IT-Security (ITS) B1

DIKU, E2023

Today’s agenda

Key Exchange

Key Management

Certificates

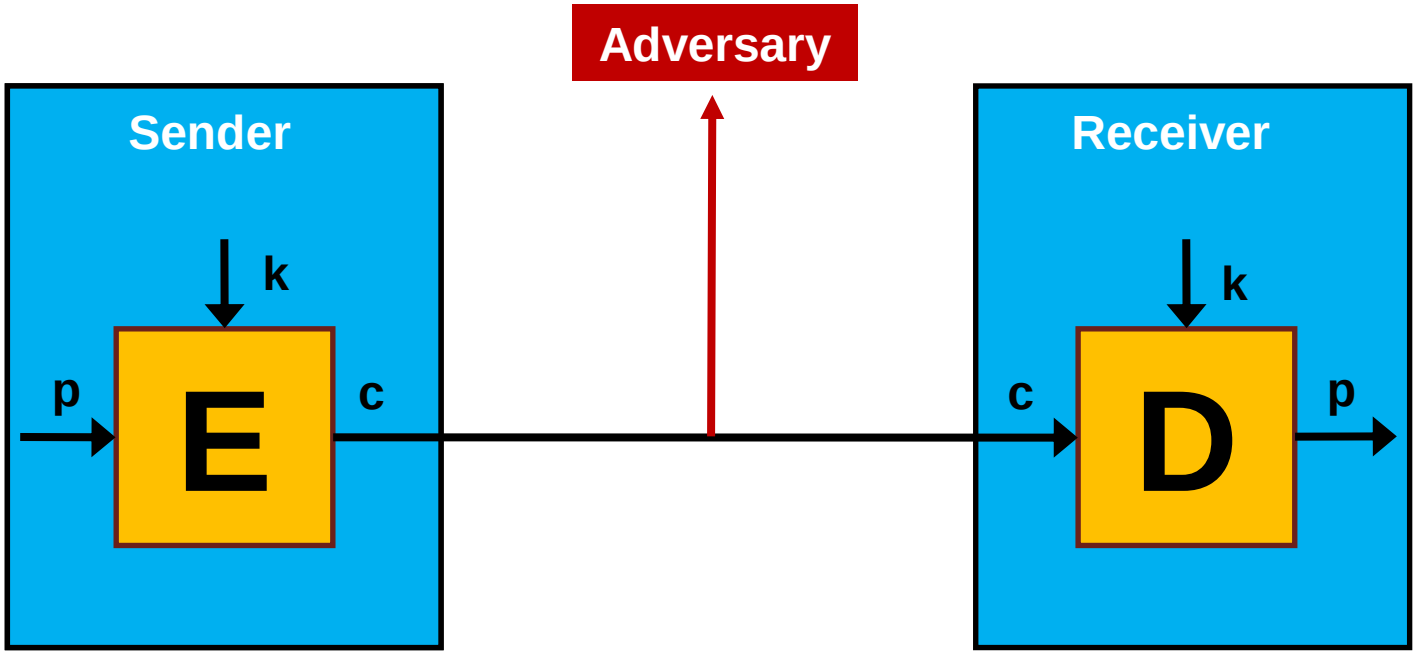
Lecture plan

Week	Date	Time	Lecture	Topic
36	04 Sep	10-12	TL	Security concepts and principles
	08 Sep	10-12	TL	Cryptographic building blocks
37	11 Sep	10-12	TL	Key establishment and certificate management
	15 Sep	10-12	CJ	User authentication, IAM
38	18 Sep	10-12	CJ	Operating systems security, web, browser and mail security
	22 Sep	10-12	CJ	IT security management and risk assessment
39	25 Sep	10-12	TL	Software security - exploits and privilege escalation
	29 Sep	10-12	TL	Malicious software
40	02 Oct	10-12	CJ	Firewalls and tunnels, security architecture
	06 Oct	10-12	CJ	Cloud and IoT security
41	09 Oct	10-12	TL	Intrusion detection and network attacks
	13 Oct	10-12	TL	Forensics
42				Fall Vacation - No lectures
43	23 Oct	10-12	CJ	Privacy and GDPR
	27 Oct	10-12	CJ	Privacy engineering
44	30 Oct	10-12	CJ,TL	Final guest lecture and Exam Q/A

Recap: Security goals and crypto primitives

In this class, we don’t worry about the intricate details of RSA, AES, or SHA1, but focus on the bigger picture of what we achieve with using symmetric and asymmetric ciphers, cryptographic hash functions, message authentication codes, and digital signatures.

Recap: Cryptosystems



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

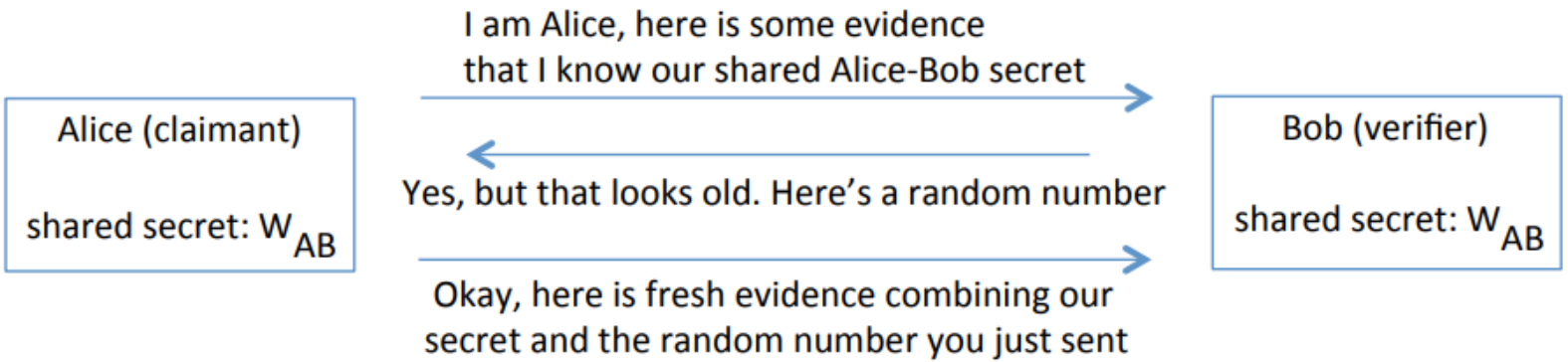
Generated by all parties working together

Asymmetric

Is e really yours?

Key distribution

Basic authenticated key exchange



Developing a key distribution scheme

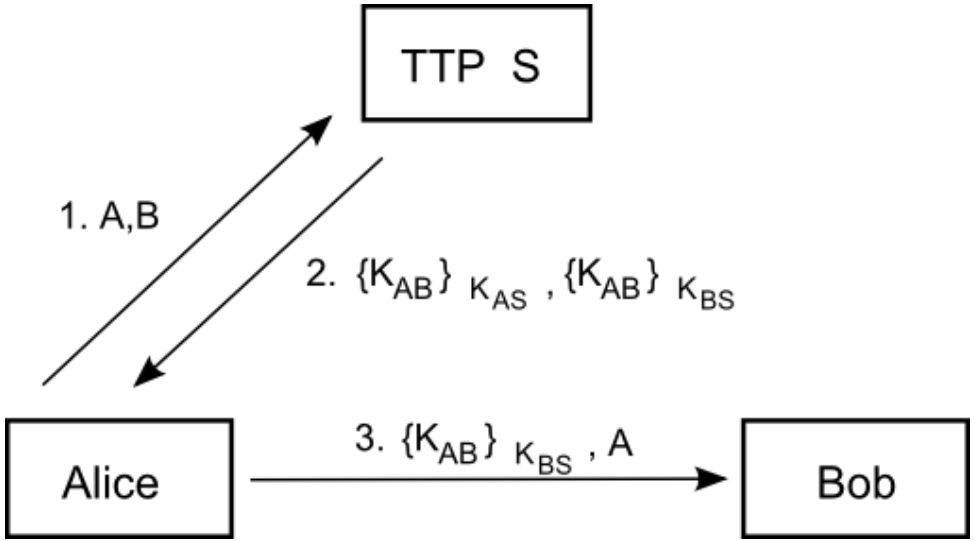
Situation:

- 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

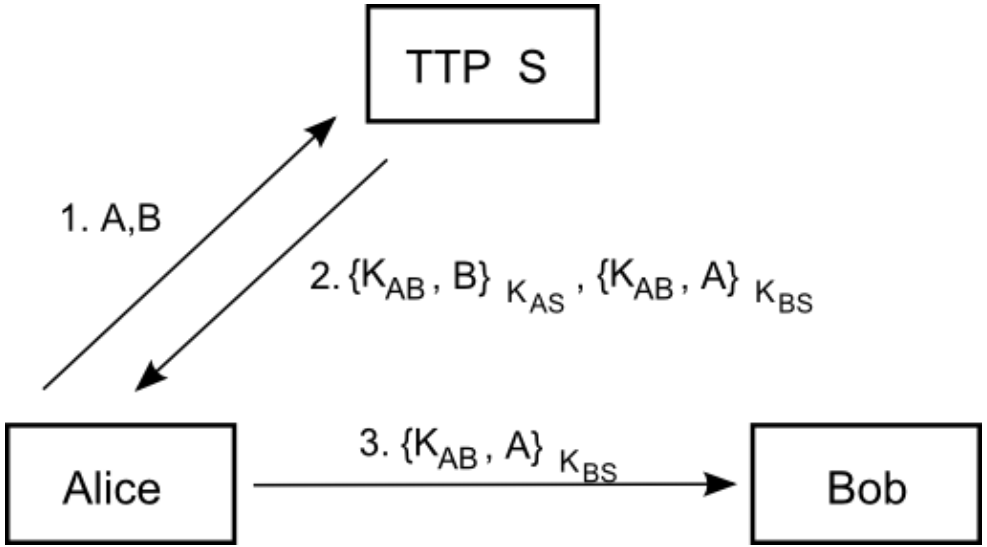
At the end, we want to achieve:

- 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

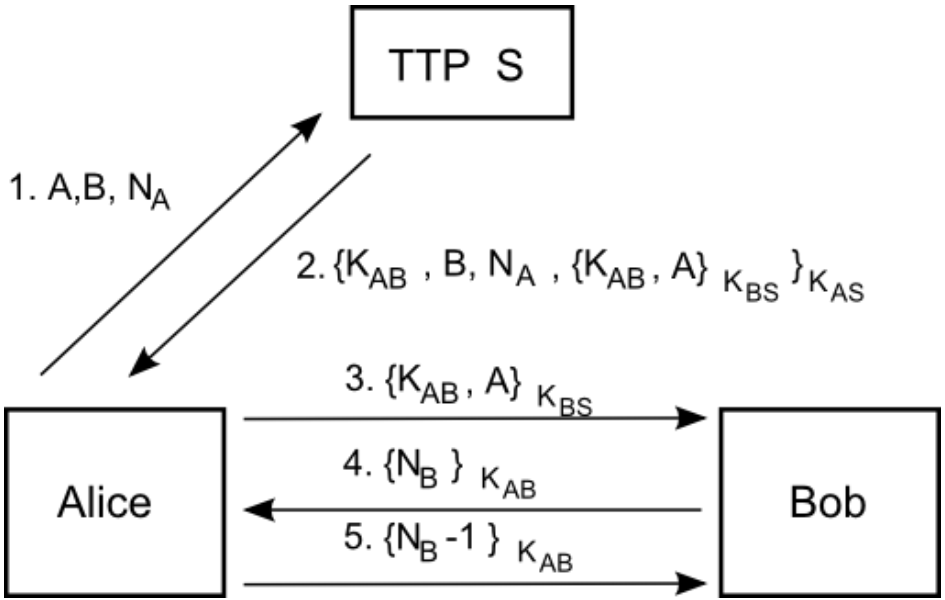
Key distribution



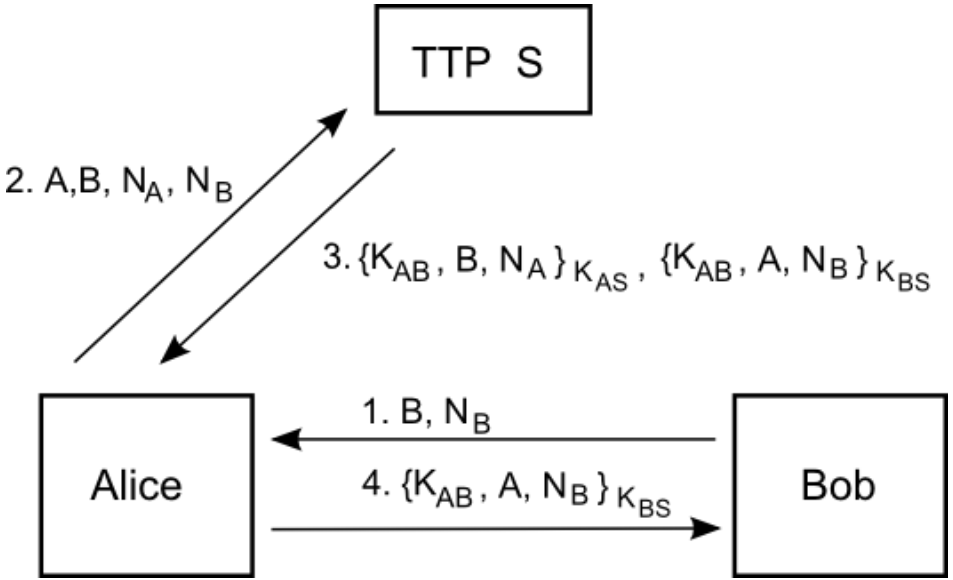
Key distribution



Key distribution



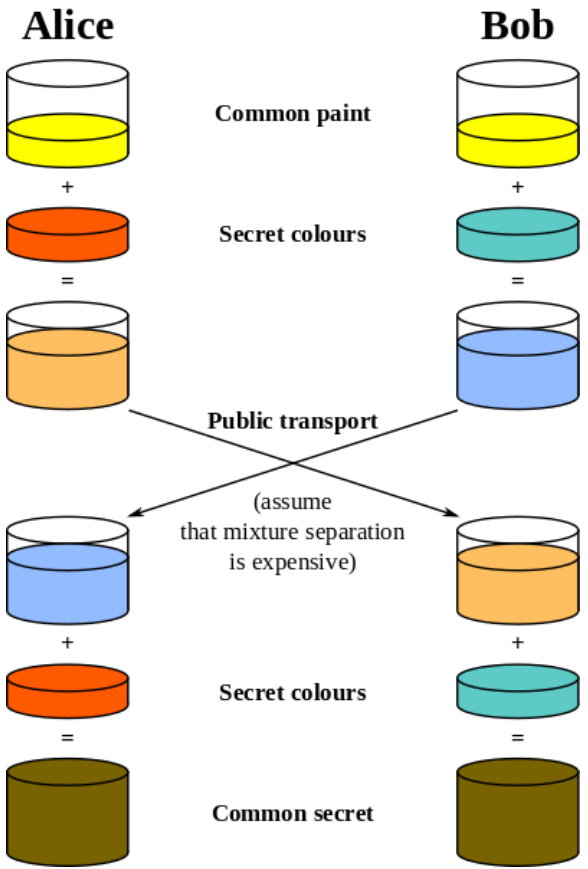
Key distribution



Key agreement

Basic idea

If you wanted to exchange secret paints



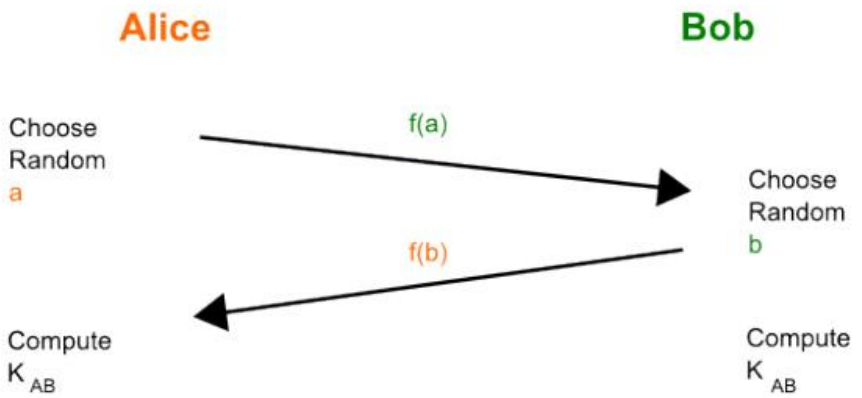
Basic idea

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

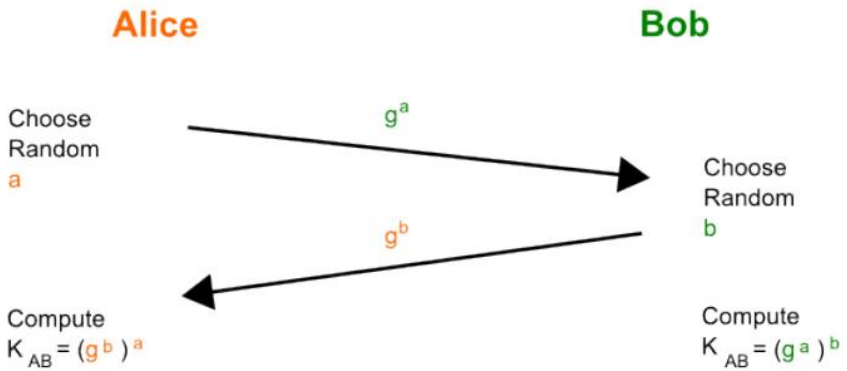
$f(x) = g^x \bmod p$

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



Is *e* really yours?

Public-key infrastructure (PKI)

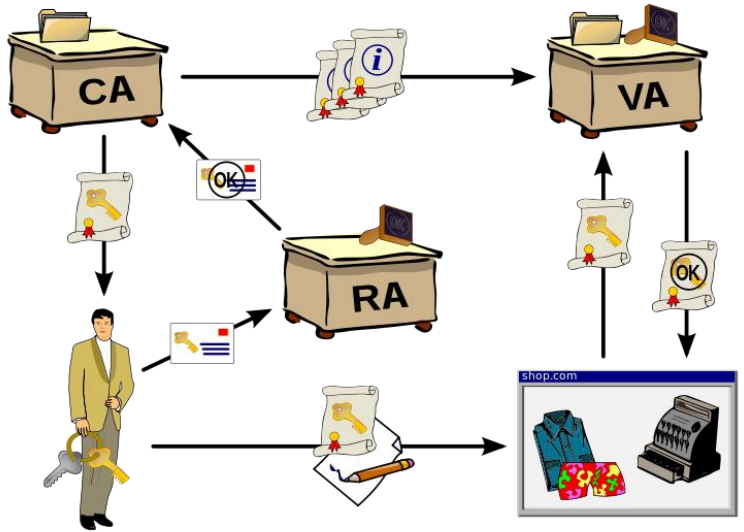
A system for the creation, storage, and distribution of **digital certificates** which are used to verify that a particular public key belongs to a certain entity

X.509 format for certificates include:

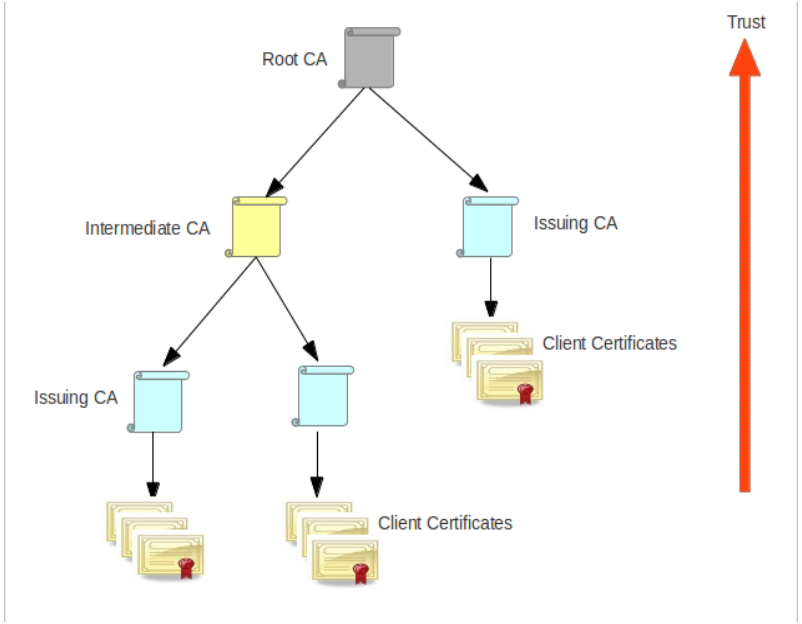
Serial number	– unique identification of certificate
Valid-From/To	– lifespan of the certificate
Subject	– the entity/person/machine/etc. identified
Public key	– the entity's public key
Signature	– the actual signature of the issuer

Issuance and verification

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

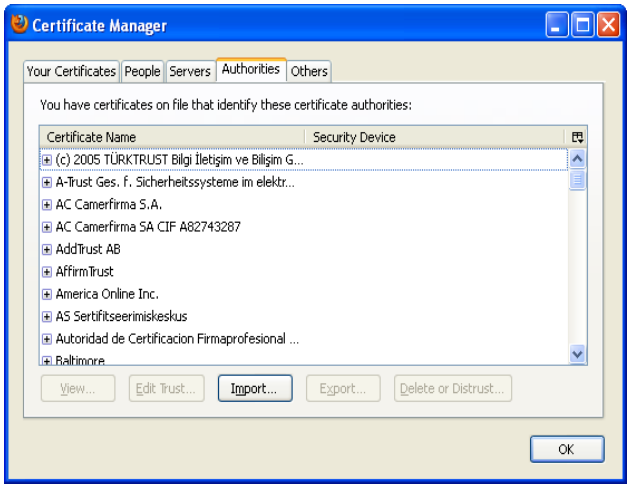


Types of PKI: CA model

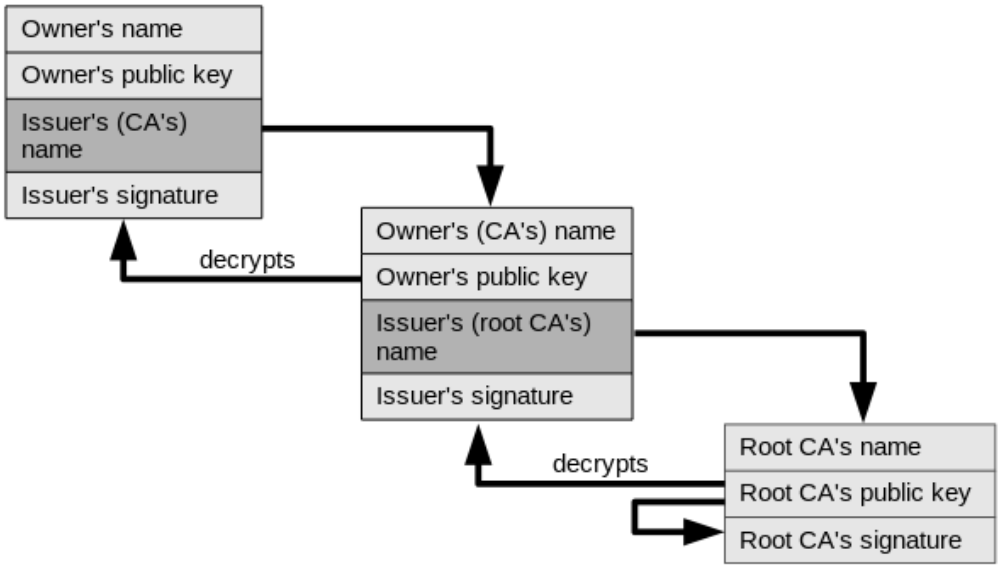


Trust in browsers

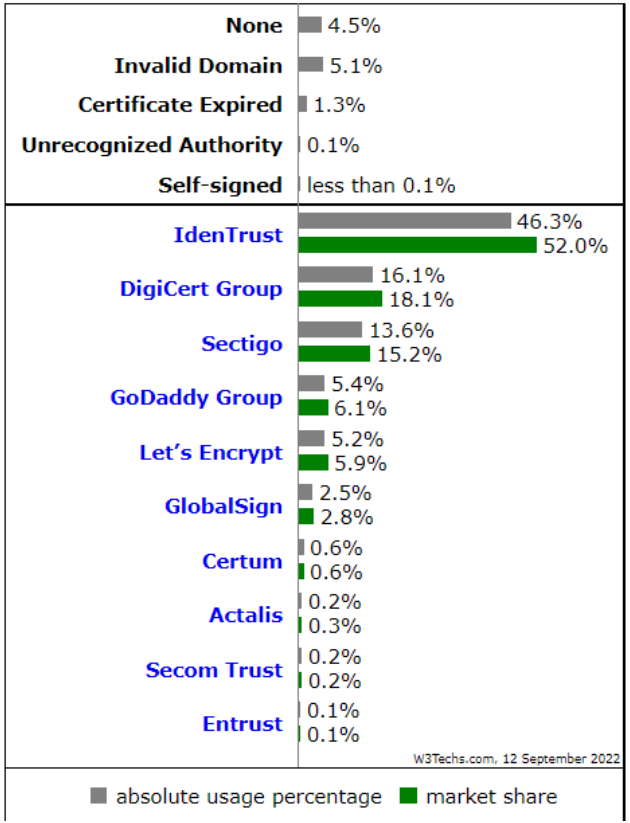
Browsers come pre-configured with a set of root CAs. Do you trust all these CAs (to authenticate properly, to avoid/inform of breaches)?



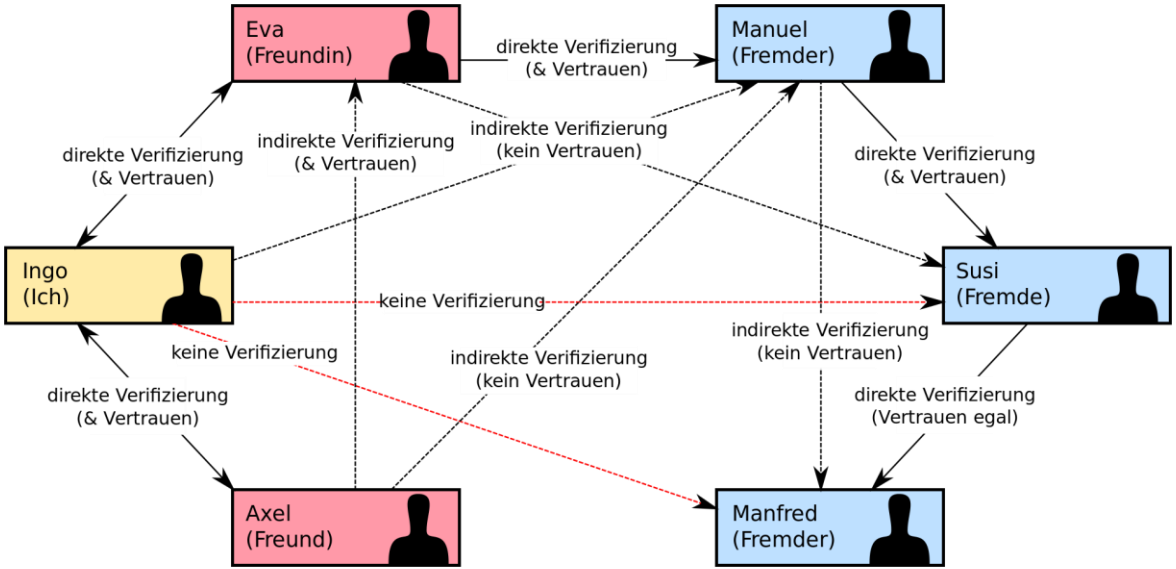
Chain of trust



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	Time	Lecture	Topic
36	04 Sep	10-12	TL	Security concepts and principles
	08 Sep	10-12	TL	Cryptographic building blocks
37	11 Sep	10-12	TL	Key establishment and certificate management
	15 Sep	10-12	CJ	User authentication, IAM
38	18 Sep	10-12	CJ	Operating systems security, web, browser and mail security
	22 Sep	10-12	CJ	IT security management and risk assessment
39	25 Sep	10-12	TL	Software security - exploits and privilege escalation
	29 Sep	10-12	TL	Malicious software
40	02 Oct	10-12	CJ	Firewalls and tunnels, security architecture
	06 Oct	10-12	CJ	Cloud and IoT security
41	09 Oct	10-12	TL	Intrusion detection and network attacks
	13 Oct	10-12	TL	Forensics
42				Fall Vacation - No lectures
43	23 Oct	10-12	CJ	Privacy and GDPR
	27 Oct	10-12	CJ	Privacy engineering
44	30 Oct	10-12	CJ,TL	Final guest lecture and Exam Q/A