MNM
TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München
und Technische Universität München

Prof. Dr. D. Kranzlmüller
Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit

Übungsblatt 04

10. **OpenSSL**

    (a) Erstellen Sie mit Hilfe von OpenSSL eine X.509 Certificate Authority (CA) mit der Lebensdauer von 10 Jahren!

    (b) Erzeugen Sie ein Public/Private Key Pair. Signieren Sie den Public Key mit Hilfe ihrer CA. Das Zertifikat soll 1 Jahr gültig sein.

    (c) Lassen Sie sich die Details ihres Zertifikates in für Menschen lesbarer Form ausgeben.

    (d) Konvertieren Sie ihr Zertifikat in das PKCS Format.

    (e) Entfernen Sie das Passwort aus ihrem Schlüssel.

    (f) Widerrufen Sie das Zertifikat.

11. **Sichere Webserver**

    (a) Installieren Sie ds Paket *apache2* auf ihrer Maschine.

    (b) Aktivieren Sie den Webserver auf dem Port 443/https. Stellen Sie dem Webserver ein Maschinen-Zertifikat Signiert von ihrer eigenen CA aus, damit dieser sich authentisieren kann!

    (c) Überprüfen Sie ihre Konfiguration, indem Sie ihre CA in einen Browser importieren. Auf dem Rechner Test4all stehen ihnen mehrere Browser zur Verfügung.