Crypto 101

@OliverMilke
@cloudogu

AGENDA

1. **meta**
2. Überblick | Abgrenzung
3. Key Pair vs. Signature
4. Cipher Suite

Vortrag

- ✓ Crypto is hard to get right
  - Dutch Election Security Talk
- ✓ Begriffe / Konzepte
  - Dinge, über die ich gestolpert bin
  - nicht „from Scratch“
- ✓ Fragen erwünscht

cloudogu

About me

Oliver Milke

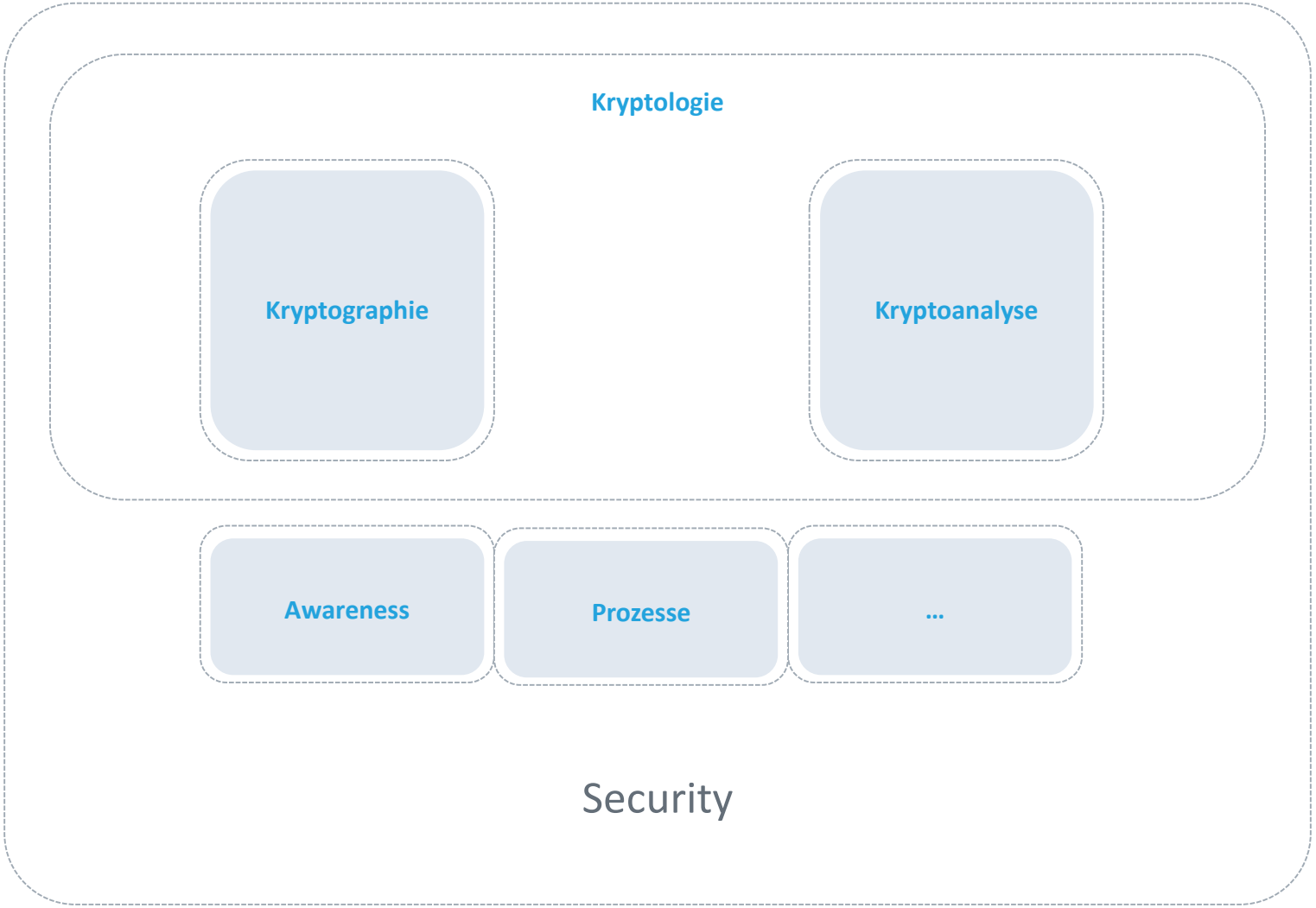
Software Craftsman

- http://oliver-milke.de/
- https://twitter.com/OliverMilke
- https://github.com/omilke
- https://stackoverflow.com/users/2108919/omilke

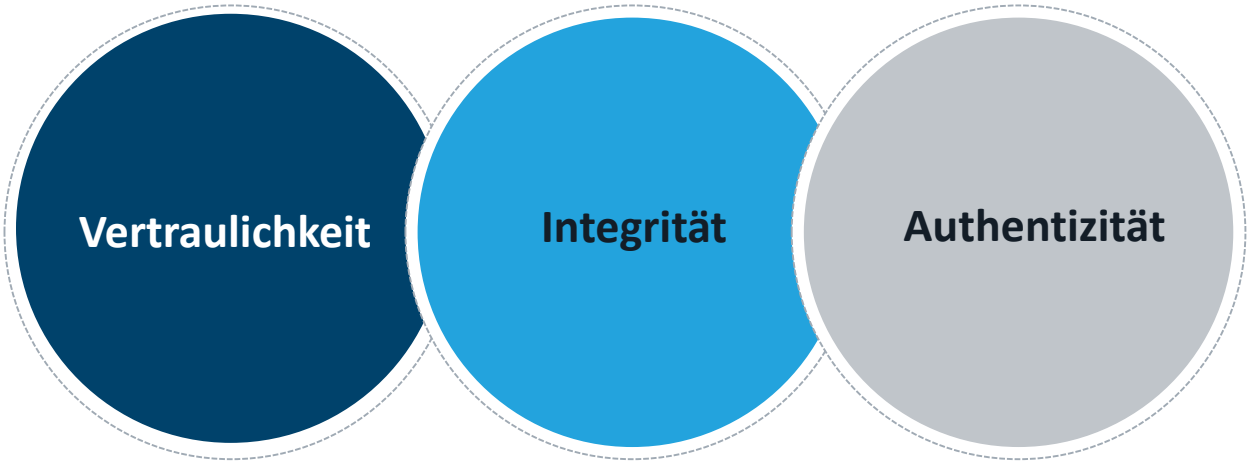
- > 10 Jahre Softwareentwicklung
- Crypto und Security im Bereich Mobile Online Dienste bei VW
- Software Craftsman @Cloudogu EcoSystem
- JUG Ostfalen
- Fitness / Freeletics

AGENDA

1. meta
2. **Überblick | Abgrenzung**
3. Key Pair vs. Signature
4. Cipher Suite


Kryptologie
Kryptographie
Kryptoanalyse
Awareness
Prozesse
...
Security

Ziele



Kerckhoffs' Prinzip

- ✓ SQL verschlüsselt?
- ✓ Authorization: Basic d2lraTpwZWRpYQ==
- ✓ Sicherheit durch Geheimhaltung des Schlüssels
  - nicht des Algorithmus
  - Gegenteil: Security By Obscurity

KRYPTOGRAPHISCHE PRIMITIVEN

Kryptographischer Hash

- Einwegfunktion
- Kollisionsresistent
- MD*, SHA-*, bCyrpt

Symmetrische Verschlüsselung

- 1 Schlüssel für Ver- und Entschlüsselung
- Schnell
- Stream Cipher
- Block Cipher
  - Verschiedene Modi
  - AES
    - Rijndael Cipher

KRYPTOGRAPHISCHE PRIMITIVEN

Asymmetrische Verschlüsselung

- 2 inverse Schlüssel (Key Pair)
- Operationen können mit jeweils anderem Schlüssel umgekehrt werden
- langsam

Digitale Signatur

- Asymmetrisch verschlüsselter Hash

KRYPTOGRAPHISCHE PRIMITIVEN

Kryptografisch sichere Zufallszahlengenerierung

- Zufall durch eine Maschine?
- Noncen
  - Schutz vor Replay

Sicherheit von Kryptographie

- Einwegfunktionen
  - „vorwärts“ ist einfach
  - „rückwärts“ ist schwer / unmöglich
- Problemklassen
  - Integerfaktorisierung
    - RSA
  - Diskreter Logarithmus
    - Diffie-Hellman, ElGamal
    - endliche Körper / Elliptische Kurven
  - AES
- Exploits
  - Spezifikation
  - Implementierung
    - Side Channel Attack

Passwörter

? Speicherung für Anmeldung

✓ Salt
- Individuell für jedes Passwort

! Pepper
- Gleich für alle Passwort

✓ Argon2

✓ PBKDF2

✓ sCrypt / bCrypt

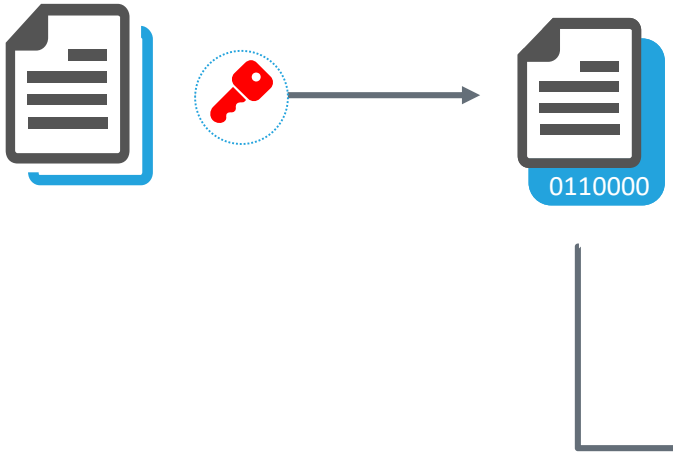
Hash

Hash

- ✓ Einwegfunktion
- ✓ Integrität kann überprüft werden
- ✓ Unsicherer Transportweg
  - Austausch von Original und Hash möglich

Message Authentication Code

Hash **+ Shared Secret**



- ✓ Unsicherer Transportweg
  - Austausch nicht möglich
- ✓ Integrität und Authentizität

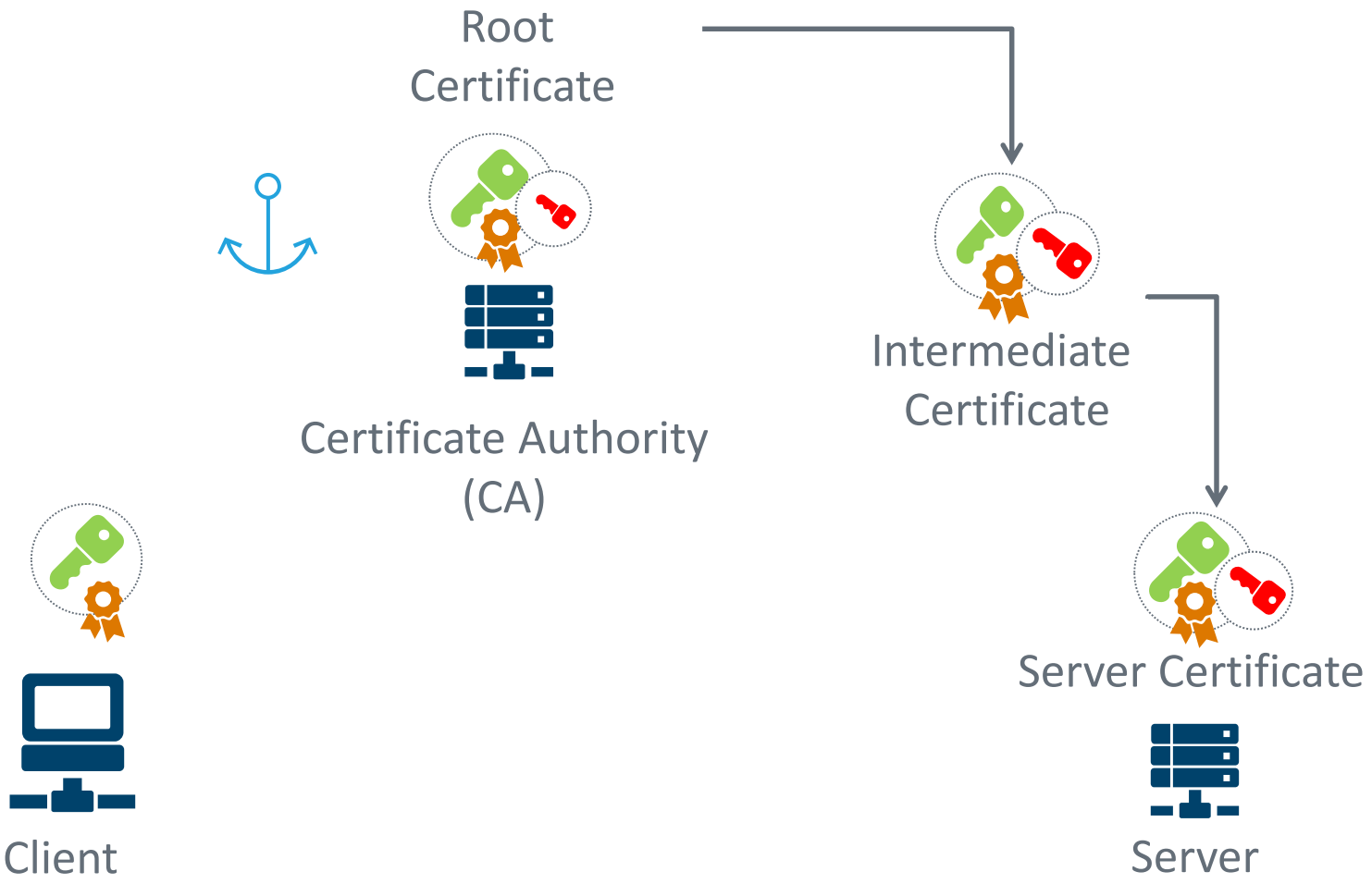
HMAC

AGENDA

1. meta
2. Überblick | Abgrenzung
3. **Key Pair vs. Signature**
   …oder: was ist ein Trust Anchor?
4. Cipher Suite

Host-Authentifizierung
SSH

Host-Authentifizierung
TLS



AGENDA

1. meta

2. Überblick | Abgrenzung

3. Key Pair vs. Signature
   …oder: was ist ein Trust Anchor?

4. **ECDHE-ECDSA-AES256-GCM-SHA384**
   …oder: Was ist eine Cipher Suite?

Transport Layer Security
TLS

- ✓ Verbindung ist verschlüsselt

- ✓ Welcher Algorithmus?
  - ECDHE-ECDSA-AES256-GCM-SHA384
    - AES im GCM-Modus mit 256bit Schlüssel
    - SHA-384 HMAC

Transport Layer Security
TLS

- ✓ Verbindung ist verschlüsselt
  - AES256-GCM-SHA384
- ✓ Woher kommt der Schlüssel?
  - ECDHE-ECDSA-AES256-GCM-SHA384
    - Ephemeral Elliptic Curve Diffie-Hellman

Transport Layer Security
TLS

- ✓ Verbindung ist verschlüsselt
  - AES256-GCM-SHA384
  - Key Exchange mit ECDHE
- ✓ Richtiger Host (meine Bank)?
  - ECDHE-ECDSA-AES256-GCM-SHA384
    - Elliptic Curve Digital Signature Algorithm

Cipher Suite

- Crypto-System
  - Beteiligte Primitiven
  - Konstanten mit spezifizierten Details

- Abhängig vom Protokoll
  - Beispiel TLS 1.2
    - TLS 1.3 verwendet andere Konzepte

Schlussfolgerung

Java Libs

- Crypto Lib (bCrypt)
  http://www.bouncycastle.org/java.html

- Password Policy
  http://www.passay.org/
  (ehemals vt-password)

Links

- Password Hashing
  security.stackexchange.com Thread

- OWASP Password Storage Cheat Sheet
  https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

- OWASP Forgot Password Cheat Sheet
  https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet

Links

! Qualys SSL Lab Server Test
https://www.ssllabs.com/ssltest/

! Mozilla Config Generator
https://mozilla.github.io/server-side-tls/ssl-config-generator/

✓ Bruce Schneier
https://www.schneier.com/

✓ Security Bewertungen
https://www.keylength.com/

Oliver Milke

Get in touch

- https://twitter.com/OliverMilke
- http://oliver-milke.de/
- dev@oliver-milke.de

Thank you

For watching

feedback plz