isec 2024: Fragestunde

W49

Signaturen

— privater Schlüssel: signieren
— öffentlicher Schlüssel: Signatur prüfen

Verfahren:

— RSA
— El Gamal ➔ DSA
— (ECC: ECDSA, EdDSA "25519")

Zertifikate

— X.509 (wirklich: RFC 5280)
— Zertifikatsketten, Wurzelzertifikate
— PKI
— Nutzung in: Web-Server, S/MIME

Authentisierung: Mensch-Gerät

1. Wissen
2. Besitz
3. (biometrische) Merkmale

— Kombinationen (n-Faktor)

Passwords

- Server: Password-Verschlüsselung
- Offline-Angriffe
- Wahl guter Passwörter
  - NIST SP 800-63B
- OTP-Token
  (vgl. TOTP nach RFC 6238)
- Biometrie