# IT-Security (ITS) B1

# DIKU, E2024

# Today's agenda

Crypto recap

Putting it all together

Key exchange

Key management

Certificates

# Assignments

There are 6 weekly assignments during the course.

| Week | Date | Topic |
| --- | --- | --- |
| 36 | 08 Sep | No handin first week |
| 37 | 15 Sep | Assignment 1 handin |
| 38 | 22 Sep | Assignment 2 handin |
| 39 | 29 Sep | Assignment 3 handin |
| 40 | 06 Oct | Assignment 4 handin |
| 41 | 13 Oct | Assignment 5 handin |
| 42 | 20 | Possible re-handin of one assignment (1-4) |
| 43 | 27 Oct | Assignment 6 handin |

Pass/fail; groups of up to 3; expect at least 66 % correct to pass; re-handin of only one.

# Recap: Security goals and crypto primitives

Don’t worry about the details of RSA, AES, or SHA1

Focus on the bigger picture of what we achieve with

- symmetric / asymmetric ciphers
- cryptographic hash functions
- message authentication codes
- digital signatures

# Key management

# Many keys to protect

Master key

Session key

Signature key

Data encryption key

Key encryption key

...

# Protect during entire lifecycle

Generation

Exchange

Storage/backup

Use

Expiration

Revocation

Destruction

# Key exchange options include

**Pre-distribution**

Generated and distributed “ahead of time” e.g. physically

**Distribution**

Generated by a trusted third party (TTP) and sent to all parties

**Agreement**

Generated by all parties working together

**Asymmetric**

Is e really yours?

# Key distribution

# Developing a key distribution scheme

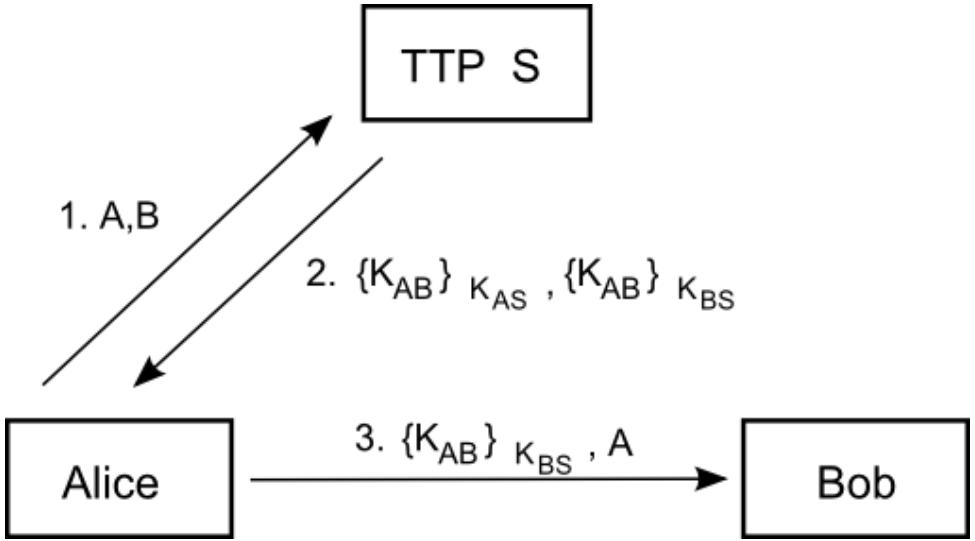
Situation:

- A and B want to exchange keys remotely
- Both A and B share a key (K_AS, K_BS) with a trusted third party, S

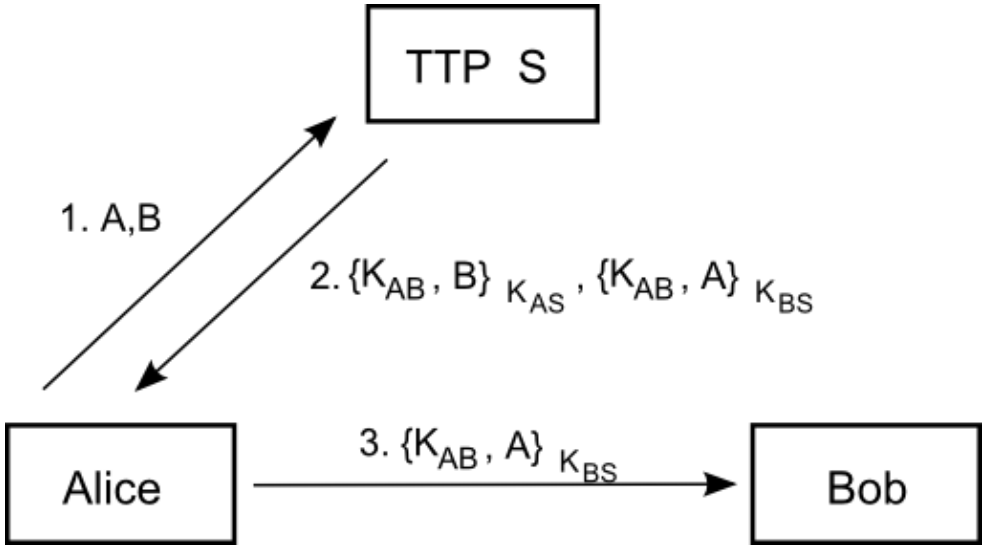
At the end, we want to achieve:

- A and B know a new key K_AB
- No one but A, B, and possibly S knows K_AB
- A and B know that K_AB is newly generated

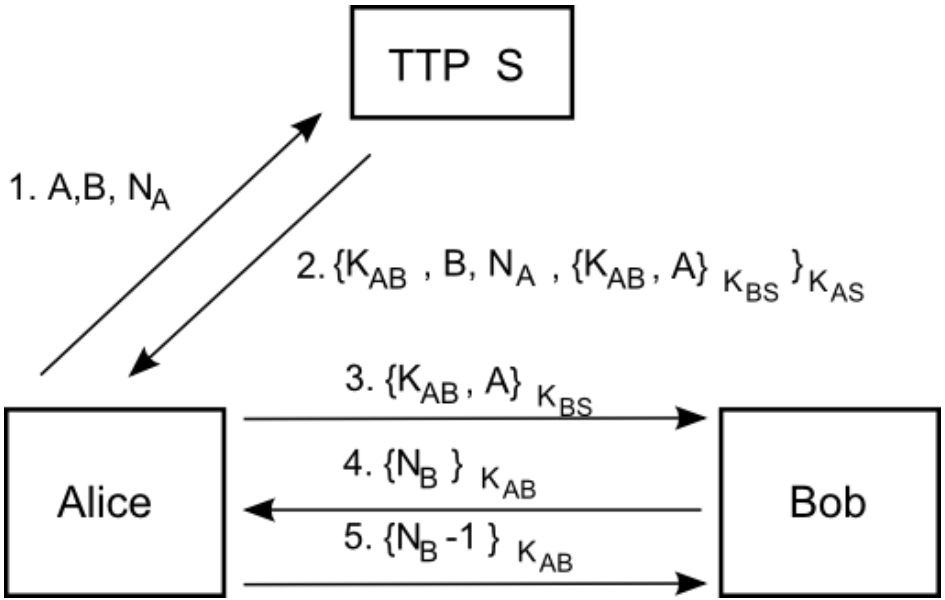
# Key distribution



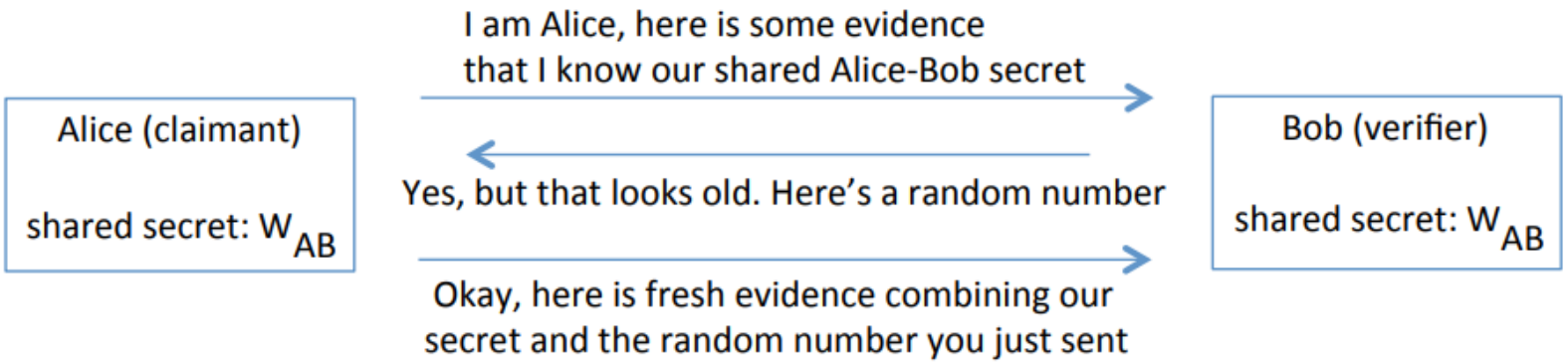
# Key distribution



# Key distribution



# Basic authenticated key exchange



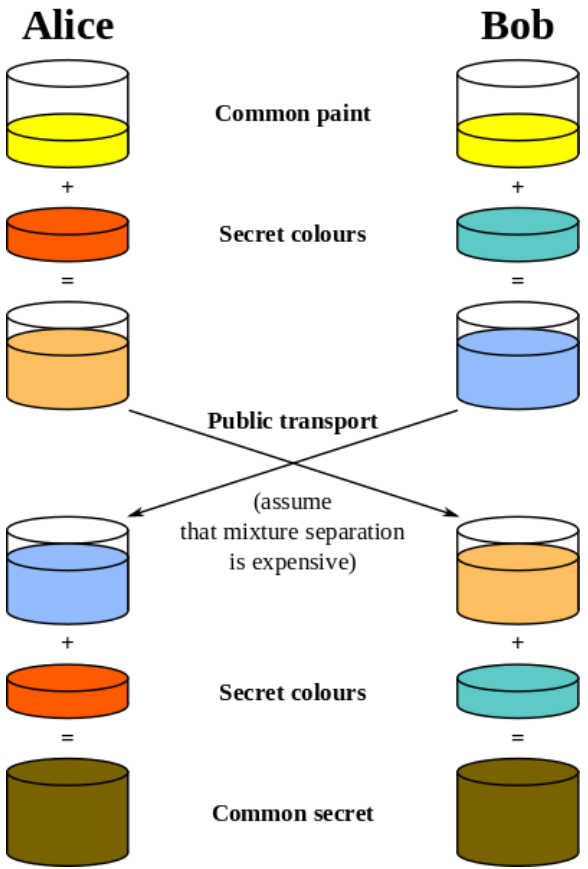
# More key management risks

| Attack | Short description |
|---|---|
| replay | reusing a previously captured message in a later protocol run |
| reflection | replaying a captured message to the originating party |
| relay | forwarding a message in real time from a distinct protocol run |
| interleaving | weaving together messages from distinct concurrent protocols |
| middle-person | exploiting use of a proxy between two end-parties |
| dictionary | using a heuristically prioritized list in a guessing attack |
| forward search | feeding guesses into a one-way function, seeking output matches |
| pre-capture | extracting client OTPs by social engineering, for later use |

# Key agreement

# Basic idea

If you wanted to exchange secret paints



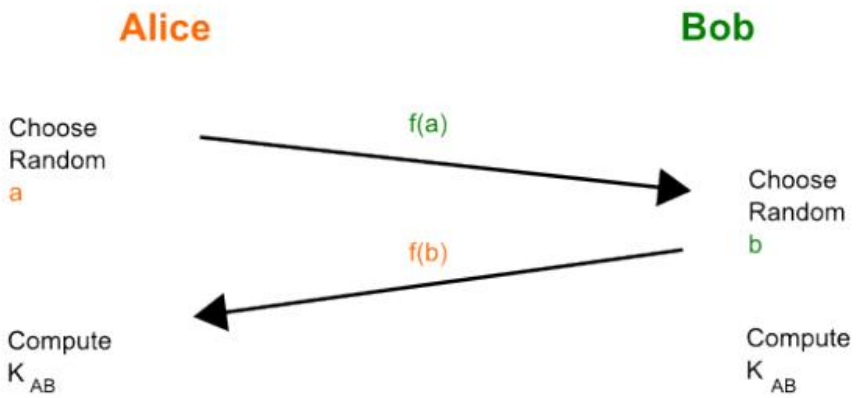
# Basic idea

Choose a function f such that

$$f(a,f(b)) = f(b,f(a))$$

And

$$f^{-1}(x) \text{ is hard}$$



# Solution by Diffie-Hellman, 1976

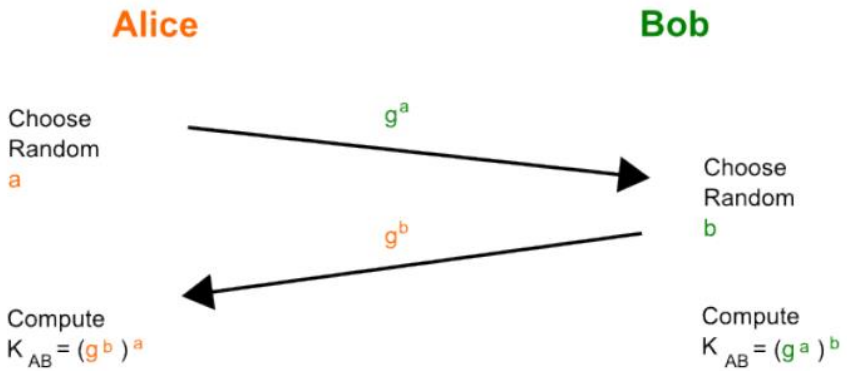
$f(x) = g^x \bmod p$

Given $g^a$, find x so $g^x = g^a$

Discrete logarithm problem

Given $g^a$ and $g^b$, find $g^{ab}$

Computational Diffie-Hellman assumption



# Diffie-Hellman: toy example (security)

| Alice | | Bob | | Eve | |
|---|---|---|---|---|---|
| **Known** | **Unknown** | **Known** | **Unknown** | **Known** | **Unknown** |
| $p = 23$ | | $p = 23$ | | $p = 23$ | |
| $g = 5$ | | $g = 5$ | | $g = 5$ | |
| $\mathbf{a = 6}$ | $\mathbf{b}$ | $\mathbf{b = 15}$ | $\mathbf{a}$ | | $\mathbf{a}, \mathbf{b}$ |
| $A = 5^{\mathbf{a}} \bmod 23$ | | $B = 5^{\mathbf{b}} \bmod 23$ | | | |
| $A = 5^{\mathbf{6}} \bmod 23 = 8$ | | $B = 5^{\mathbf{15}} \bmod 23 = 19$ | | | |
| $\mathbf{B = 19}$ | | $\mathbf{A = 8}$ | | $A = 8, B = 19$ | |
| $\mathbf{s} = B^{\mathbf{a}} \bmod 23$ | | $\mathbf{s} = A^{\mathbf{b}} \bmod 23$ | | | |
| $\mathbf{s} = 19^{\mathbf{6}} \bmod 23 = \mathbf{2}$ | | $\mathbf{s} = 8^{\mathbf{15}} \bmod 23 = \mathbf{2}$ | | $\mathbf{s} = 19^{\mathbf{a}} \bmod 23 = 8^{\mathbf{b}} \bmod 23$ | |
| $\mathbf{s = 2}$ | | $\mathbf{s = 2}$ | | | $\mathbf{s}$ |

# Is *e* really yours?

# Public-key infrastructure (PKI)

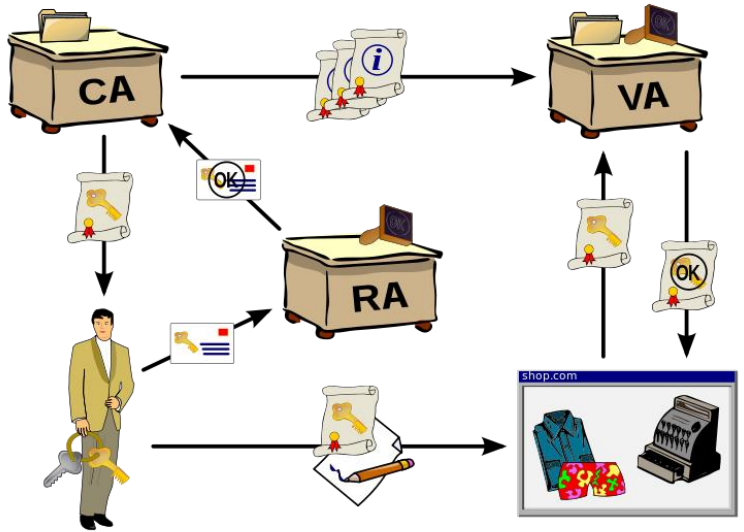
A system for the creation, storage, and distribution of **digital certificates** which are used to verify that a particular public key belongs to a certain entity

X.509 format for certificates include:

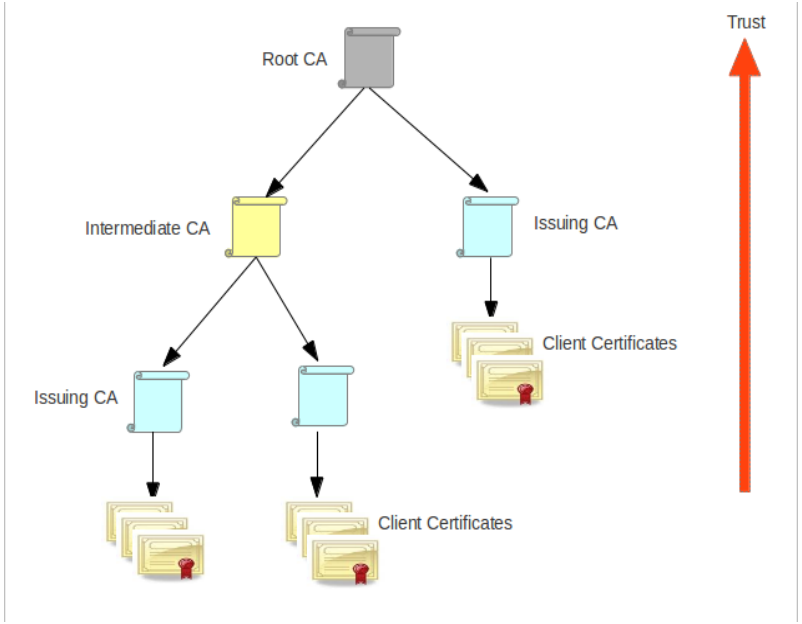
| | |
|---|---|
| Serial number | – unique identification of certificate |
| Valid-From/To | – lifespan of the certificate |
| Subject | – the entity/person/machine/etc. identified |
| Public key | – the entity's public key |
| Signature | – the actual signature of the issuer |

# Issuance and verification

A private key is created by you – the certificate owner – when you request your certificate with a Certificate Signing Request (CSR).

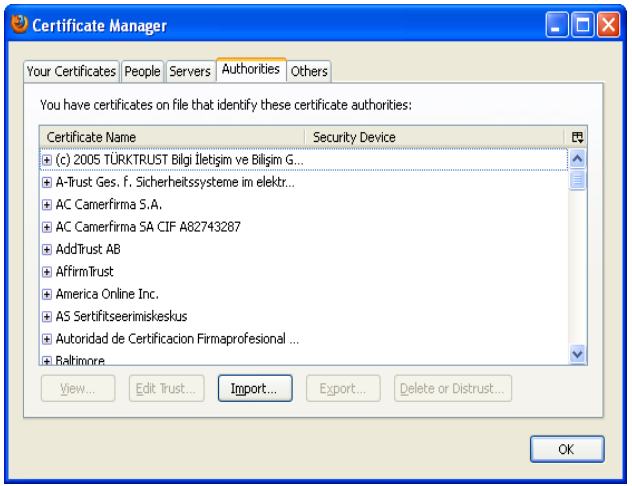


# Types of PKI: CA model

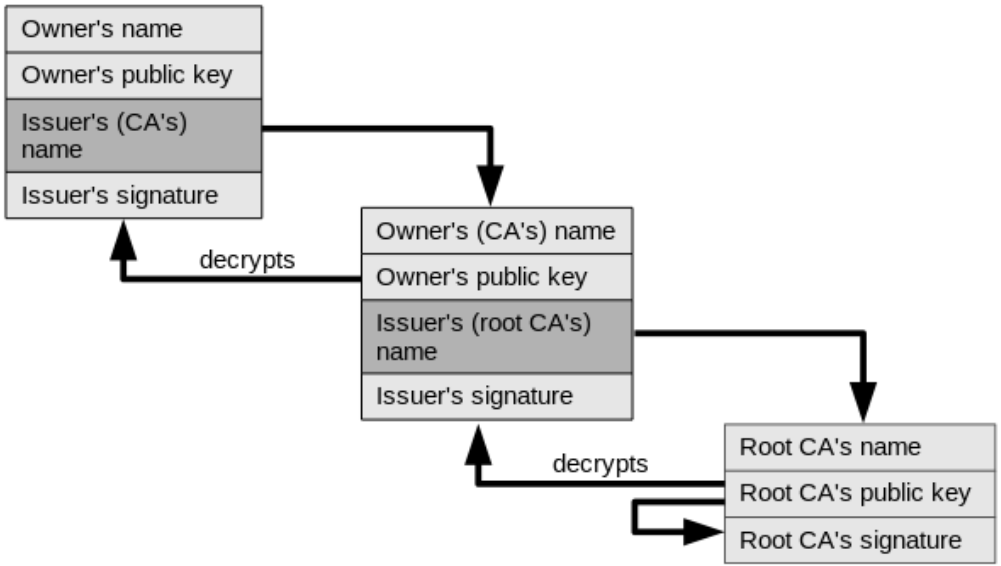


# Trust in browsers

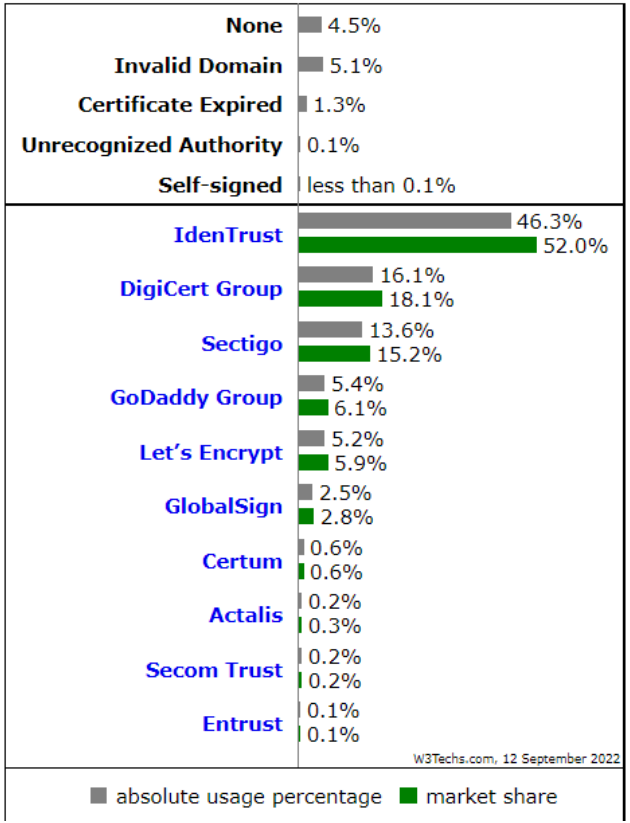
Browsers come pre-configured with a set of root CAs. Do you trust all these CAs (to authenticate properly, to avoid/inform of breaches)?



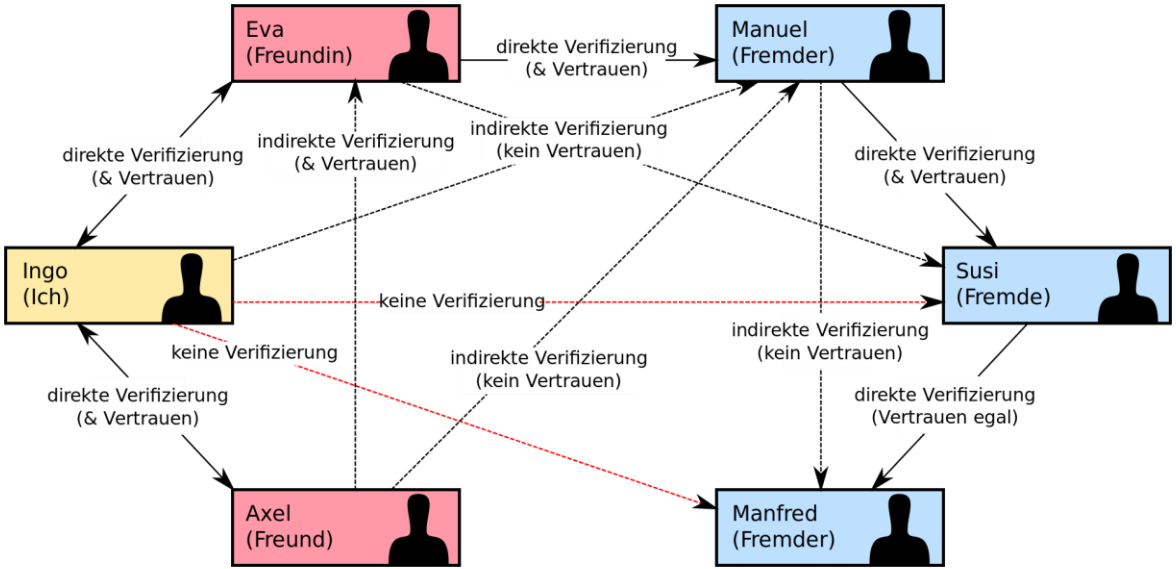
# Chain of trust



# CA providers



# Types of PKI: Web of trust



# Revocation of certificates

Certificate revocation list (CRL):

> A list of (serial numbers for) certificates that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted

Online Certificate Status Protocol (OCSP):

> Protocol used for obtaining the revocation status of an X.509 digital certificate

# Lecture plan

| Week | Date | Topic |
| --- | --- | --- |
| 36 | 02 Sep | Security concepts and principles |
| | 06 Sep | Cryptographic building blocks |
| 37 | 09 Sep | Key establishment and certificate management |
| | 13 Sep | User authentication, IAM |
| 38 | 16 Sep | Operating systems security, web, browser and mail security |
| | 20 Sep | IT security management and risk assessment |
| 39 | 23 Sep | Software security - exploits and privilege escalation |
| | 27 Sep | Malicious software |
| 40 | 30 Oct | Firewalls and tunnels, security architecture |
| | 04 Oct | Cloud and IoT security |
| 41 | 07 Oct | Intrusion detection and network attacks |
| | 11 Oct | Forensics |
| 42 | | Fall Vacation - No lectures |
| 43 | 21 Oct | Privacy and GDPR |
| | 25 Oct | Privacy engineering |
| 44 | 28 Oct | Final guest lecture and Exam Q/A |