Zertifikate

X509-Zertifikate

Ausstellung von Serverzertifikaten

Muss ein größerer Benutzerkreis bedient werden, ist man darauf angewiesen, dass die Zertifizierungsstelle allen üblichen Browsern bereits bekannt ist. Im Rahmen des ACOnet werden solche Zertifikate über TU.it kostenlos zur Verfügung gestellt.

Für nur lokal genutzte Server bietet sich die Erzeugung von "self signed" Zertifikaten an. Das OpenSSL-Kommando lautet:

openssl req -x509 -days 9999 -new -newkey rsa:4096 -sha256 -text -nodes -out selfSigned.pem

Dabei wird die Schlüssellänge auf 4096 (sonst ist 2048 üblich) Bits und das Hashing-Verfahren auf das von modernen Clients verlangte SHA-256 festgelegt.
Der private (geheime) Schlüssel wird unter dem Dateinamen privkey.pem abgelegt.