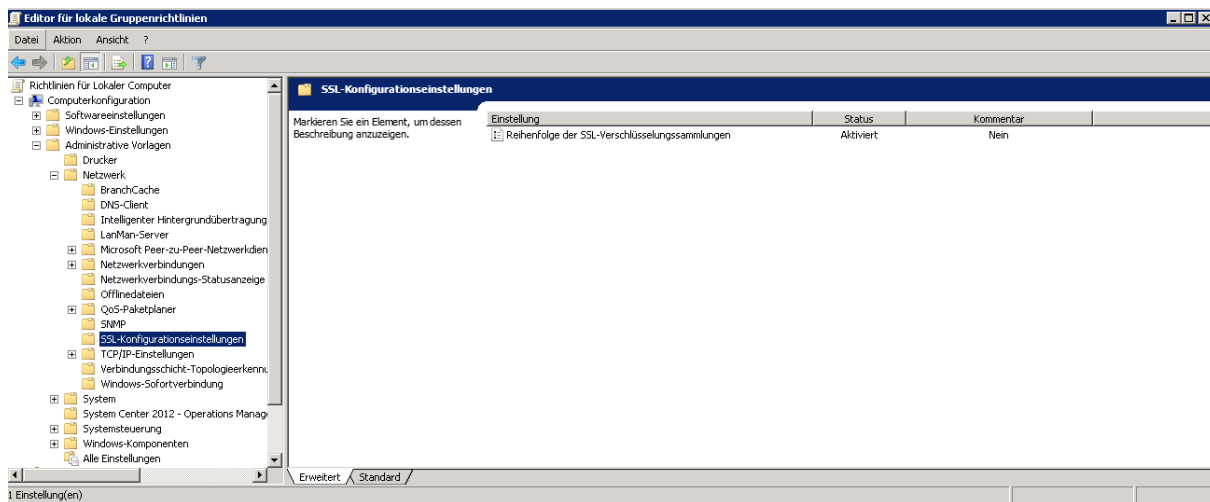
Diese Clients koennen jetzt NICHT mehr zugreifen

Google Chrome 28.0.1500.97	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
IE 6 / XP	No FS ¹	No SNI ²	Protocol or cipher suite mismatch	Fail ³
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 8 / XP	No FS ¹	No SNI ²	Protocol or cipher suite mismatch	Fail ³
Opera SSL 1.0.111	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	No FS	128
Safari 5.1.9 / OS X 10.6.8			Protocol or cipher suite mismatch	Fail ³
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	No FS	128

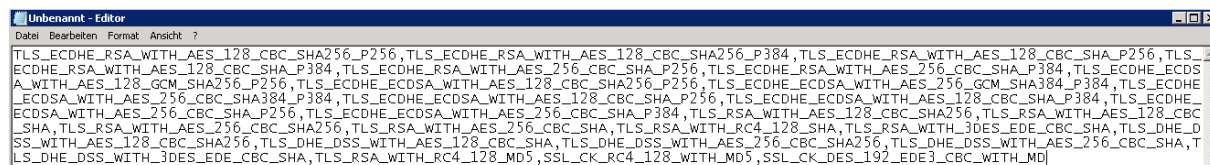
Forward Secrecy aktivieren

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. [MORE INFO »](#)

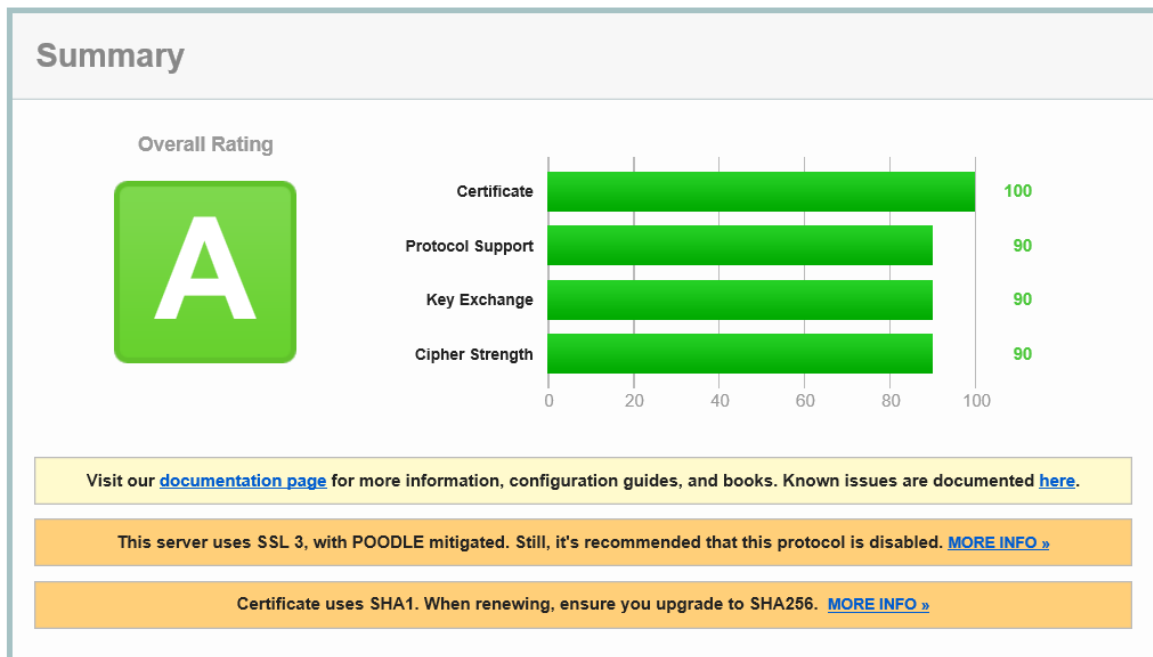
Cipher Suites anpassen



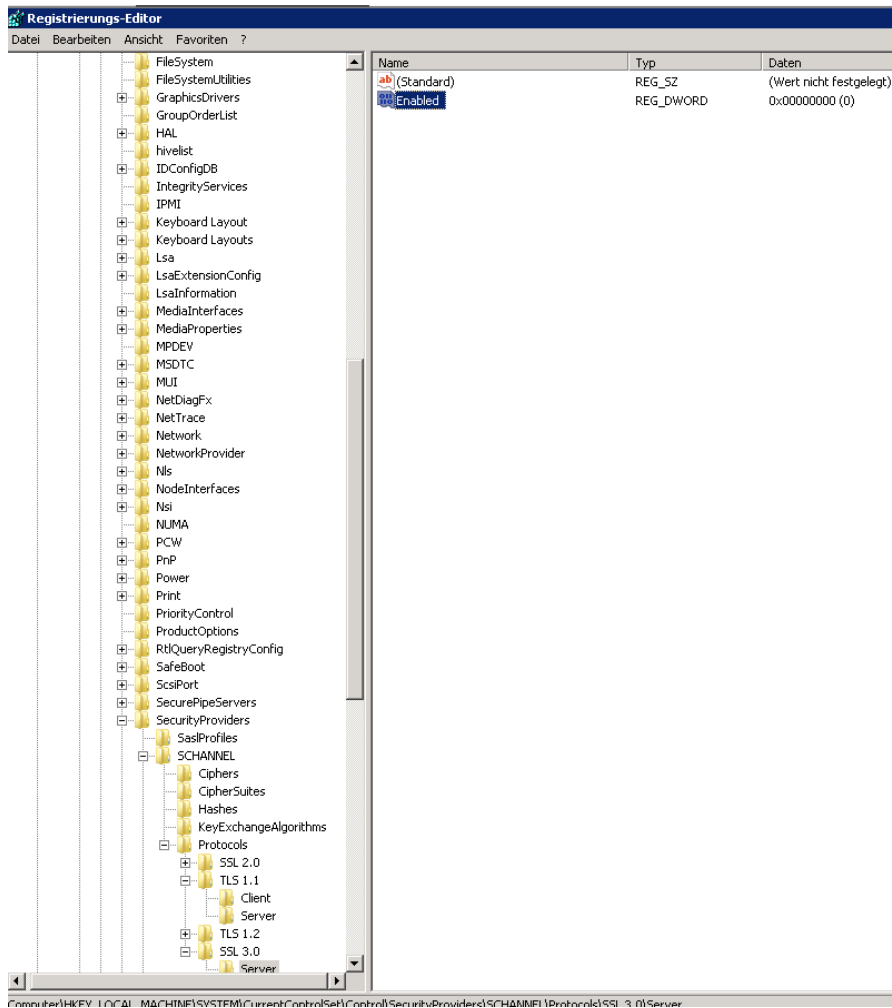
Alle Cipher Suites beginnend mit TLS_ECDHE* nach oben stellen



Besser



Jetzt den Pudel aeeh POODLE noch beseitigen



Great ...

Summary

Overall Rating

A

Certificate	<div style="background-color: #27ae60; height: 15px; width: 100%;"></div>	100
Protocol Support	<div style="background-color: #27ae60; height: 15px; width: 95%;"></div>	95
Key Exchange	<div style="background-color: #27ae60; height: 15px; width: 90%;"></div>	90
Cipher Strength	<div style="background-color: #27ae60; height: 15px; width: 90%;"></div>	90

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

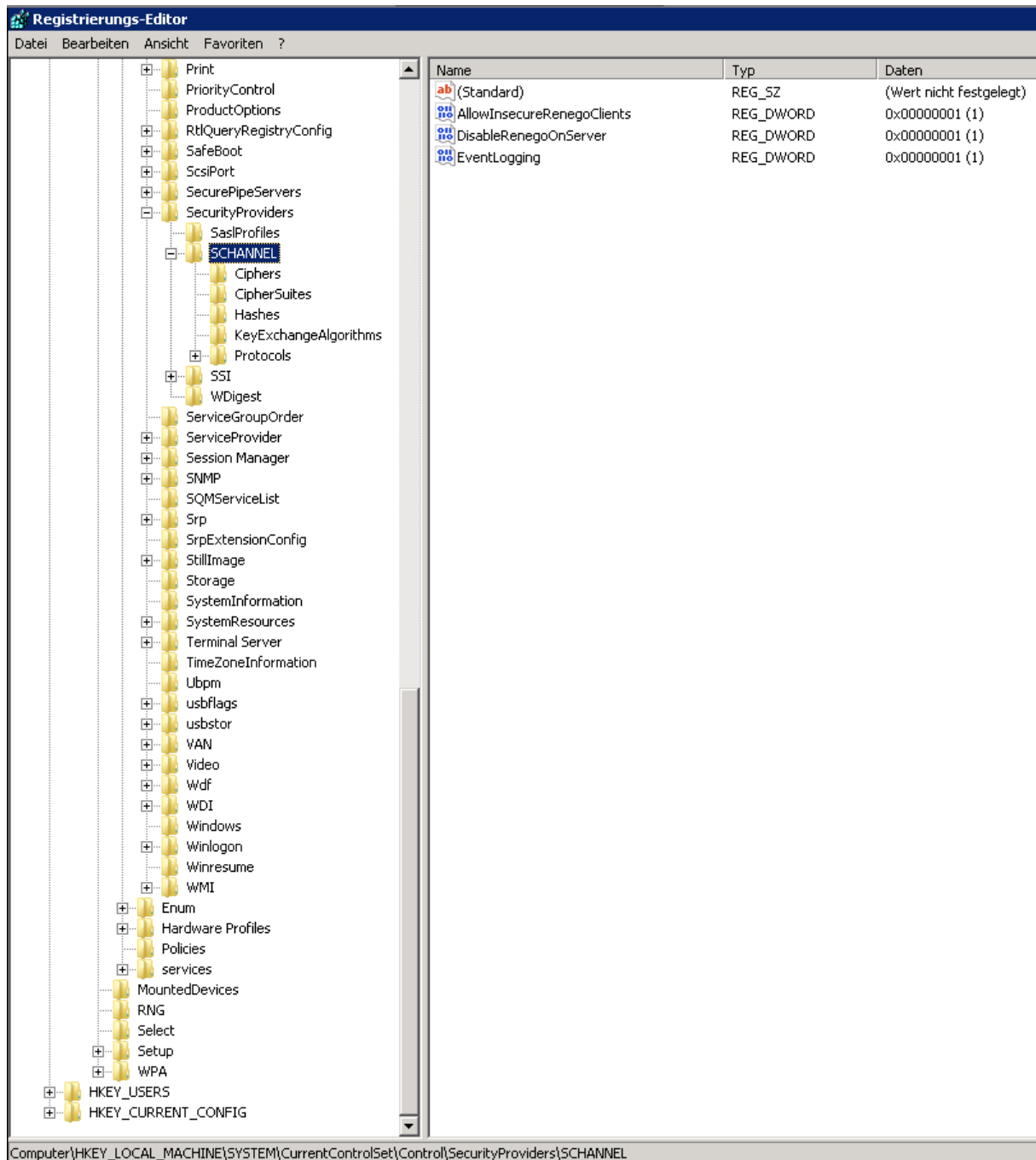
Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. [MORE INFO »](#)

This server is not vulnerable to the POODLE attack because it doesn't support SSL 3. [MORE INFO »](#)

Und danach oder zwischen den Aenderungen das Testen nicht vergessen!

Nachtrag: Outlook 2011 fuer MAC hat mit diesen Einstellungen auf einem aktuelle Apple OS Probleme.

SSL 3 kann aus sein, aber AllowInsecureRenegoClients muss aktiviert sein



The screenshot shows the Windows Registry Editor with the following registry values:

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
AllowInsecureRenegoClients	REG_DWORD	0x00000001 (1)
DisableRenegoOnServer	REG_DWORD	0x00000001 (1)
EventLogging	REG_DWORD	0x00000001 (1)

Path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL