

IT-Sicherheit im Wintersemester 2021/2022

Übungsblatt 10

Besprechung: 25.01.2022

Aufgabe 38: (T) X.509

- Fassen Sie kurz das Aufgabenspektrum einer CA zusammen.
- Welche grundsätzlichen Ansätze existieren für den Widerruf eines Zertifikats? Erläutern Sie diese!
- Für die Echtzeit-Überprüfung des Status eines Zertifikats wurde das Online Certificate Status Protocol entwickelt. Beschreiben Sie dessen grundsätzlichen Ablauf.

Aufgabe 39: (T) Bring your own device (BYOD)

Bring-Your-Own-Device (BYOD), also die dienstliche Nutzung privater Geräte, ist gerade bei kleineren Unternehmen oder Startups beliebt. Firmendaten dürfen dabei auf privaten, nicht firmeneigenen Geräten gespeichert und verarbeitet werden.

- Welche Vorteile bringt der BYOD-Ansatz für Mitarbeiter:innen und Firma mit sich?
- Welchen Nachteilen sehen sich beide Parteien gestellt?
- Ein verwandtes Konzept ist die private Nutzung dienstlicher Geräte. Stellen Sie es BYOD gegenüber! Welche anderen Ansätze wären darüber hinaus denkbar, um Mitarbeiter und Arbeitgeber zu unterstützen?

Aufgabe 40: (T) OIDC

Open ID Connect (OIDC) implementiert eine simple Authentifizierung auf Basis des OAuth 2 Frameworks. Es ermöglicht die Nutzung einer zentral gespeicherten, digitalen Identität bei verschiedenen Services (<https://openid.net/connect/faq/>).

- Erklären Sie den allgemeinen Ablauf der Authentifizierung mit OIDC.
- Nennen Sie die zwei Hauptakteure in einer OIDC Interaktion und beschreiben Sie deren Rolle.
- Die Identität wird bei OIDC mit Hilfe von ID Token übertragen. Erläutern Sie den Aufbau eines solchen Tokens.