IT-Sicherheit

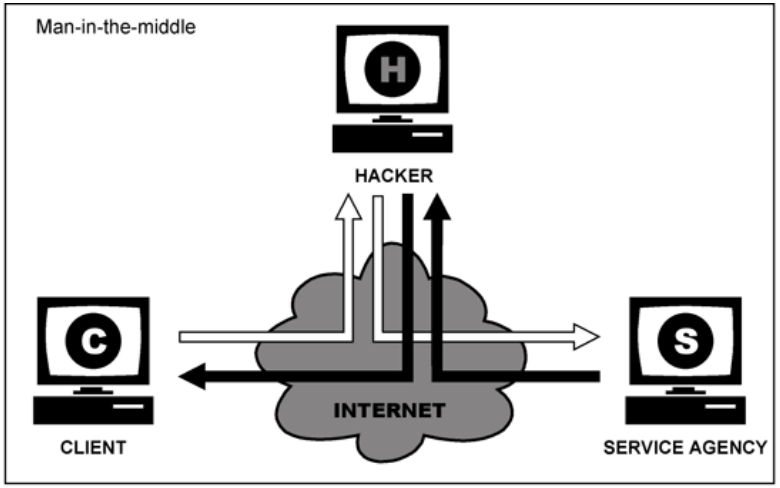
Vertrauen, Zertifikate, PKI

Schlüsselmanagement und Vertrauen

- **Schlüssel (Keys) und ihre Verwaltung sind ein besonders sicherheitskritischer Aspekt in jedem kryptographisch gesicherten System**

- **Zwei Kernprobleme**
  - **Private Schlüssel dürfen nicht in falsche Hände geraten**
  - **Man muss sicher sein, den richtigen Schlüssel zu haben**
    - wg. Man-in-the-Middle-Angriffe (MITM)

- **Mögliche Lösungen**
  - **Web of Trust**
  - **Trusted Third Party**



Web of Trust

- **Die Echtheit von Schlüsseln wird durch ein Netz von gegenseitigen Bestätigungen (Signaturen), kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen („Owner Trust“) bestätigt.**
  - **Schlüssel werden individuell gespeichert („Key-Rings“)**
  - **Schlüssel werden verifiziert durch Überprüfung von Hashes**
    - z.B. PGP, ssh, oder Threema-Messenger (mit QR-Codes)

- **Vorteil**
  - **Vertrauen kann individuell gemanagt werden**

- **Nachteile**
  - **Keine authentifizierte Kommunikation mit Unbekannten**
  - **Viel Sachverstand erforderlich**

Trusted Third Party

- **Wenn Schlüssel nicht in einem Web of Trust Peer-to-Peer ausgetauscht werden können, verwendet man i.d.R. eine vertrauenswürdige dritte Partei („Trusted Third Party“, TTP)**

- **Der Grad des Vertrauens kann variieren**
  - **Beispiel symmetrische Verschlüsselung (Kerberos als TTP)**
    - Der TGS kennt jeden Shared Secret Key und kann somit jede Nachricht entschlüsseln
  - **Beispiel asymmetrische Verschlüsselung (Public Key-Verfahren)**
    - Hier vertraut man der TTP „nur“, dass der richtige Public Key bereit gestellt wird, der Private Key ist der TTP i.d.R. nicht bekannt.

- **TTPs können auch noch andere Aufgaben übernehmen**
  - **Time-Stamping-Server, Beweishüter, Datentreuhänder, Zustellungsagent und „vollstreckendes“ Organ**
  - **Vergl. Notar im analogen Leben**

Public Key Infrastructure (PKI)

- **Was ist PKI?**
  - **Eine PKI ist eine TTP für die Nutzung von Public-Key Kryptographie**
  - **Eine Public Key Infrastructure stellt Komponenten und Dienste zur Verfügung, um digitale Zertifikate zu verwalten, d.h.**
    - Ausstellen
    - Verteilen
    - Prüfen
    - Zurückziehen

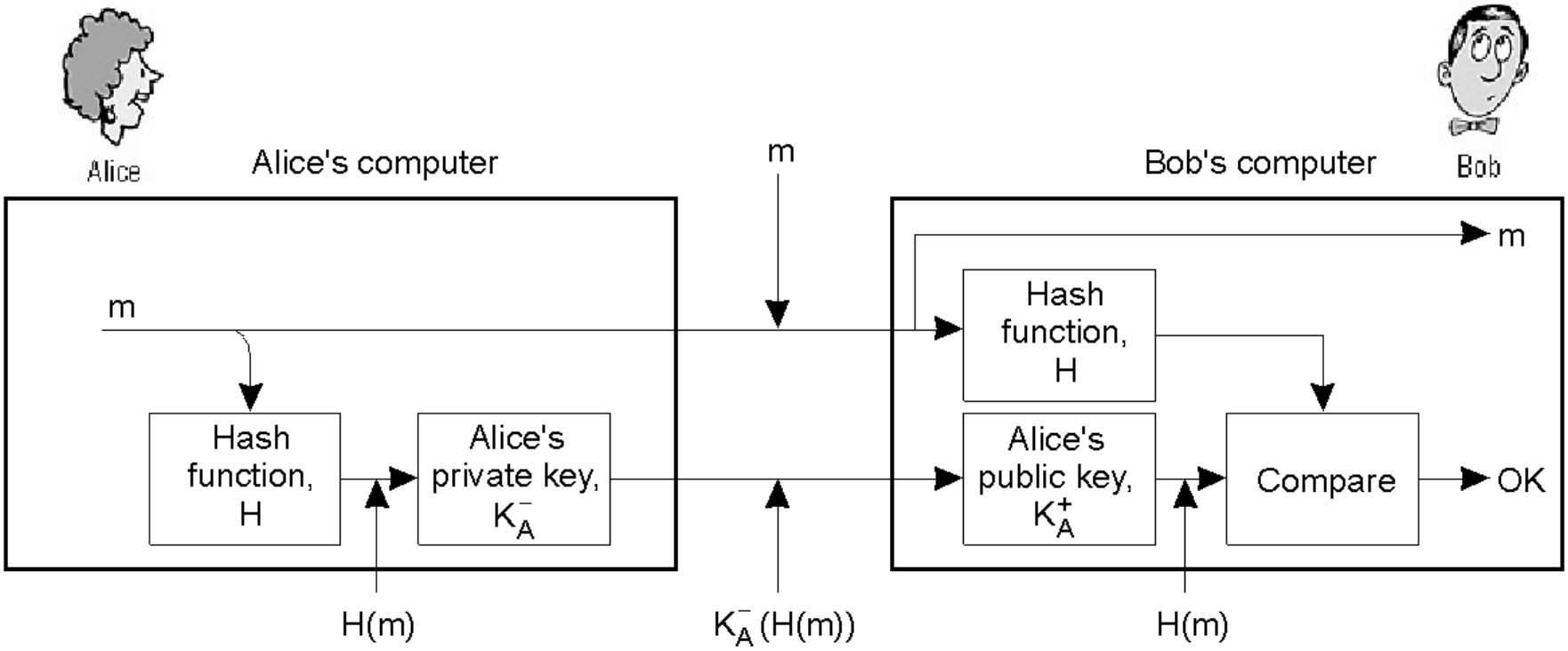
PKI Anwendungen (1)

- **Gegenseitige Authentifizierung und Verschlüsselung**
  - **Web-Dienste**
    - HTTPS
  - **Authentifizierung von Bürgern für Verwaltungs- und Geschäftszwecke**
    - eID (Personalausweis)
  - **Benutzer und Geräte**
    - Remote User: VPN
    - Internes Netzwerk: 802.1x (LAN, WLAN)
  - **2-Faktor-Authentifizierung (Smart Cards)**
- **Starke Verschlüsselung**
  - **Datenträger und Dateien**
    - z.B. EFS

PKI Anwendungen (2)

- **Sichere E-Mails**
  - S/MIME
  - Innerhalb des Unternehmens
  - Kommunikation mit externen Geschäftspartnern
- **Signierung von Dokumenten**
  - Signaturgesetz: z.B. Rechnungen
  - Intern: z.B. Audit-Logs
- **Signierung von Code, Macros, urheberrechtlich geschütztem Material**

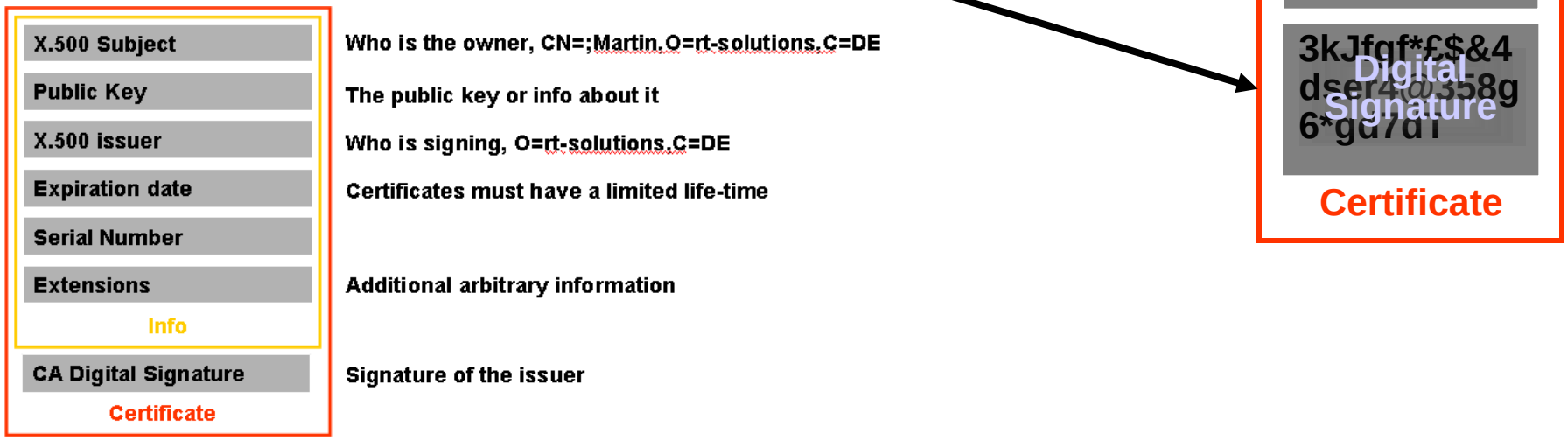
Digital Signaturen



- **Digital Signatur mit einem Public-Key Verfahren und einer Hash-Funktion**

Was ist ein Zertifikat?

- **Bestandteile:**
  - Ein öffentlicher Schlüssel
  - Informationen über die Instanz, die zertifiziert wurde
- **Digital signiert von einer vertrauenswürdigen Instanz**



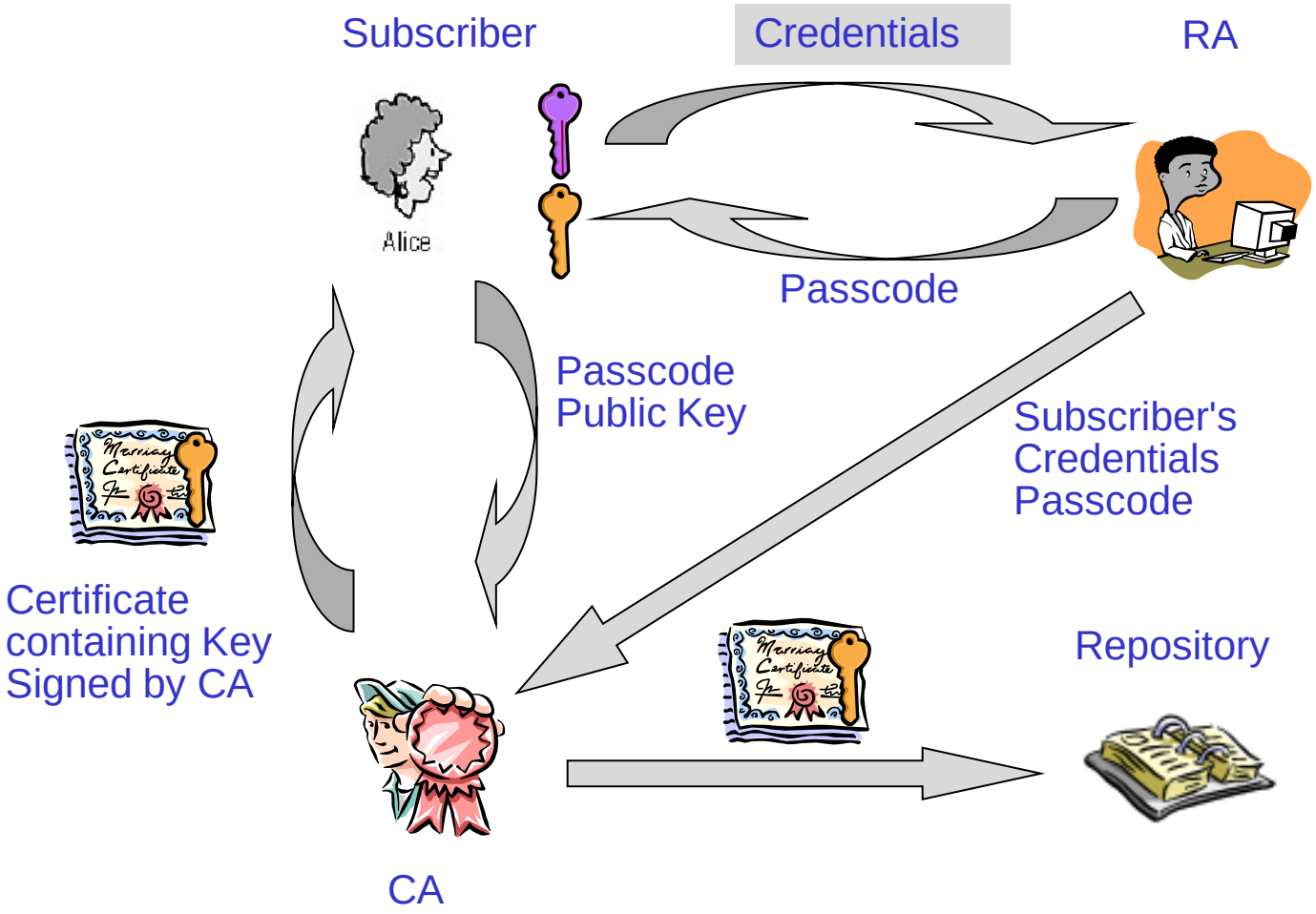
PKI Komponenten (1)

- **Root CA (Certificate Authority)**
  - Oberste Instanz der Vertrauenskette
  - Jeder vertraut dieser Instanz
  - Stellt Zertifikate aus
- **Subordinate CA**
  - CA innerhalb einer mehrstufigen CA-Hierarchie
- **Registration Authority (RA)**
  - Authentifizierung der zu zertifizierenden Benutzer/Geräte, *bevor* eine Zertifizierung erfolgen darf
  - Die Stärke der Authentifizierung kann als Klassifizierung für Zertifikate dienen

PKI Komponenten (2)

- **Directory**
  - Speichert Identitäten und deren öffentliche Schlüssel
- **Ggf. Validation Authority**
  - Erhält Listen von gesperrten Zertifikaten von CA
  - Beantwortet online Anfragen bei der Überprüfung
- **Personal Security Environment**
  - Speichert privaten Schlüssel eines Teilnehmers

Prozess der Erstellung eines Zertifikats



Standard: X.509

- ITU-T-Standard für eine Public-Key-Infrastruktur
  - Seit 1998, aktuell Version 3
- Bestandteile eines Zertifikats

Zertifikat
- Version
- Seriennummer
- Algorithmen-ID
- Aussteller
- Gültigkeit
  - von
  - bis
- Zertifikatinhaber
- Zertifikatinhaber-Schlüsselinformationen
  - Public-Key-Algorithmus
  - Public Key des Zertifikatinhabers
- Eindeutige ID des Ausstellers (optional)
- Eindeutige ID des Inhabers (optional)
- Erweiterungen

Zertifikat-Signaturalgorithmus

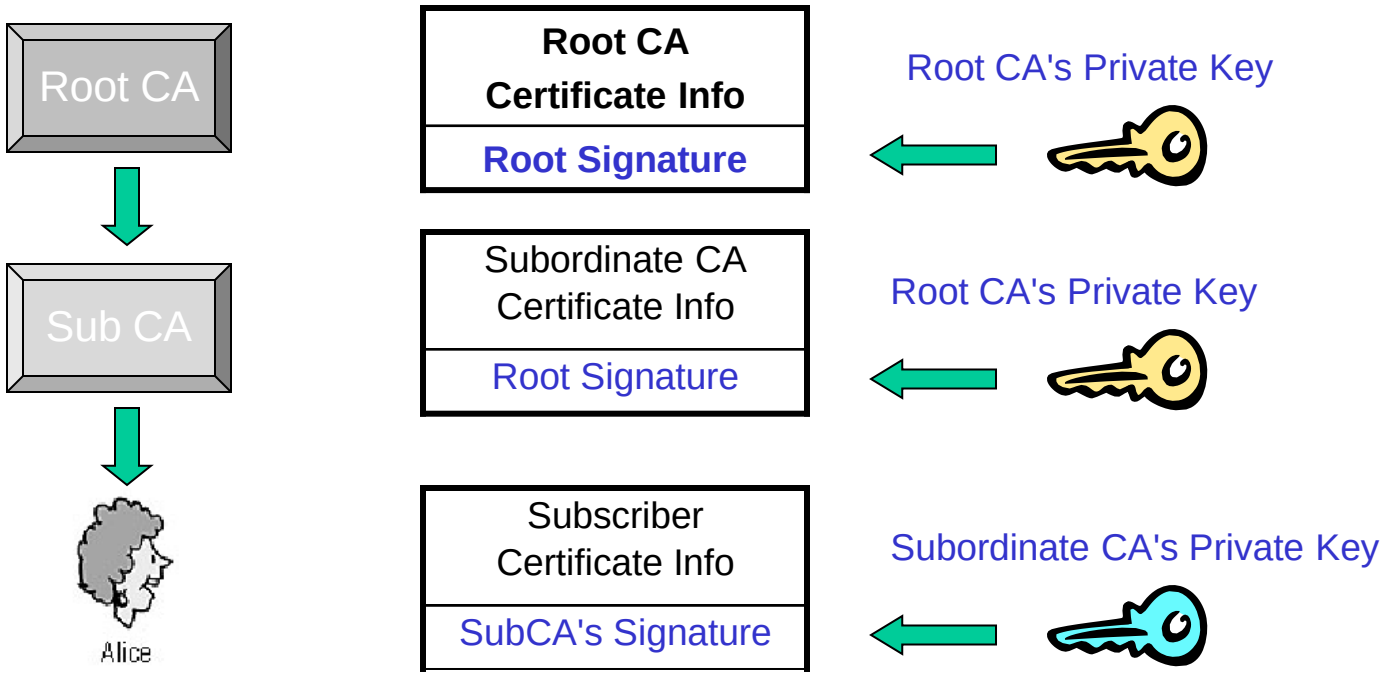
Zertifikat-Signatur

In den Erweiterungen
Alles durch die Signatur bestätigt
- Alternativer Name (z.B. Email-Adresse)
- Zweck (z.B. Server-Authentifikation, Email, CA)
- URI der CRL
- URI des OCSP-Responders
- URI von CP/CPS

Weitere Public-Key Cryptography Standards (PKCS)

- **PKCS#7**
  - Cryptographic Message Syntax Standard (RFC 5652)
  - Bildet die Basis für S/MIME und wird zum Signieren und/oder Verschlüsseln von Nachrichten einer PKI genutzt.
- **PKCS#10**
  - Certification Request Standard (RFC 2986)
  - Format der Nachrichten, die zu einer CA gesendet werden, um die Zertifizierung eines Schlüsselpaares zu erfragen.
- **PKCS#12**
  - Personal Information Exchange Syntax Standard (RFC 7292)
  - Dateiformat, das dazu benutzt wird, private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern.

Zertifizierungspfad

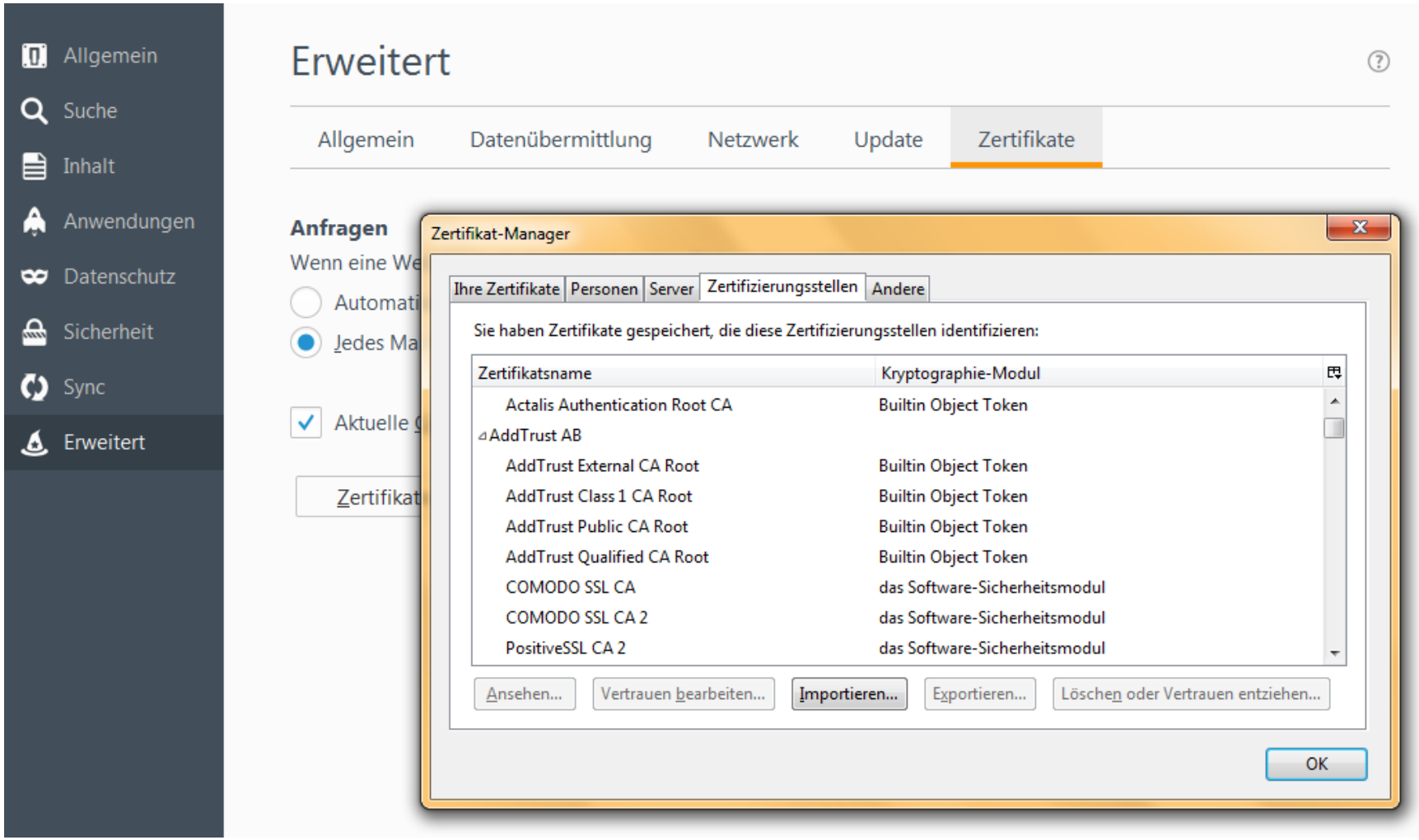


Prüfung eines Zertifikates

- **Vertrauensprüfung**
  - **Vertraut man der Root CA oder explizit einer Subordinate CA**
  - **Steht eine der CAs auf dem Pfad eventuell auf einer Black-List**
- **Gültigkeitszeitraum**
  - **Alle Zertifikate auf dem Pfad müssen noch gültig sein**
    - D.h. kein Zertifikat läuft länger als das seiner ausstellenden CA
    - Root-CA haben typische Gültigkeiten von 10-20 Jahren
- **Zweck**
  - **Muss dem intendierten entsprechen**
- **Widerruf**
  - **Wurde die Seriennummer in der Zwischenzeit widerrufen**

- **Signaturprüfung**
  - **Aller Zertifikate auf dem Pfad**

Vertrauen durch vorinstallierte Root CAs



Zertifizierungsrichtlinien

- Vertrauen soll durch Auditierung der Policy und Prozesse der CA gesichert werden
- CP - Certificate Policy
  - Zertifizierungsrichtlinien
- CPS - Certification Practise Statement
  - Ausführungsbestimmungen der Zertifizierungsrichtlinien
- Nach RFC 3647
  - Legen die Prozesse der PKI und die zugesicherten Eigenschaften der Zertifikate fest

eIDAS–Verordnung (1)

- **electronic IDentification, Authentication and trust Services**
  - **EU-Verordnung seit 2016**
    - https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html
  - **Somit unmittelbar geltendes Recht in allen 28 EU-Mitgliedstaaten sowie im Europäischen Wirtschaftsraum**

- **Deutsches Vertrauensdienstegesetz (VDG) ergänzt 2017 die eIDAS–Verordnung (EU) Nr. 910/2014**
  - **löste das alte (und impraktikable) Signaturgesetz (SigG) von 2001 ab**
  - **bestimmt die Mitwirkungspflichten der Anbieter**
    - Erstellung, Überprüfung und Validierung von elektronischen Signaturen
  - **legt die zuständige nationale Aufsicht fest**

  - **Regelt Aufsichten**
    - **Bundesnetzagentur**: elektronische Signaturen, Siegel, Zeitstempel und Einschreiben-Zustelldienste
    - **BSI**: Webseiten-Zertifikate

eIDAS–Verordnung (2)

- **Elektronische Identifizierung**
  - zur Identifizierung von natürlichen oder juristischen Personen
  - keine Harmonisierung von nationalen eID-Systemen
  - aber Interoperabilität zwischen den Systemen
  - nationalen Systeme können bei der Kommission notifiziert werden
  - Notifizierung auf freiwillig, aber Anerkennung notifizierter eIDs ist verpflichtend

  - Vertrauensniveaus "niedrig", "substanziell" und "hoch“
  - "substanziell" oder "hoch" wird nur anerkannt, wenn auf dem entsprechenden Vertrauensniveau notifiziert ist

eIDAS–Verordnung (3)

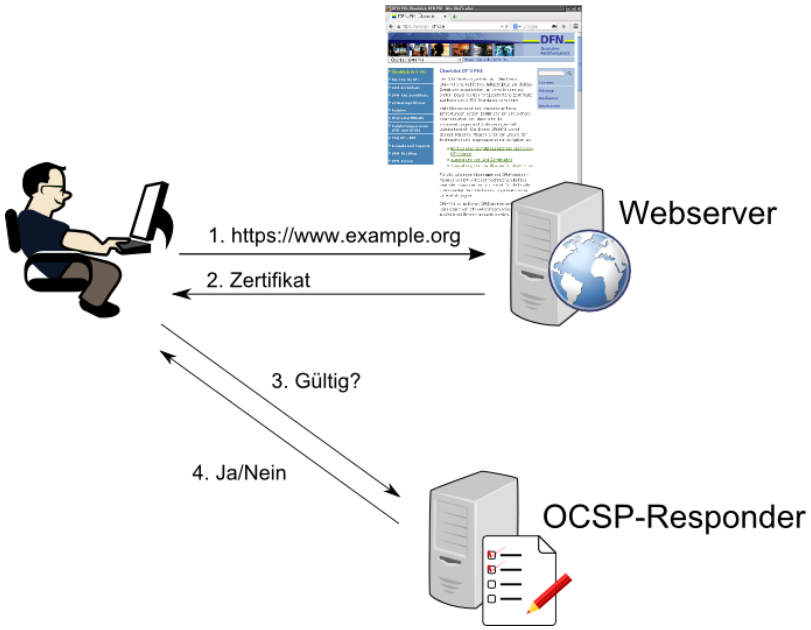
- **eIDAS-Verordnung sieht Vertrauensdienste vor für**
  - Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln
  - Zustellung elektronischer Einschreiben
  - Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung
  - Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten

Widerruf von Zertifikaten (1)

- „Certificate Revocation“, erforderlich wenn
  - ein privater Schlüssel kompromittiert wurde
  - ein Benutzer oder Gerät gesperrt werden soll
- CA stellt signierte Certificate Revocation List (CRL) aus
  - Beinhaltet Seriennummern der widerrufenen Zertifikate
  - Typische Ablageorte: Active Directory, FTP- oder Webserver
- CRLs haben eine Gültigkeit
  - Typisch: Tage
  - Können beim Validierer gecachet werden
  - Nachteil: keine kurzfristige Sperrung möglich

Widerruf von Zertifikaten (2)

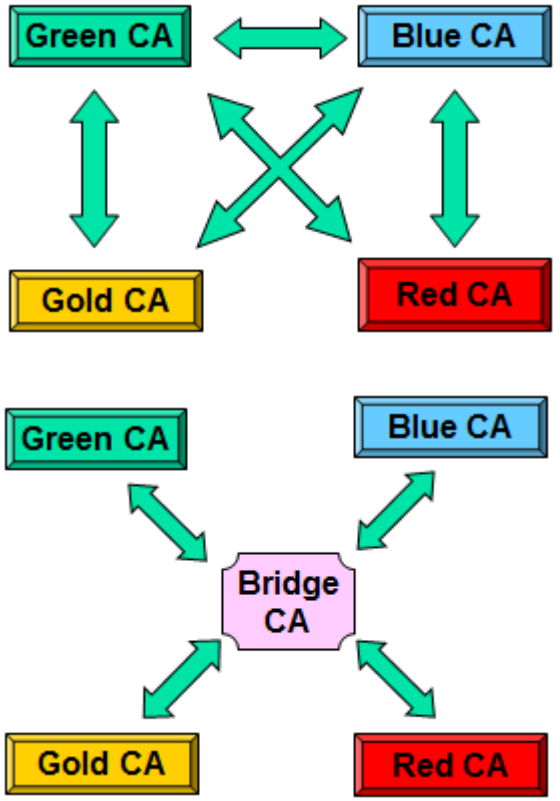
- **Online Certificate Status Protocol (OCSP, RFC 6960)**
  - Netzwerkprotokoll, um den Status von X.509-Zertifikaten bei einem Validierungsdienst abzufragen
  - „OCSP-Responder“ erhält aktuelle CRL der CA und beantwortet nur, gesperrt oder nicht
  - Keine weitere Prüfung
- **Online-Sperrinformationen**
  - Erfordert Netzwerkverbindung
  - Kann auch bei „OCSP Stapling“ über den Webserver ausgeliefert werden (aktuell signiert vom OCSP-Responder)



Vertrauensmodelle

- **Hierarchisch**
  - **Klassisches Modell einer Unternehmens-PKI**

- **Cross-Zertifizierung**
  - **Zertifizierung über PKI-Grenzen hinweg**
    - z.B. zwischen PKI verschiedener Unternehmen oder Länder
  - **Bridge CA als Lösung für quadratisch wachsende Zahl von Cross-Zertifikaten**



Problem: Schlüsselverlust

- **Im klassischen Modell der PKI kennt nur der Subscriber den Private Key**
  - **Was passiert, wenn der verloren geht (z.B. SmartCard defekt)?**
  - **Wenn das Unternehmen die Daten eines Mitarbeiters entschlüsseln muss (z.B. Revision)**

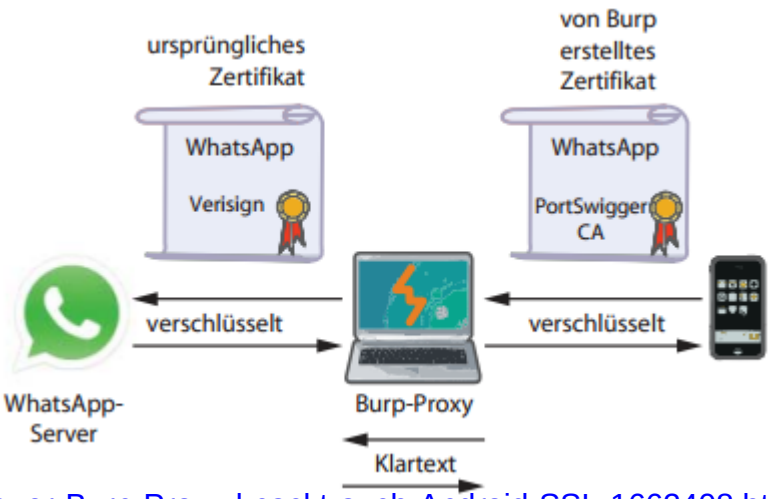
- **Lösung 1: Neues Zertifikat**
  - **Akzeptabel für alle Authentifizierungs-Zertifikate**
  - **Nutzlos, wenn Daten mit dem Public Key verschlüsselt wurden**
    - Z.B. Festplatten- oder Emailverschlüssselung

- **Lösung 2: Schlüssel-Backup**
  - **Bei der CA**
    - aber CA kennt dann alle Schlüssel
  - **Verschlüsselt mit Recovery-Schlüssel**
    - Recovery-Prozess erforderlich (ggf. 4-Augen-Prinzip)

Problem: Kompromittierte CA

- **CA Private Key gestohlen oder CA-Betreiber nicht mehr vertrauenswürdig**
  - **Ist in der Vergangenheit bereits öfter passiert (z.B. „DigiNotar“)**
  - **Root CA/Subordinate CA kommt auf Blacklist**

- **Was, wenn das nicht bekannt ist (ggf. staatliche Eingriffe)?**
  - **CA stellt absichtlich falsche neue Zertifikate aus**
  - **Dienen zur Authentifikation eines MITM**
    - Abhören, Code Injection
  - **Auch Web-Proxies können das, um TLS-Verbindungen aufzubrechen und zu scannen.**
    - Dann muss die eingebaute CA des Proxies als vertrauenswürdig eingetragen sein



http://www.heise.de/security/meldung/Neuer-Burp-Proxy-knackt-auch-Android-SSL-1662408.html

HTTP Public Key Pinning (1)

- **Vorschlag von Google, definiert in RFC 7469**
  - **Unterstützt in Chrome und Firefox**
- **Schutz gegen den unbemerkten Austausch von Zertifikaten**
  - **Im HTTP-Header werden genannt**
    - Key-Hashes von gültigen Keys (mind. 2)
    - Maximales Alter
    - Eine URL zum Melden von Fehlern (Angriffen?)
  - **Beim ersten Zugriff werden diese im Browser gecachet**
  - **Kann Schlüssel des Zertifikats oder einer ausstellenden CA sein**

```
Public-Key-Pins: max-age=5184000;
pin-sha256="jYEKhFo1FULVqIk/Nph3hu1SDWhifZamgYGxnk3Zuys=";
pin-sha256="h0h88SscIXy94RvNI7O2CDUpuCwXL1WvX1jH8Hb1/9A=";
includeSubdomains;
report-uri="https://example.com/hpkp.php"
```

HTTP Public Key Pinning (2)

- **Probleme**
  - **Funktioniert nicht, wenn MITM schon beim ersten Zugriff aktiv ist**
  - **Probleme beim Schlüsselwechsel**
    - z.B. wg. Verlust/Korrumpierung des Private Keys
    - Deswegen mind. 2 Keys oder CA-Key
  - **Fehler/Angriffs-Meldung kann vom MITM abgefangen werden**