Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

# IT-Sicherheit im Wintersemester 2017/2018
# Übungsblatt 10

**Termin:** 30.01.2018 bis 12:00 Uhr

## Aufgabe 21: (K) X.509

a. Fassen Sie kurz das Aufgabenspektrum einer CA zusammen.

b. Welche grundsätzlichen Ansätze existieren für den Widerruf eines Zertifikats? Erläutern Sie diese und widerrufen Sie Ihr Zertifikat.

c. Für die Echtzeit-Überprüfung des Status eines Zertifikats wurde das Online Certificate Status Protocol entwickelt. Beschreiben Sie dessen grundsätzlichen Ablauf.

## Aufgabe 22: (K) Network-Security & 802.1X

Zur Absicherung von Netzen existieren verschiedene Verfahren. Eine sehr einfache, aber effiziente Möglichkeit, Netztraffic zu separieren, stellt der Einsatz von Virtual LANs (VLANs) dar. Eine im WLAN-Umfeld häufig anzutreffende Maßnahme ist der Einsatz von 802.1X.

a. Erläutern Sie knapp den Aufbau eines VLAN-Tags. Beschreiben Sie kurz die Priorisierung. Welche Prioritätseinstufung schlagen Sie für Video- bzw. IP-Telefonie vor?

b. 802.1X ist ein in WLAN- und VLAN-Infrastrukturen häufig verwendeter Network Access Control-Mechanismus. Sie benötigen in einem Besprechungsraum am LRZ Internet-Zugang über das dort zur Verfügung stehende, 802.1X-gesicherte WLAN. Welche erste Nachricht sendet der Supplicant üblicherweise, wenn der Authenticator nicht bekannt ist?

c. Welche Gefahr besteht beim Senden der Identitätsinformationen des Supplicants auf Ihrem Notebook an den WLAN-Access Point?

d. Skizzieren Sie die weitere Kommunikation zwischen ihrem Notebook, dem WLAN-Access Point und dem RADIUS-Server generell. Welchen großen Vorteil bietet die Verwendung von EAP-TLS? Was ist hierbei jedoch zwingende Voraussetzung?