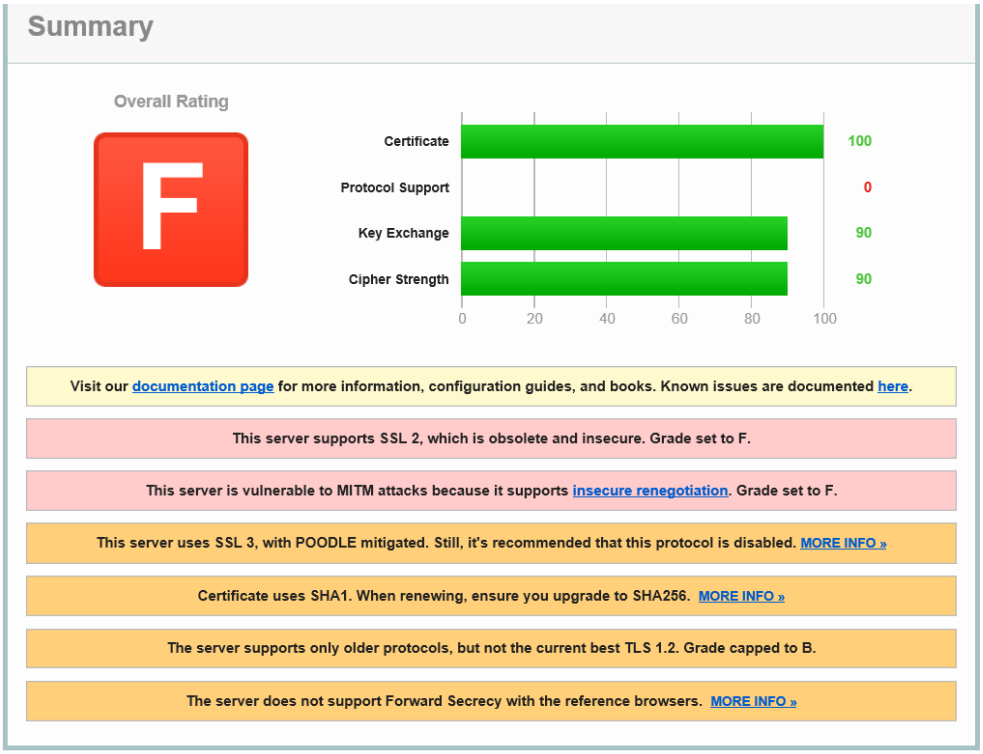
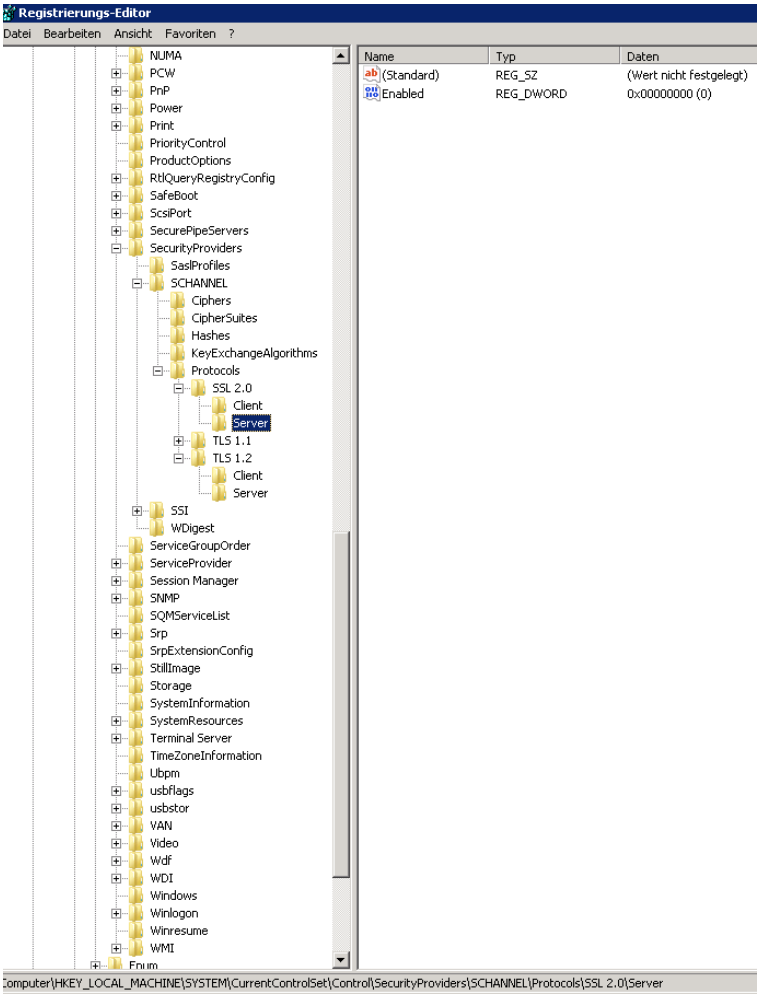
SSL Test Forefront TMG

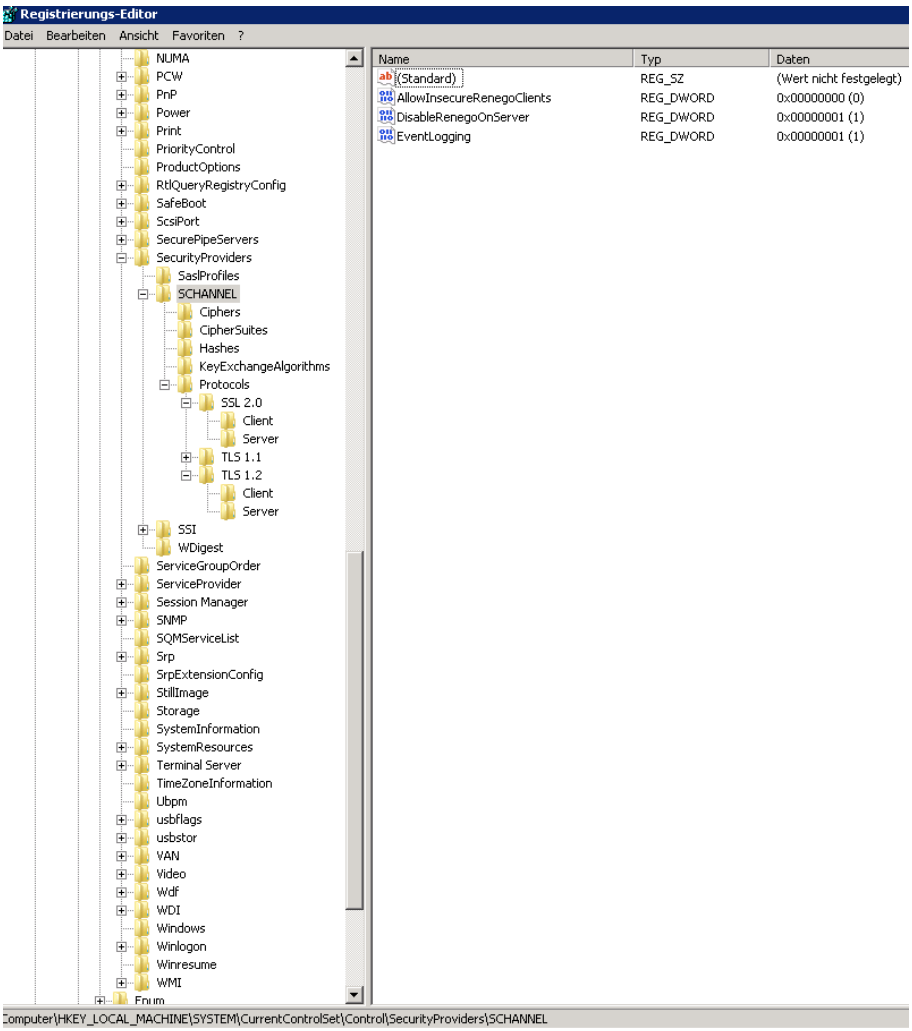


SSL 2.0 fuer den Server deaktivieren

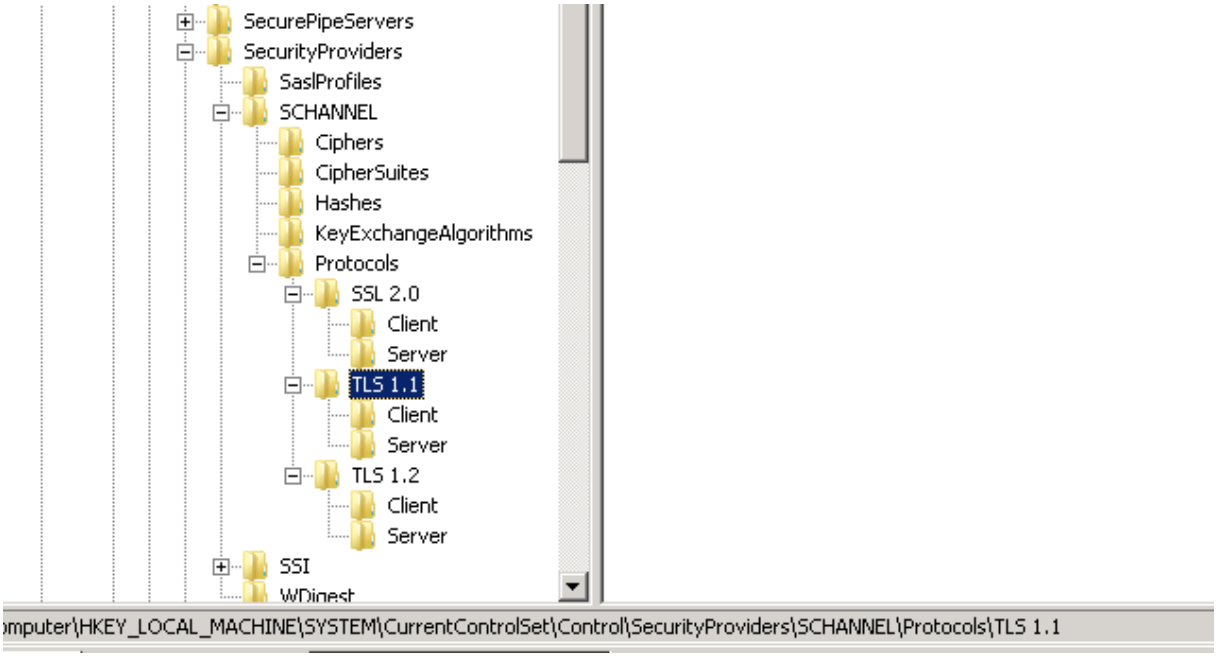


Weak Negotiation deaktivieren

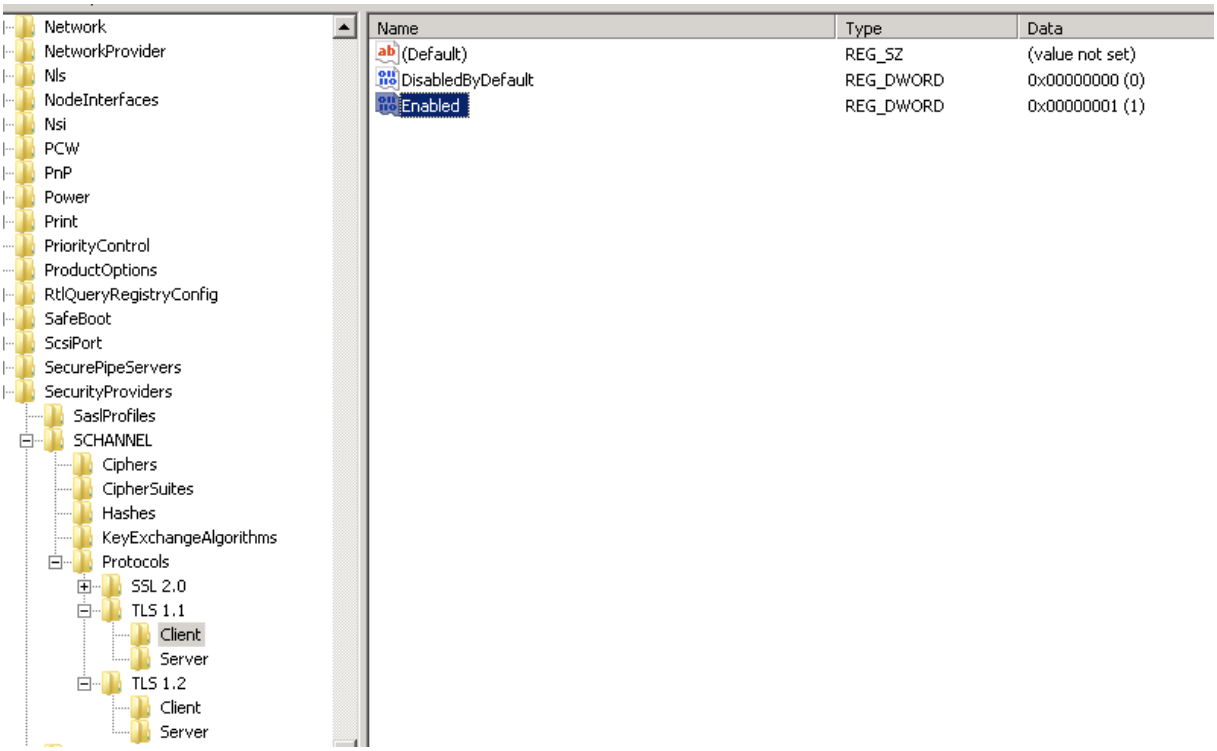
Weak Negotiation fuer Server deaktivieren



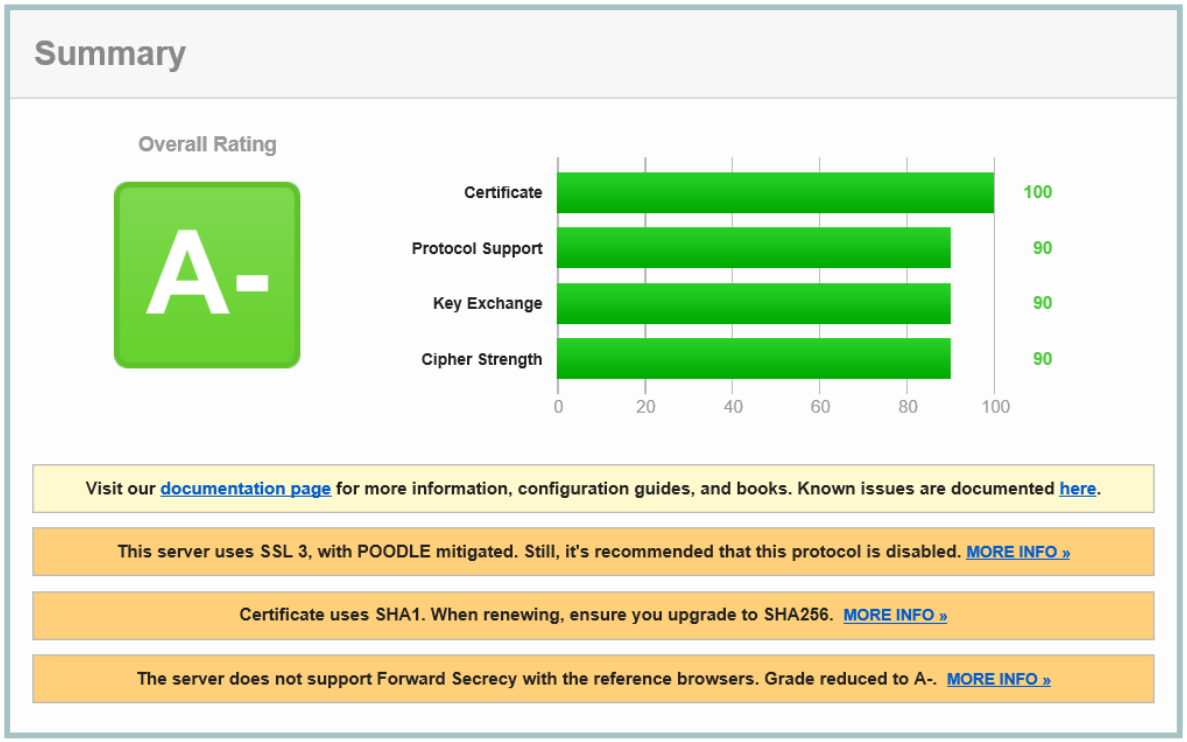
TLS 1.1 und TLS 1.2 aktivieren



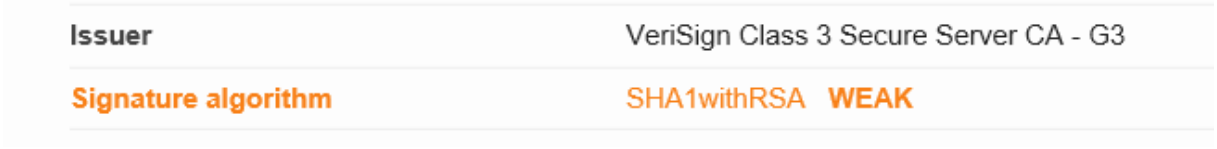
Eintraege



Server booten



Details



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

TLS 1.0	Yes
SSL 3 **INSECURE**	Yes

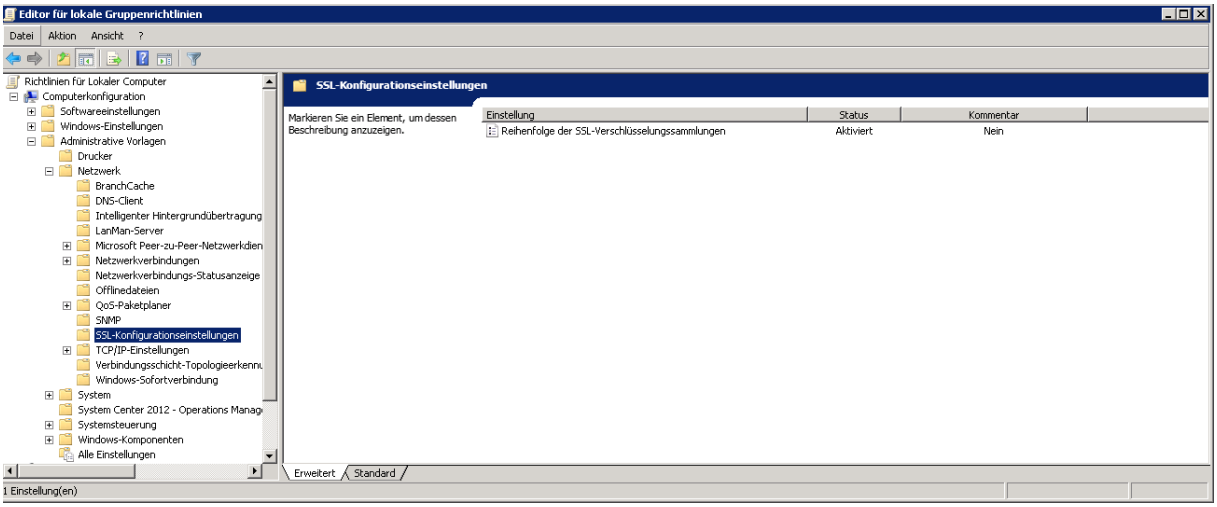
Diese Clients koennen jetzt NICHT mehr zugreifen

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]
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

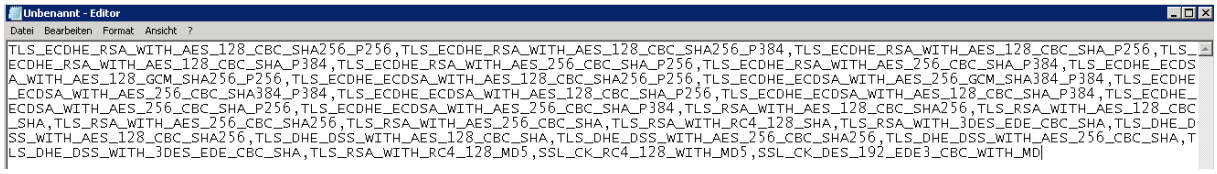
Forward Secrecy aktivieren

> **The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. MORE INFO »**

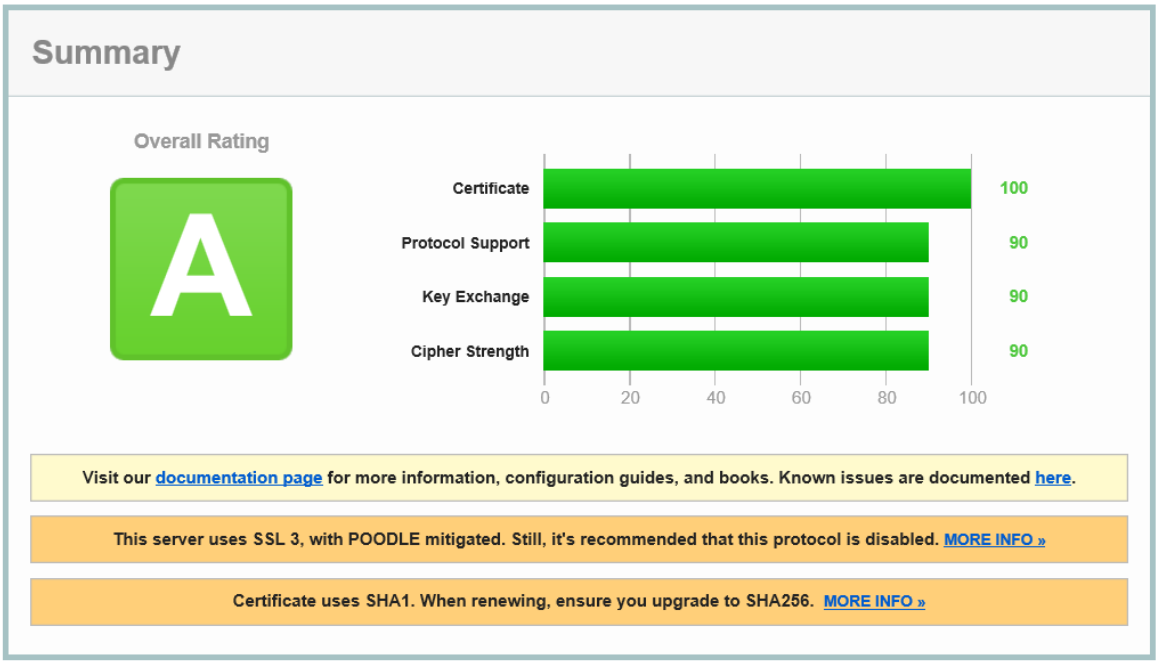
Cipher Suiten anpassen



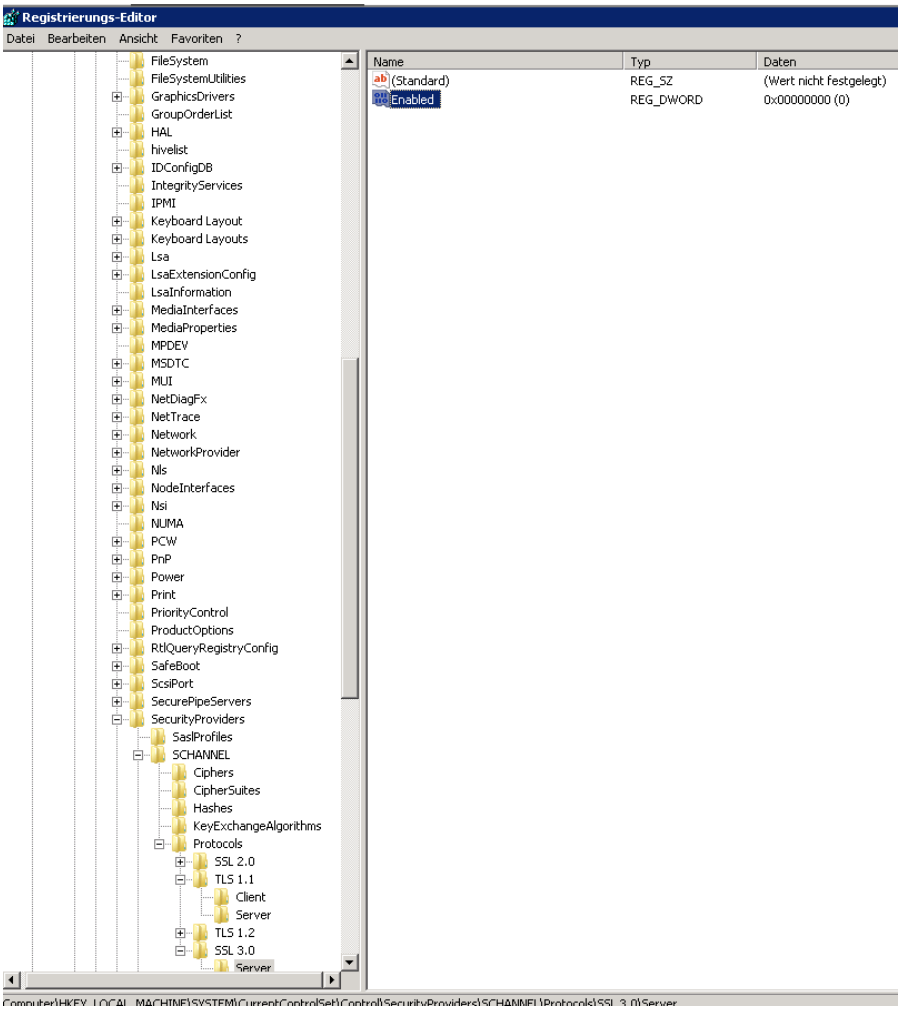
Alle Cipher Suites beginnend mit TLS_ECDHE* nach oben stellen



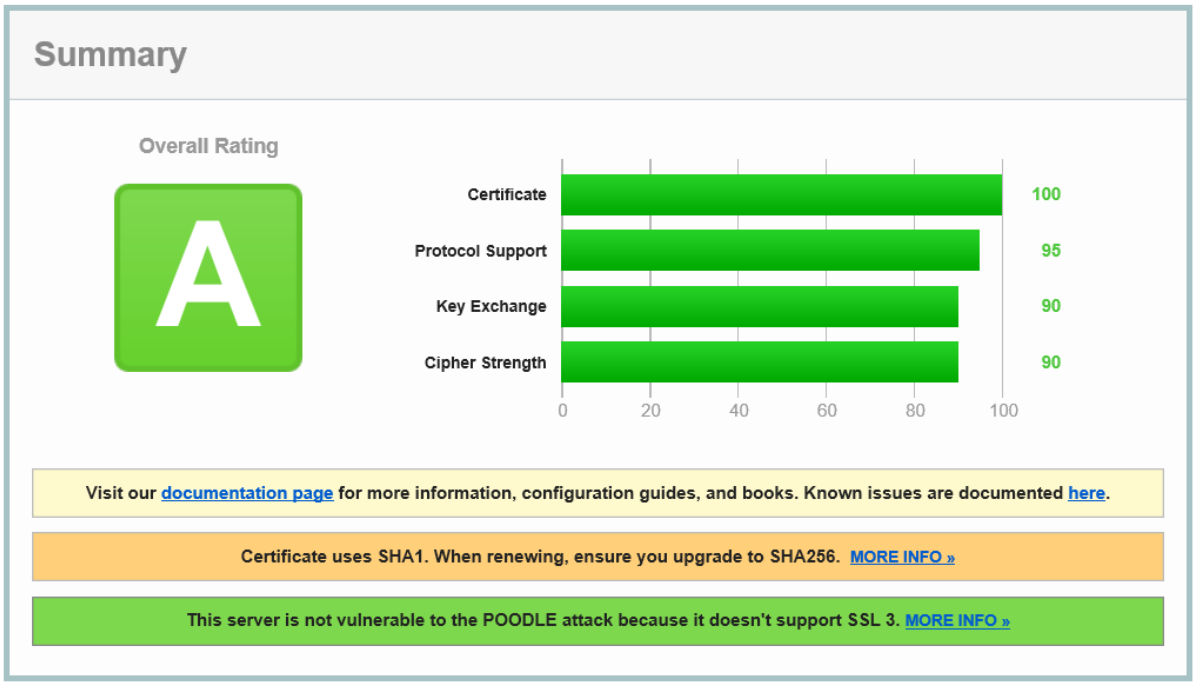
Besser



Jetzt den Pudel aeeh POODLE noch beseitigen



Great …



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