

# Crypto 101

---

Oliver Milke  
TRIOLOGY GmbH

# AGENDA

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

# WER SEID IHR?

1 Entwickler?

2 Dev Ops?

# Vortrag

- ✓ Crypto is hard to get right
  - [Dutch Election Security Talk](#)

- ✓ Begriffe / Konzepte
  - Dinge, über die ich gestolpert bin
  - nicht „from Scratch“

- ✓ Fragen erwünscht

A word cloud of cryptography terms. The words are arranged in a roughly triangular shape, with 'Cryptography' being the largest and most central word. Other prominent words include 'symmetric', 'hash', 'RSA', 'authentic', 'signature', 'integrity', 'AES', 'handshake', 'encryption', 'ecc', 'oneway', 'asymmetric', 'cipher', and 'password'. The words are in various shades of gray and are oriented in different directions, creating a dynamic and abstract visual representation of the field.

symmetric  
hash  
Cryptography  
RSA  
authentic  
signature integrity  
AES handshake  
encryption ecc oneway  
asymmetric cipher  
password



## About me

### Oliver Milke

Software Craftsman

 <http://oliver-milke.de/>

 <https://twitter.com/OliverMilke>

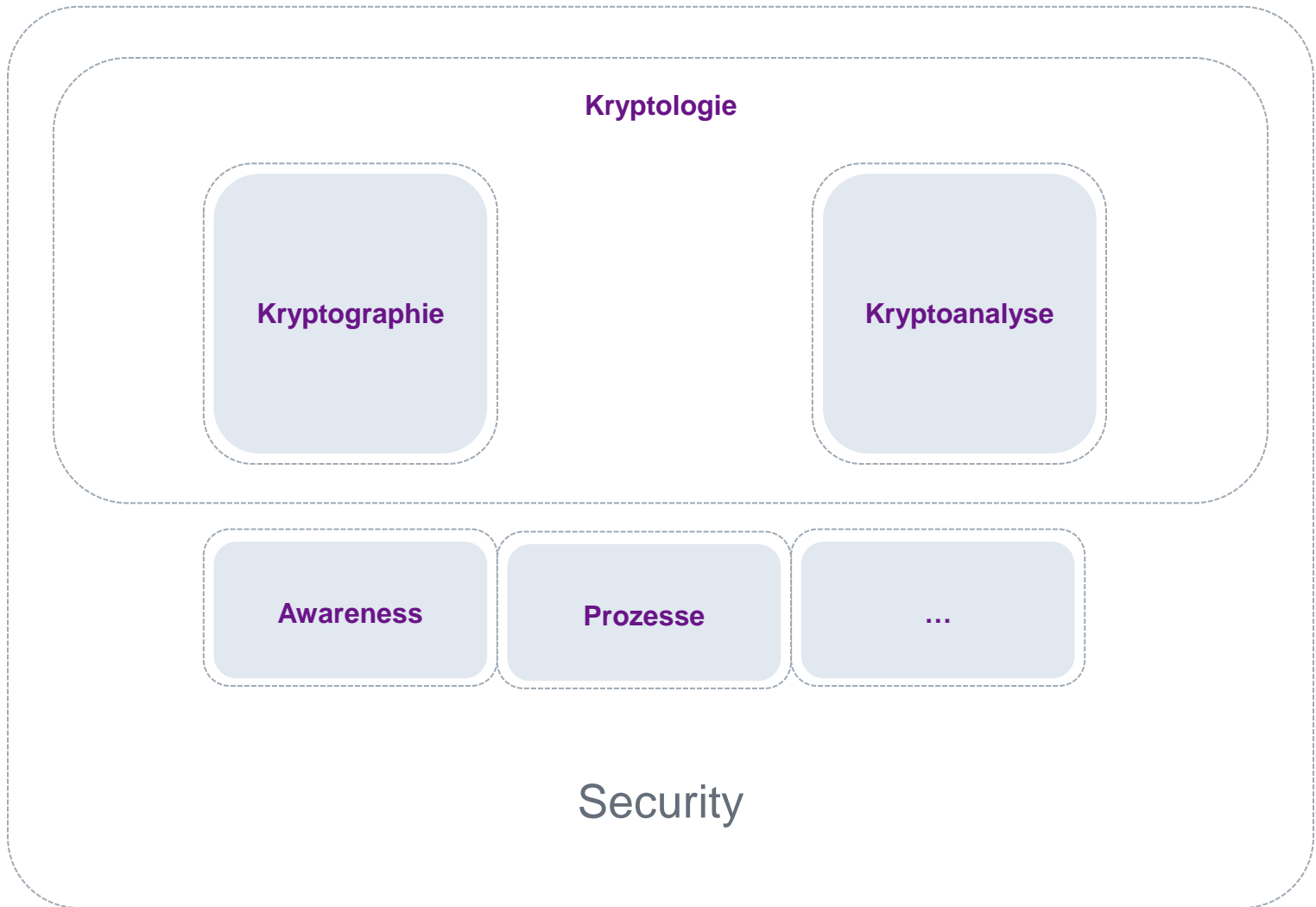
 <https://github.com/omilke>

 <https://stackoverflow.com/users/2108919/omilke>

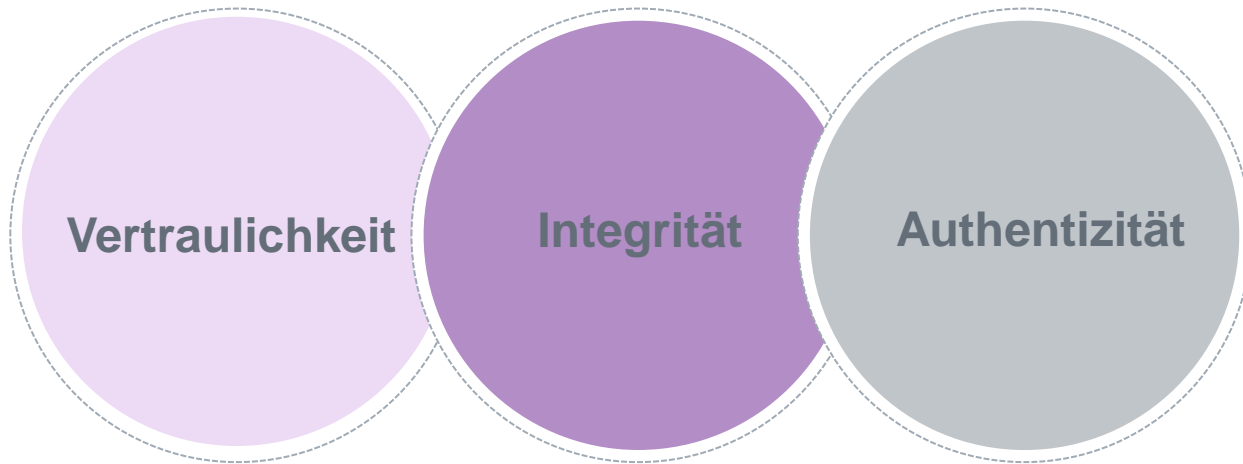
- > 10 Jahre Softwareentwicklung
- Crypto und Security im Bereich Mobile Online Dienste bei VW
- JUG Ostfalen
- Fitness

# AGENDA

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



# 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-\*, bCrypt



## 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
  - Elyptische Kurven
- AES



## Exploits

- Spezifikation
- Implementierung
  - Side Channel Attack

# Passwörter

 Speicherung für Anmeldung

 Salt

- Individuell für jedes Passwort

 Pepper

- Gleich für alle Passwort

 bCrypt

 PBKDF2

# Hash

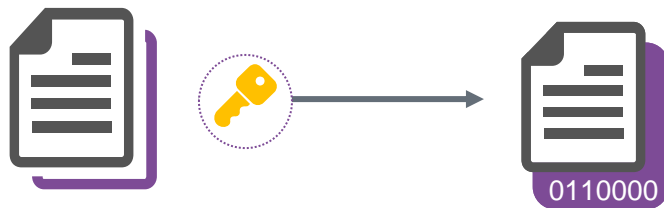
## Hash



- ✓ 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**

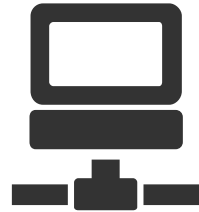


# AGENDA

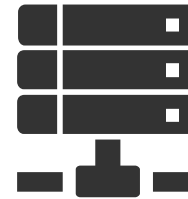
- 1 meta
- 2 Überblick | Abgrenzung
- 3 **Key Pair vs. Signature**  
...oder: was ist ein Trust Anchor?
- 4 Cipher Suite

# Host-Authentifizierung SSH

---

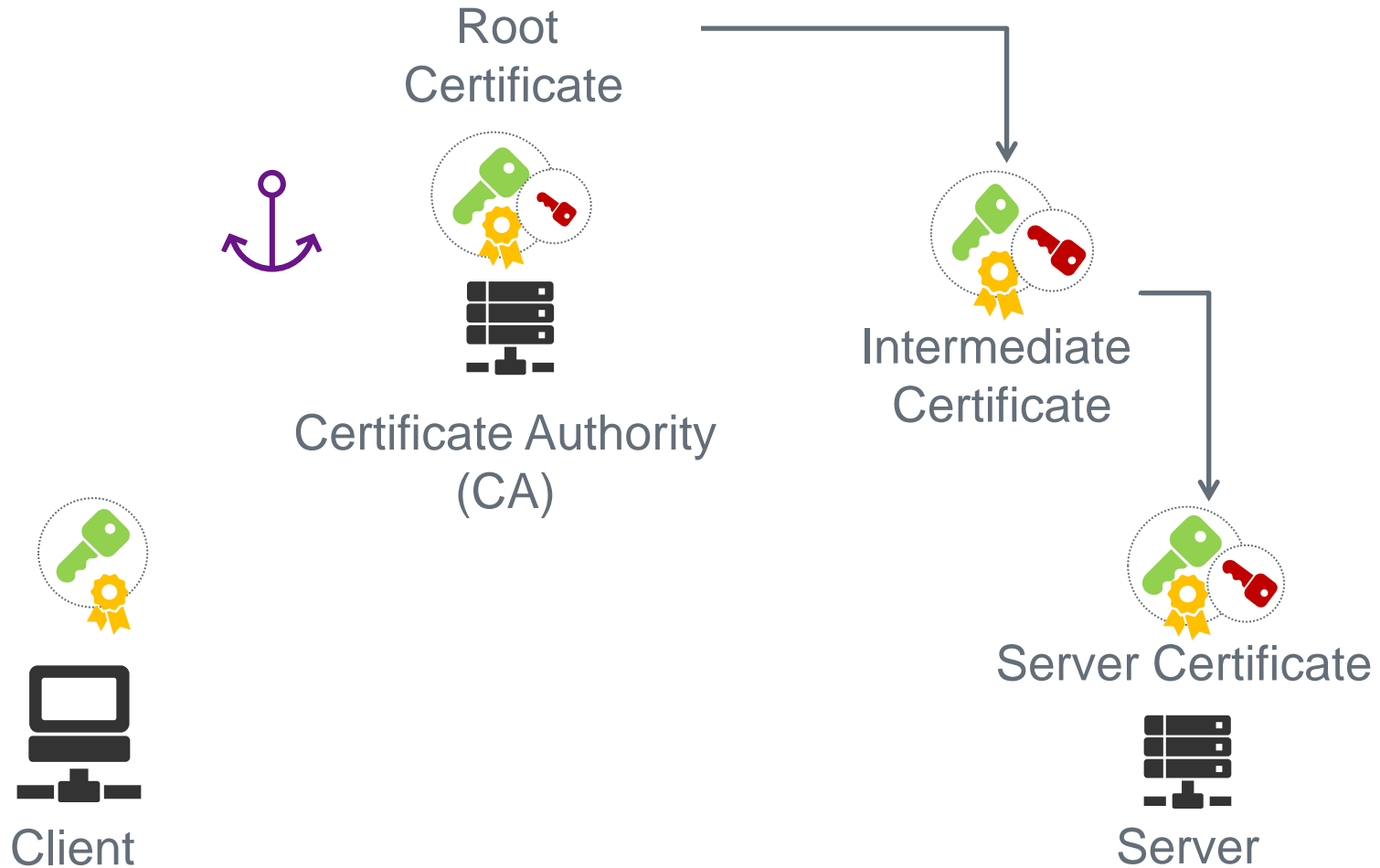


Client



Server

# Host-Authentifizierung TLS



# AGENDA

1 meta

2 Überblick | Abgrenzung

3 Key Pair vs. Signature

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 Elyptic 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

# It's all about the vector

? Passwort Speichern

? Mobile Online Dienste

# Java Libs



Crypto Lib (bCrypt)

<http://www.bouncycastle.org/java.html>



Password Policy

<http://www.passay.org/>

# 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/>



Password Hashing

[security.stackexchange.com](https://security.stackexchange.com) Thread

Oliver Milke

## Get in touch

- <https://twitter.com/OliverMilke>
- <http://oliver-milke.de/>
- [dev@oliver-milke.de](mailto:dev@oliver-milke.de)

- Vortragsbewertungen

Thank you  
For watching  
See you soon!