

# Einführung in Public Key Infrastrukturen (PKI)

Kryptologie ICS.KRYPTO

Prof. Armand Portmann

**Informatik**

6. Mai 2024

## **Lernziele**

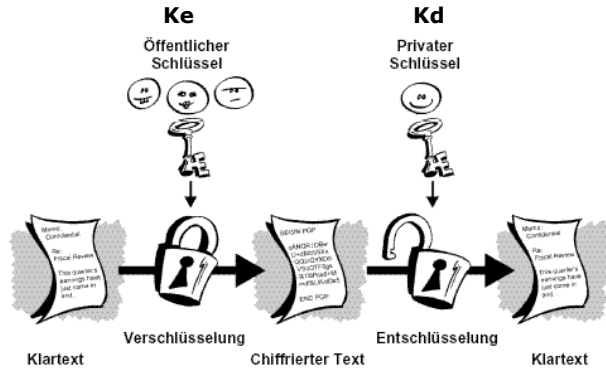
- Sie kennen die Mechanismen, die PKI-Verfahren zugrunde liegen (verschlüsseln, signieren)
- Sie wissen, wann öffentliche und wann private Schlüssel beim Einsatz von PKI-Verfahren zur Anwendung gelangen
- Sie wissen, worauf beim Beantragen von Zertifikaten zu achten ist
- Sie wissen, wie Zertifikate erzeugt werden
- Sie kennen die wichtigsten Key-Management-Aspekte beim Umgang mit öffentlichen und privaten Schlüsseln
- Sie wissen, aus welchen Komponenten eine PKI aufgebaut ist und welche Aufgaben diese haben
- Sie wissen, wie Zertifikate überprüft werden und welche Rolle dabei Zertifikatsketten spielen

## **Inhaltsübersicht**

- Kurze Repetition asymmetrische Verschlüsselung und digitale Signaturen
- Signieren und Verschlüsseln anhand eines praktischen Beispiels
- Sicherheitsanforderungen an private und öffentliche Schlüssel
- Zertifikate und ihr Lebenszyklus (Erzeugung, Erneuerung, Ungültigkeitserklärung)
- Bausteine einer Public Key Infrastruktur
- Prüfen der Gültigkeit von Zertifikaten
- Zertifikatsketten

# **Repetition Verschlüsseln und Signieren**

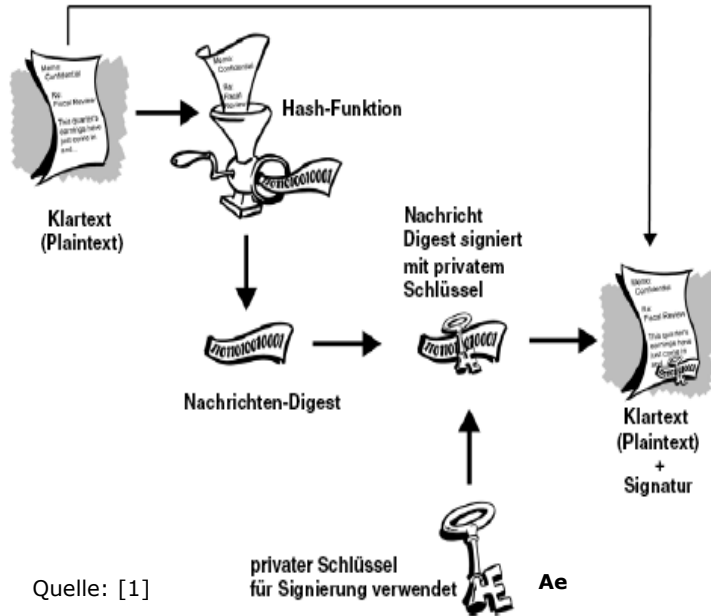
# Asymmetrische Verschlüsselung



Quelle: [1]

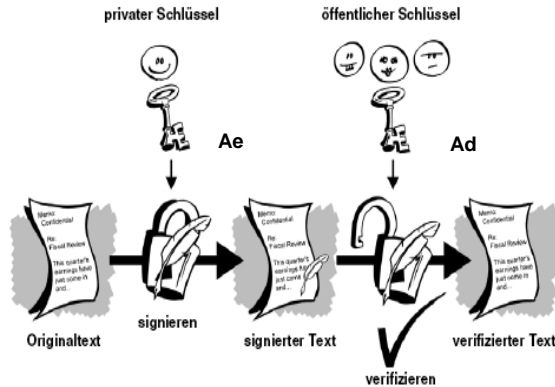
- Unterschiedliche Schlüssel zum Ver- und Entschlüsseln ( $K_e$ ,  $K_d$ )
- Jeder Teilnehmer hat ein Schlüsselpaar
  - $K_e$ : öffentlicher Schlüssel (public key, encrypt key)
  - $K_d$ : privater Schlüssel (private key, decrypt key)
- Aus der Kenntnis des einen Schlüssels lassen sich keine Rückschlüsse auf den anderen Schlüssel ziehen
- Algorithmen: RSA, Elliptische Kurven, El Gamal auf Basis Diffie Hellmann

## Digitale Signatur – Erstellung



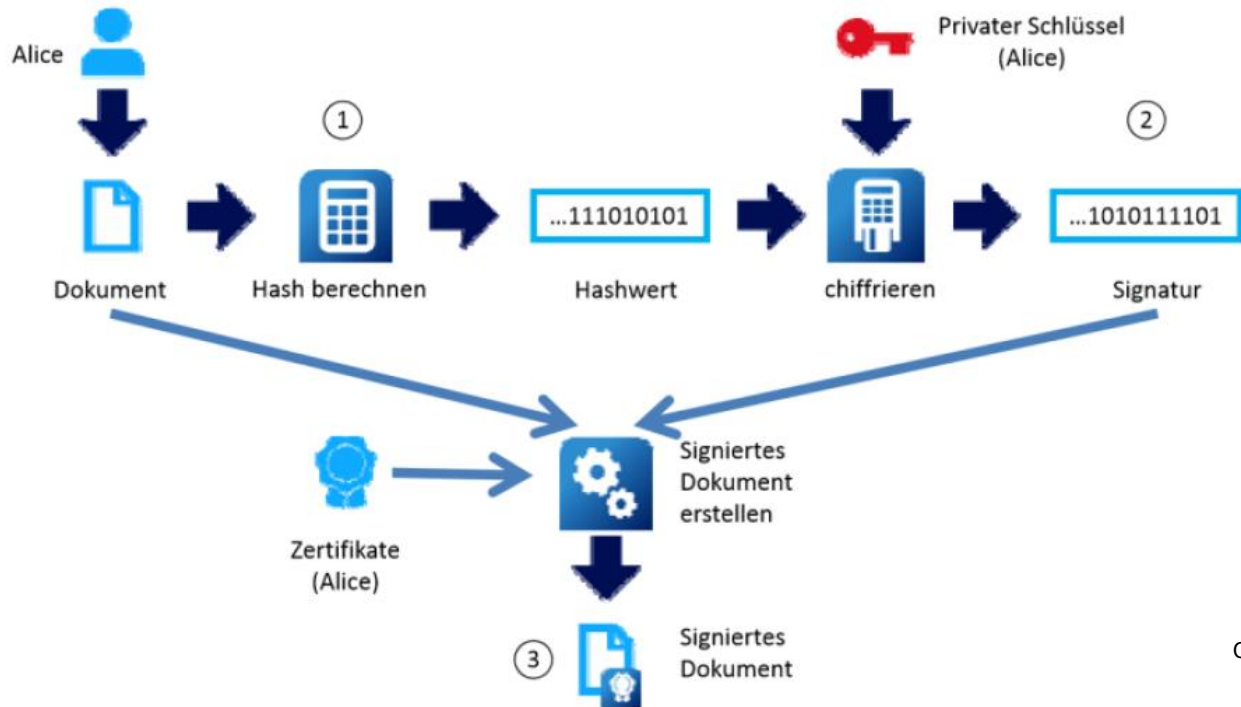
- Beim Signieren mit RSA wird der Hash-Wert einer Meldung mit dem privaten Schlüssel verschlüsselt

## Digitale Signatur – Erstellung und Verifikation



- Ae: privater Schlüssel (private key, encrypt key)  
➔ Zum Erstellen der Signatur
- Ad: öffentlicher Schlüssel (public key, decrypt key)  
➔ Zum Verifizieren der Signatur
- Hinweis: Bei Verschlüsselung gerade umgekehrt!

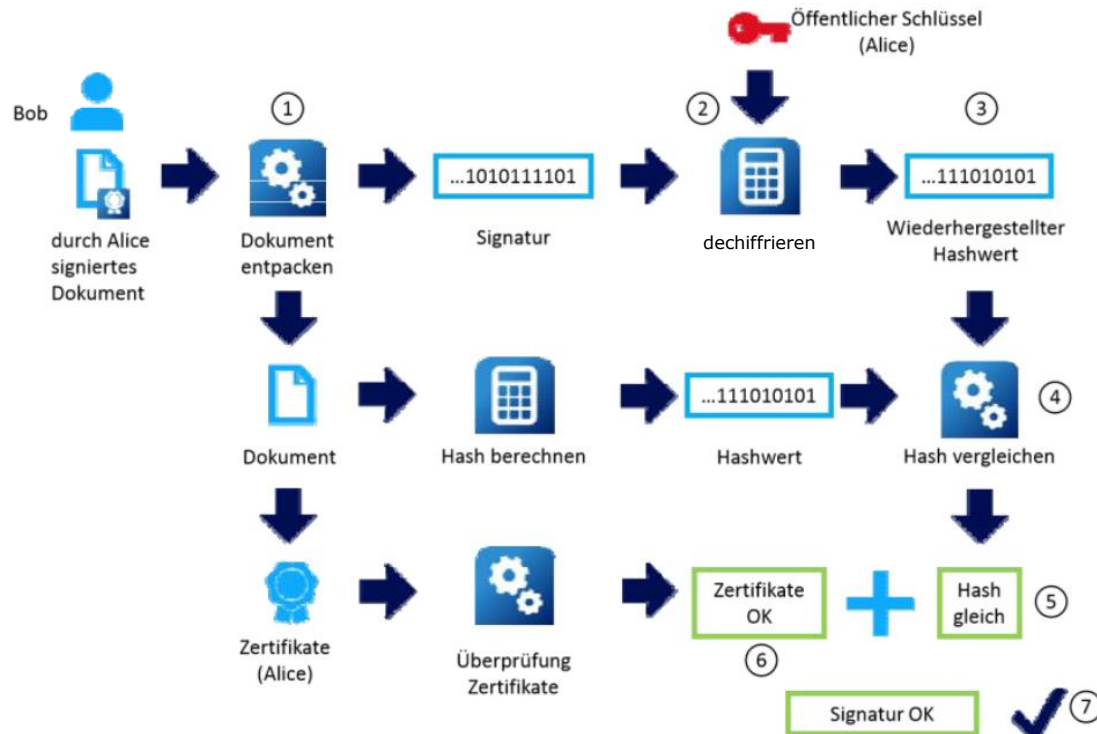
## Digitale Signatur – Erstellung



Quelle: [2]



## Digitale Signatur – Verifikation



## **Eigenschaften von digitalen Signaturen**

Digitale Signaturen...

- beweisen die Integrität (=Unverändertheit) von Dokumenten (Unterschied zur handschriftlichen Unterschrift!).
- beweisen die Authentizität (=Urheberschaft, Echtheit) von Dokumenten.
- können effizient erstellt und verifiziert werden (obwohl asymmetrische Algorithmen etwa 1000-mal langsamer sind als symmetrische Algorithmen).

## Rekapitulation Verschlüsseln und Signieren





	<b>Öffentlicher Schlüssel</b>	<b>Privater Schlüssel</b>
<b>Authentizität</b>	Signatur überprüfen	Signatur erstellen
<b>Vertraulichkeit</b>	Verschlüsseln	Entschlüsseln

Aufgabe:

Ordnen Sie die folgenden vier Vorgänge je einem der obigen vier Tabellenfelder zu:

«Signatur überprüfen», «Entschlüsseln», «Verschlüsseln», «Signatur erstellen»

## Rekapitulation Verschlüsseln und Signieren

	Sender  has	Recipient  has
 Signing		
 Encrypting		

Aufgabe:

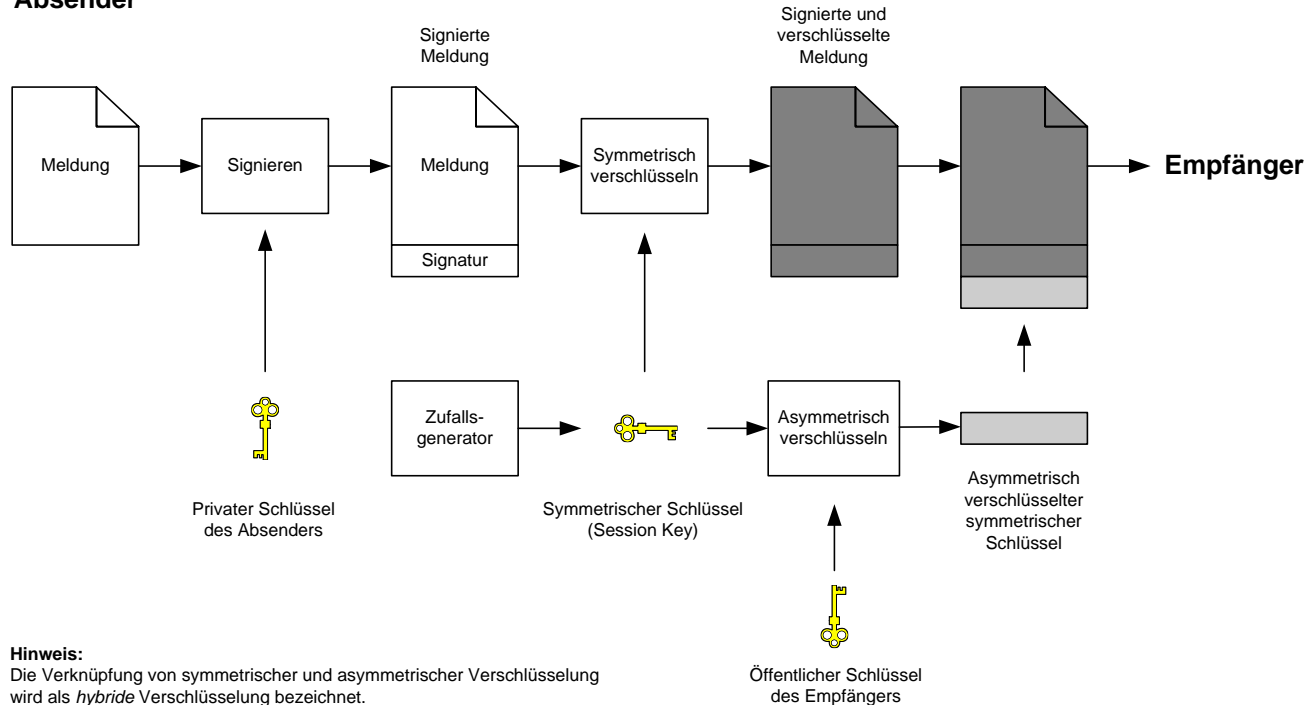
Ordnen Sie die folgenden vier Schlüssel je einem der obigen vier Tabellenfelder zu:

«Sender private key», «Recipient public key», «Sender public key», «Recipient private key»

# **Signieren und Verschlüsseln am praktischen Beispiel**

## Anwendungsbeispiel: Signieren und Verschlüsseln einer E-Mail

### Absender

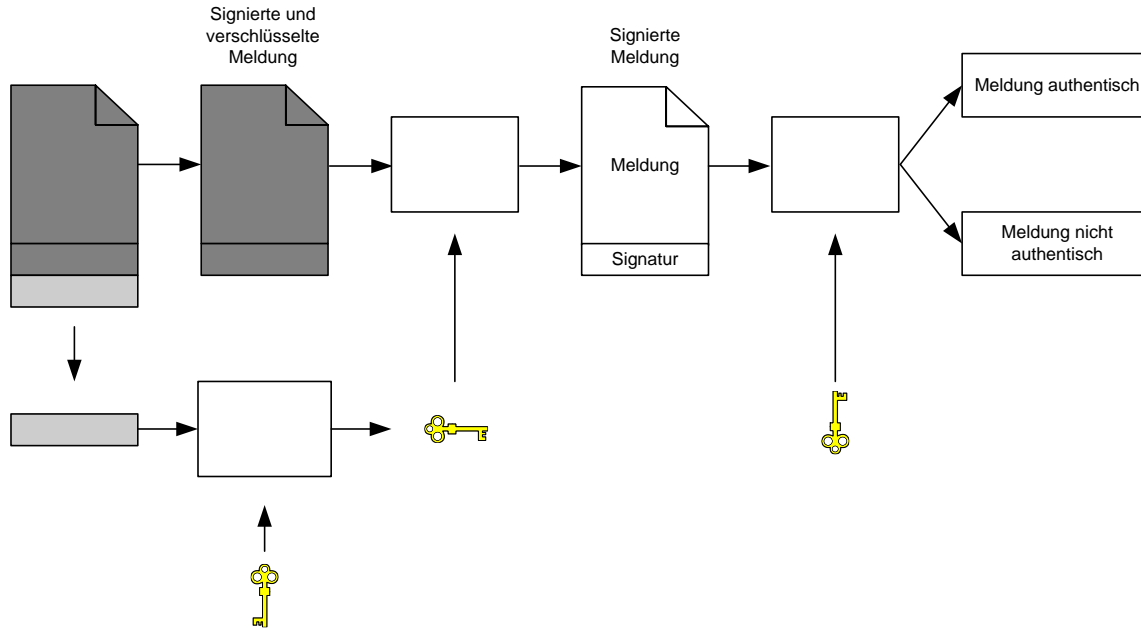


#### Hinweis:

Die Verknüpfung von symmetrischer und asymmetrischer Verschlüsselung wird als *hybride* Verschlüsselung bezeichnet.

## Anwendungsbeispiel: Entschlüsseln und Verifizieren einer E-Mail

### Empfänger



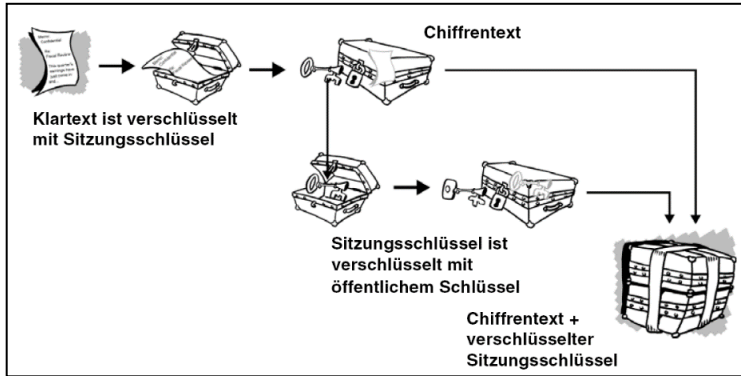
## **Bemerkungen zum Verschlüsseln und Signieren**

Reihenfolge von Signieren und Verschlüsseln bei gleichzeitiger Anwendung:

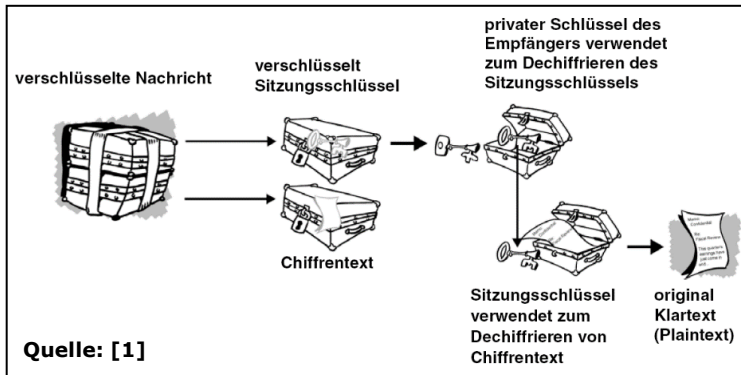
- Zuerst wird signiert, dann wird verschlüsselt
- Begründung: Die Signatur soll die Authentizität des Klartext-Dokuments belegen und durch die Entschlüsselung nicht verloren gehen



## Rekapitulation Hybride Verschlüsselung



Senderseite



Empfängerseite

# **Sicherheitsanforderungen an private und öffentliche Schlüssel**

## **Diskussion**

- Was muss beim öffentlichen Schlüssel sichergestellt sein?
- Worauf muss bei der Ablage des privaten Schlüssels geachtet werden?

## **Diskussion**

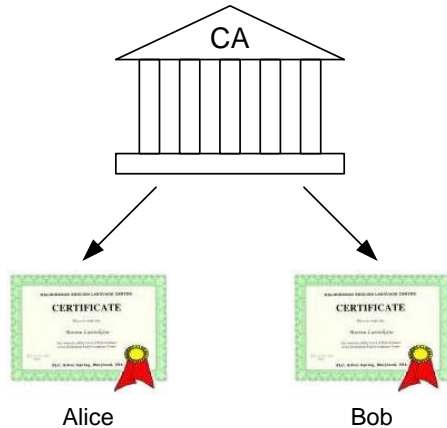
Welche Probleme ergeben sich bei fehlender Authentizität des öffentlichen Schlüssels ...

... im Signaturkontext?

... im Verschlüsselungskontext?

## Lösung

Schaffung einer vertrauenswürdigen Institution, die öffentliche Schlüssel beglaubigt und publiziert



Vertrauenswürdige Institution  
=  
Zertifizierungsstelle  
=  
Certificate Authority (CA)

## Lösung

- Durch die Beglaubigung wird der öffentliche Schlüssel zweifelsfrei einer Person zugeordnet
- Durch die Publikation wird er allen möglichen Kommunikationspartnern zugänglich gemacht
- Die digitale Beglaubigung eines öffentlichen Schlüssels wird als «Zertifikat» bezeichnet

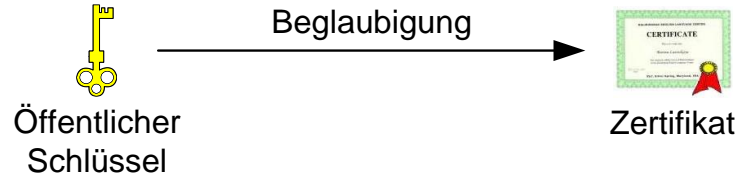


- Hinweis: Zertifikate können nicht nur für Personen ausgestellt werden, sondern auch für Computer

## Nochmals: Anforderung an öffentliche Schlüssel

Öffentliche Schlüssel müssen beglaubigt, d.h. eindeutig einer Person (einem Computer) zugeordnet werden können

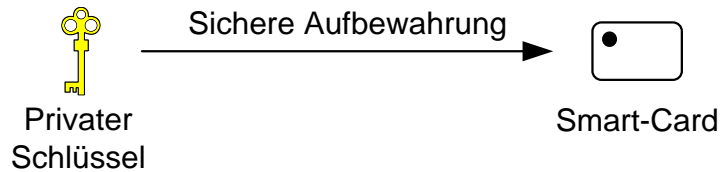
→ Schlüssel in ein Zertifikat «verpacken»



## Nochmals: Anforderung an private Schlüssel

Private Schlüssel müssen sicher (d.h. nur für den Besitzer zugänglich) aufbewahrt werden

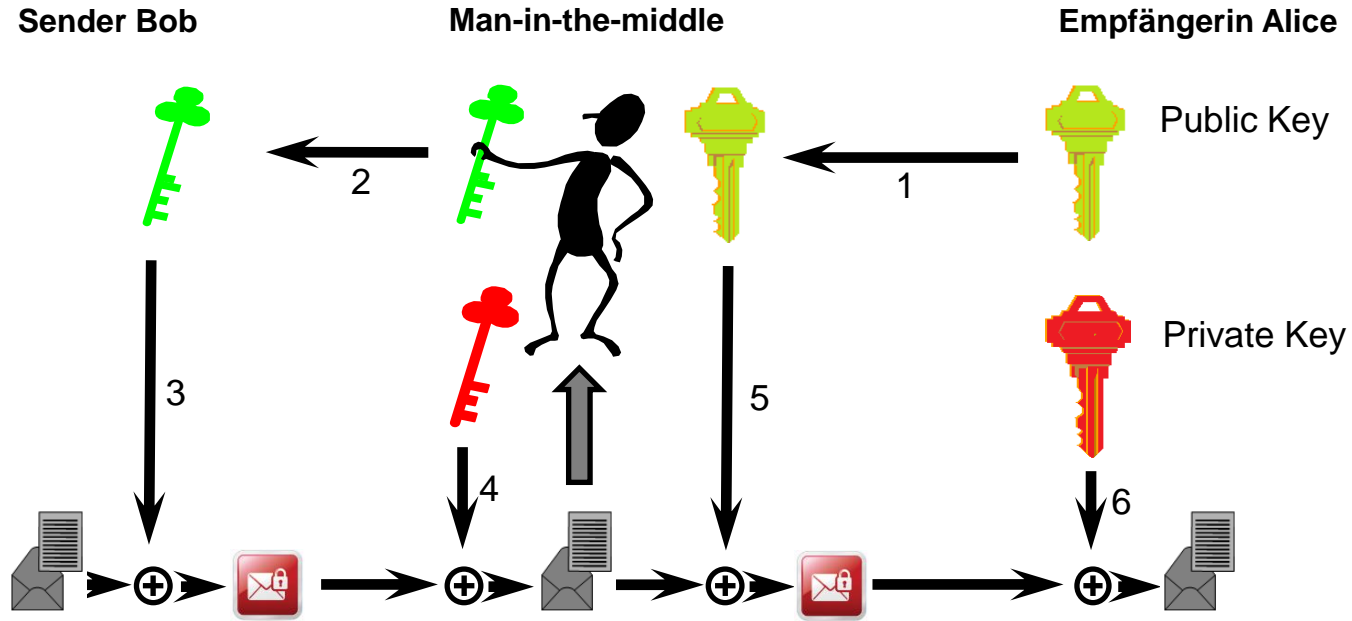
→ Schlüssel auf Smart-Card ablegen<sup>1</sup>



<sup>1</sup> Neben den Smart-Cards gibt es auch andere sichere Ablagemedien.



## Wenn die Authentizität des öffentlichen Schlüssels beim Verschlüsseln fehlt...

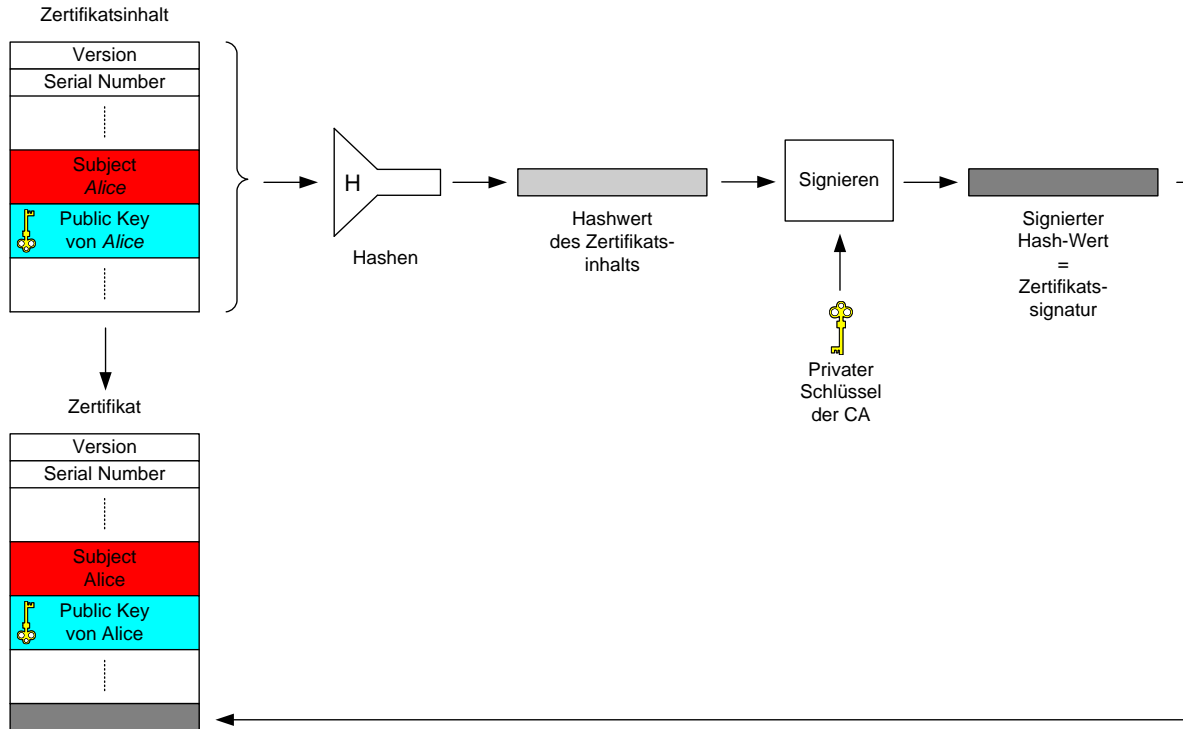


# **Zertifikate und ihr Lebenszyklus**

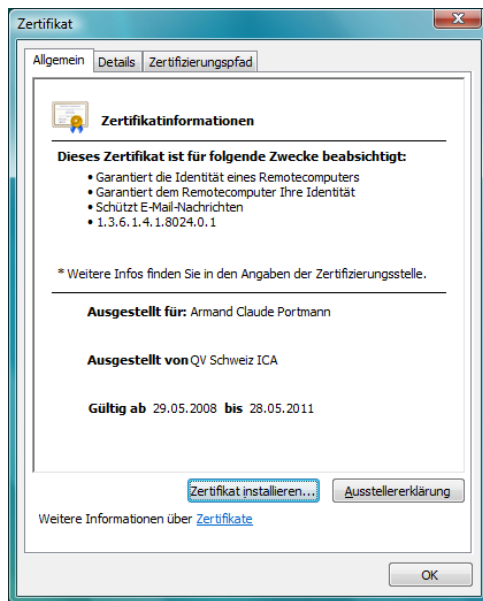
## Herstellen eines Zertifikats

- Antragssteller identifiziert sich bei der CA mithilfe eines Identitätsdokuments (z.B. Pass od. ID)
- Aus Namen des Antragsstellers, dessen öffentlichem Schlüssel und weiteren Informationen wird ein Datensatz gebildet (Zertifikatsinhalt)
- Dieser Datensatz wird mithilfe des privaten Schlüssels der CA signiert (=digitale Beglaubigung)  
→ Zertifikat
- CA veröffentlicht das Zertifikat

# Herstellen eines Zertifikats



## Beispiel-Zertifikat



Version	V3
Seriennummer	29 7e
Signaturalgorithmus	sha1RSA
Aussteller	QV Schweiz ICA, Issuing Certif...
Gültig ab	Donnerstag, 29. Mai 2008 07:...
Gültig bis	Samstag, 28. Mai 2011 07:00:00
Antragsteller	armand.portmann@...
Öffentlicher Schlüssel	RSA (2048 Bits)
Zugriff auf Stelleninformatio...	[1]Stelleninformationszugriff: ...
Zertifikatrichtlinien	[1]Zertifikatrichtlinie:Richtlinie...
Alternativer Antragstellerna...	RFC822-Name=armand.portm...
Erweiterte Schlüsselverwen...	Serverauthentifizierung (1.3.6...
Stellenschlüsselkennung	Schlüssel-ID=3a 52 64 0b da e...
Sperrlisten-Verteilungspunkte	[1]Sperrlisten-Verteilungspunk...
Schlüsselkennung des Antra...	2d 94 05 3f 90 49 00 cd 50 11 ...
Basiseinschränkungen	Typ des Antragstellers=Endei...
Schlüsselverwendung	Digitale Signatur, Zugelassen, ...
Fingerabdruckalgorithmus	sha1
Fingerabdruck	62 5f c3 96 b8 53 da 09 6d d1 ...

E = armand.portmann@...  
CN = Armand Claude Portmann  
OU = Standard Personal Certificate  
L = Luzern  
S = LU  
C = CH

0a 02 82 01 01 00 a7 e9  
f1 83 51 c5 16 46 30 c9  
57 72 71 29 d3 99 8d f9  
6c 9b 2d c2 ff 0c 25 e5  
8e 32 02 d5 ff 43 d9 77  
7c bd 2f 58 7b 23 4a d2  
..  
..  
..

Wozu dient der Fingerabdruck des Zertifikats? Wie wird er erstellt?

## **Zertifikatsklassen**

- Zur Beurteilung der Vertrauenswürdigkeit von Zertifikaten wird in der Regel ein Klassifizierungssystem verwendet
- Dieses System macht u.a. Vorgaben für folgende Faktoren
  - Registrierungsprozess inkl. Art des geforderten Identitätsnachweises des Antragsstellers
  - Im Zertifikat verwendeter Name des Antragsstellers
  - Zu verwendender Token (Hard-/Soft-Token)
  - Erlaubte Zertifikatsinhaber (z.B. natürliche Personen)
  - Anforderungen an die CA (Betrieb, Personal, Prozesse)

## **Zertifikatsklassen**

### **Class 1 Certificates (wenig Sicherheit)**

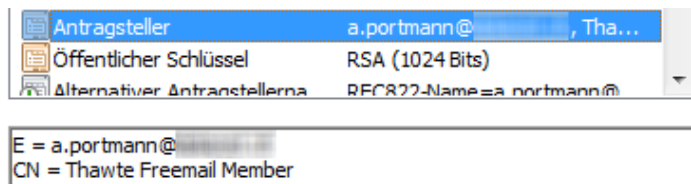
- Keine Überprüfung der Identität des Antragsstellers
- Es wird lediglich sichergestellt, dass der im Zertifikat eingetragene Name einmalig ist
- Die Zertifikate werden oft vollständig über das Internet beantragt und sind gratis
- Bsp. Freemail-Certificates
  - «Identitätsprüfung»: Antragsteller muss unter der im Zertifikat angegebenen E-Mail-Adresse erreichbar sein (Prüfung: Zustellung eines sog. E-Mail Ping)
  - Name des Antragsstellers ist nicht bei jeder CA im Zertifikat enthalten, evtl. gibt es den Hinweis «Persona not validated»

## Zertifikatsklassen

### Class 1 Certificates (wenig Sicherheit)

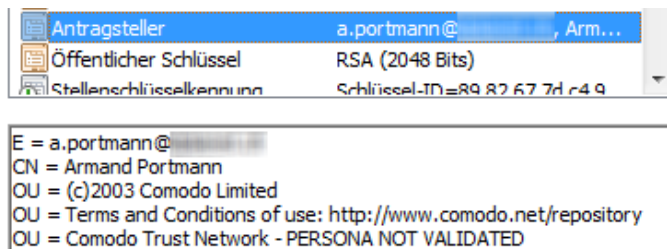
- Bsp. Freemail-Certificates

#### Thawte CA



Hinweis: Thawte hat inzwischen die  
Herausgabe von Freemail-Certificates  
eingestellt.

#### Comodo CA





## Zertifikatsklassen

### Class 1 Certificates (wenig Sicherheit)

- Bsp. Free TLS-Certificates
  - CA prüft initial und regelmässig wiederkehrend, ob der Antragsteller berechtigt ist, den gewünschten Domain-Namen zu benutzen, z.B. mithilfe eines E-Mail Pings an den Mail-Account des Administrators der Domain
  - Auf diese Weise ausgestellte Zertifikate werden als **Domain-Validated-Certificates** bezeichnet (DV-TLS-Certificates)
  - Aktuell bekanntester Herausgeber von Free TLS-Zertifikaten



<https://letsencrypt.org/>, online 19.04.24

# Getting Started

## 1) Automatic Certificate Management Environment

To enable HTTPS on your website, you need to get a certificate (a type of file) from a Certificate Authority (CA). Let's Encrypt is a CA. In order to get a certificate for your website's domain from Let's Encrypt, you have to demonstrate control over the domain. With Let's Encrypt, you do this using software that uses the [ACME protocol](#), which typically runs on your web host.

(...)

### Domain Validation

To kick off the process, the agent asks the Let's Encrypt CA what it needs to do in order to prove that it controls `example.com`. The Let's Encrypt CA will look at the domain name being requested and issue one or more sets of challenges. These are different ways that the agent can prove control of the domain. For example, the CA might give the agent a choice of either:

- Provisioning a DNS record under `example.com`, or
- • Provisioning an HTTP resource under a well-known URI on `https://example.com/`

Along with the challenges, the Let's Encrypt CA also provides a nonce that the agent must sign with its private key pair to prove that it controls the key pair.



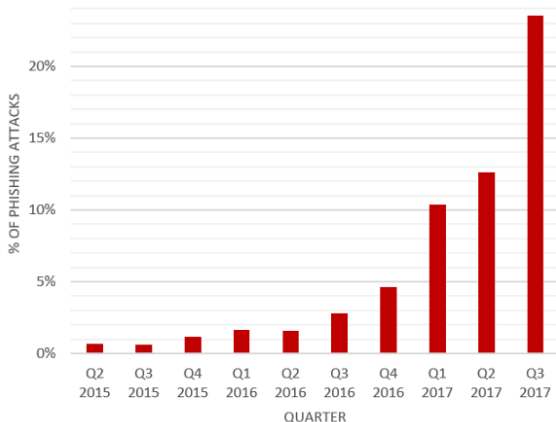
If the signature over the nonce is valid, and the challenges check out, then the agent identified by the public key is authorized to do certificate management for `example.com`. We call the key pair the agent used an "authorized key pair" for `example.com`.

<https://letsencrypt.org/how-it-works/>,  
online 13.02.19

## Ganz und gar nicht sicher: Immer mehr Phishing-Webseiten setzen auf HTTPS

Sicherheitsforschern zufolge nutzen 2017 ein Viertel aller Phishing-Webseiten HTTPS, um Opfer effektiver zu ködern.

Verglichen mit 2016 setzen dieses Jahr acht Mal mehr Phishing-Webseiten die Transportverschlüsselung HTTPS ein, [berichten Sicherheitsforscher](https://www.heise.de/security/meldung/Ganz-und-gar-nicht-sicher-Immer-mehr-Phishing-Webseiten-setzen-auf-HTTPS-3911127.html) von Phishlabs. Damit wollen Betrüger Vertrauen wecken, um so noch mehr Opfer erfolgreich abzuzocken.



(...)

### Gründe für den Anstieg

(...)

Dabei spielt natürlich auch die allgemein gesteigerte Verfügbarkeit von HTTPS-Webseiten eine Rolle.

(...)

Doch das Wachstum von Phishing-Seiten mit HTTPS steigt im Vergleich merklich rasanter: Mittlerweile setzen rund 25 Prozent der betrügerischen Seiten auf Transportverschlüsselung als Köder. Vor einem Jahr waren das Phishlabs zufolge nur rund drei Prozent.

<https://www.heise.de/security/meldung/Ganz-und-gar-nicht-sicher-Immer-mehr-Phishing-Webseiten-setzen-auf-HTTPS-3911127.html>,  
online 07.12.17

## **Zertifikatsklassen**

### **Class 2 Certificates (mittlere Sicherheit)**

- Überprüfung der Identität des Antragstellers mithilfe von Dokumenten und Datenbanken
- Bei Privatpersonen
  - Identitätsprüfung durch Zustellung einer Kopie von Pass oder ID
- Bei Firmen
  - Antragstellende Firma muss auf rechtliche und operationelle Existenz hin überprüft werden
  - Zeichnungsberechtigte Person (Revisionsstelle, Rechtsabteilung, VR-Mitglied) muss die Korrektheit des Inhalts des Zertifikatsantrags per Unterschrift bestätigen, ihre Zeichnungsberechtigung nachweisen (Kopie von Handelsregister) und ihre Identität belegen (Kopie von Pass oder ID)

## Zertifikatsklassen

### Class 2 Certificates (mittlere Sicherheit)

- Bei TLS-Zertifikaten prüft die CA, ob der Antragsteller berechtigt ist, den gewünschten Domain-Namen zu benutzen
- Auf diese Weise ausgestellte TLS-Zertifikate werden als ***Organization-Validated-Certificates*** bezeichnet (OV-TLS-Certificates)

## Zertifikatsklassen

### Class 3 Certificates (hohe Sicherheit)

- Prüfungen analog Klasse 2
- Zusätzlich *strenge* Identitätsprüfung (4 Möglichkeiten)
  - Persönliches Vorsprechen und Vorweisen eines Identitätsdokuments (Pass oder ID)
  - Zustellung eines *beglaubigten* Antragsdokuments (Notar beglaubigt die Korrektheit der auf dem Antragsformular eingetragenen Identitätsinformationen)
  - Video-Identifikation
  - Auslesen des RFID-Chips eines biometrischen Identitätsdokuments (Mobiltelefon mit RFID-Schnittstelle notwendig)



## **Zertifikatsklassen**

### **Qualified Certificates (höchste Sicherheit)**

- Signatur-Zertifikate der höchsten Gütestufe (für Gleichstellung mit handschriftlicher Unterschrift)
- Strenge Identitätsprüfung analog Klasse 3
- Zusätzlich steht die CA unter staatlicher Kontrolle (muss den sog. Anerkennungsprozess durchlaufen und jährliche Rezertifizierungsaudits durchführen)
- Qualifizierte Zertifikate werden nur für natürliche Personen ausgestellt

## **Zertifikatsklassen**

### **Extended Validation Certificates (höchste Sicherheit)**

- TLS-Zertifikate der höchsten Gütestufe (früher mit grüner Adresszeile im IE)
- Strenge Identitätsprüfung analog Klasse 3
- Weitere Prüfungen wie bei Klasse 2 OV-Zertifikaten
- Zusätzlich steht die CA unter Kontrolle (muss jährliche Audits durchführen)



## Beispiel: SwissSign TLS Zertifikate

### Managed PKI DV Domain-Validation

Die MPKI DV beinhaltet einfache und kostengünstige SSL- und E-Mail-Zertifikate, die als domain-validiert ausgewiesen werden.

Sie eignet sich für Webseiten mit einem einfachen Schutzbedürfnis.

**Use Cases:** einfache Webseiten, Blogs, Mailserver

### Managed PKI OV Organisation-Validation

Die MPKI OV beinhaltet neben den Produkten aus der MPKI DV zusätzlich SSL- und E-Mail-Zertifikate, bei denen die Organisation überprüft wurde.

Sie eignet sich für Unternehmen und Organisationen, die ihren Kunden einen hohen Schutz bieten möchten.

**Use Cases:** kleinere Webshops, Unternehmenswebseiten

### Managed PKI EV Extended Validation

Die MPKI EV beinhaltet neben den Produkten aus MPKI DV und OV zusätzlich SSL- und E-Mail-Zertifikate, bei denen auch der rechtliche Status und die Adresse des Unternehmens mittels staatlicher Register überprüft wurde.

Sie eignet sich für Unternehmen, die ihre Marke mit Sicherheit verbinden und die höchste Vertrauensstufe ausweisen möchten.

**Use Cases:** Online-Banken, grosse Webshops



#### MPKI DV

DV SSL Silver Single-Domain



DV SSL Silver Multi-Domain



OV SSL Gold Single-Domain



EV SSL Gold Single-Domain



DV SSL Silver Wildcard



OV SSL Gold Wildcard



OV SSL Gold Multi-Domain



EV SSL Gold Multi-Domain



E-Mail ID Silver (Mailbox Validated)



E-Mail ID Gold (Sponsor Validated)



**Bearbeitungsdauer \***

1 Arbeitstag

**Mindestumsatz pro Jahr**

0 CHF



#### MPKI OV



ca. 1 Woche

300 CHF



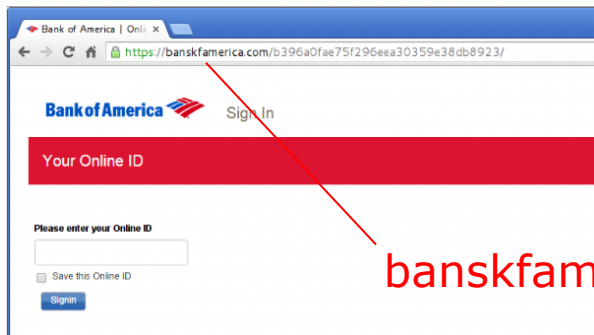
#### MPKI EV



ca. 1 Woche

500 CHF

## SSL-Zertifizierungsstellen stellen hunderte Zertifikate für Phishing-Seiten aus



**Online-Betrüger missbrauchen SSL-Zertifizierungsstellen, um sich Zertifikate für Phishing-Seiten ausstellen zu lassen, warnen Sicherheitsforscher. Schuld daran seien laxen Richtlinien der Zertifizierer.**

**banksfamerica.com (kein Schreibfehler)**

In einem Beobachtungszeitraum von einem Monat haben sich Online-Betrüger hunderte Zertifikate für Phishing-Seiten von SSL-Zertifikatsstellen wie etwa Comodo und Symantec ausstellen lassen. Phishing-Seiten wie zum Beispiel banksfamerica.com oder itunes-security.net sollen mit den Zertifikaten vertrauenswürdiger wirken. Davor warnen die Sicherheitsforscher von Netcraft. Schuld daran seien laxen Richtlinien der SSL-Zertifikatsstellen. **In vielen Fällen müssen Betrüger nur nachweisen, dass sie die Kontrolle über eine Domain haben. Postwendend erhalten sie innerhalb weniger Minuten ein Zertifikat, erläutern die Sicherheitsforscher. (...)**

Mit 41 Prozent stellte Cloudflare die meisten SSL-Zertifikate für Phishing-Seiten im August 2015 aus, berichten die Sicherheitsforscher. Dabei setzt der Internet-Dienstleister auf eine Partnerschaft mit Comodo und Globalsign. (...)

<http://www.heise.de/security/meldung/SSL-Zertifizierungsstellen-stellen-hunderte-Zertifikate-fuer-Phishing-Seiten-aus-2848793.html>, online 15.10.15

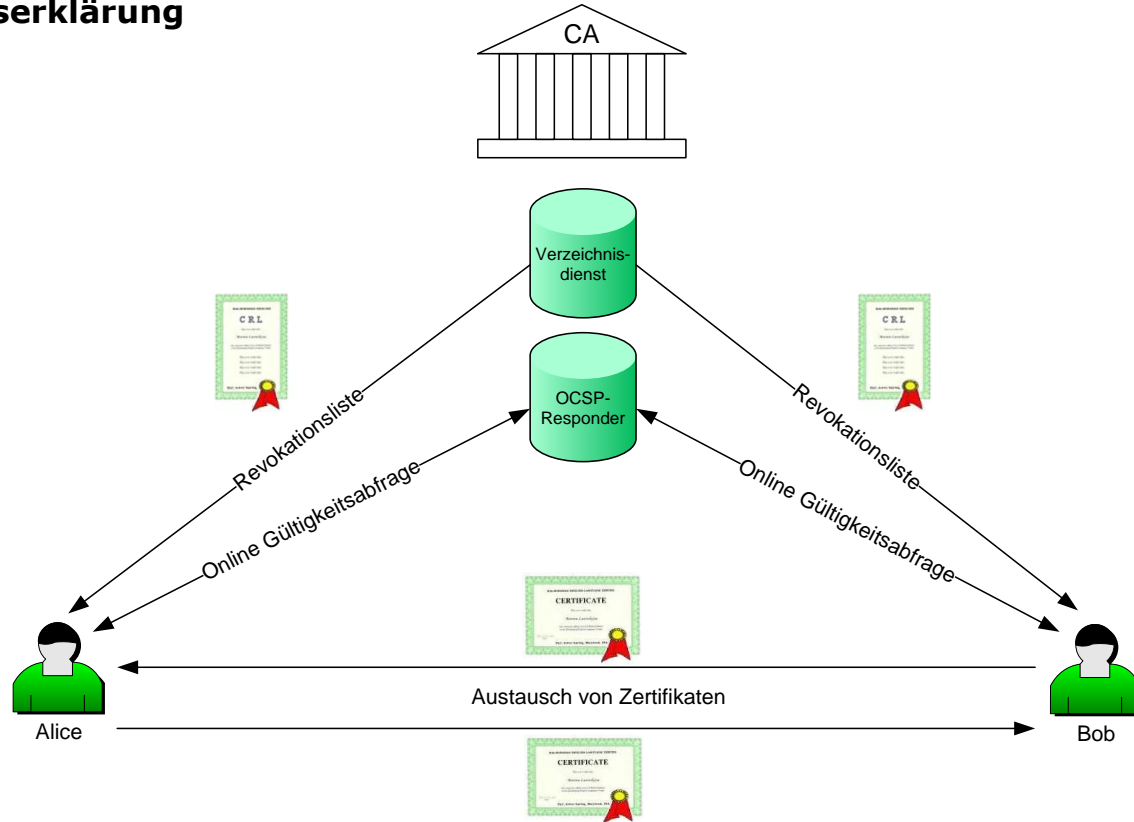
## **Ungültigkeitserklärung**

- Zertifikate können vor Ablauf des Gültigkeitsdatums für ungültig erklärt werden
- Dieser Vorgang wird als Revokation bezeichnet
- Die Identifikation der Zertifikate erfolgt über deren Seriennummer
- Gründe für die Revokation eines Zertifikats
  - Zugehöriger privater Schlüssel wurde gebrochen
  - Zertifikatsbesitzer verlässt das Unternehmen
  - Personendaten des Zertifikatsbesitzers haben geändert, sodass ein neues Zertifikat ausgestellt werden muss

## **Ungültigkeitserklärung**

- Die Liste der für ungültig erklärten Zertifikate wird Revokationsliste genannt (engl. Certificate Revocation List, CRL; dt. Zertifikatssperrliste)
- Jede CA muss eine Revokationsliste authentisch führen und publizieren
- Alternativ zur Überprüfung via Revokationsliste ist auch eine Online-Prüfung via Online Certificate Status Protocol (OCSP) möglich

# Ungültigkeitserklärung



# Digitale Zertifikate: Online-Sperrung wird optional, Sperrlisten zur Pflicht

Das Echtzeit-Protokoll OCSP hatte mit Zuverlässigkeitsproblemen und Datenschutzbedenken zu kämpfen. Ab heute müssen CAs ihre Sperrlisten besser pflegen.



(Bild: Michal Jarmoluk, gemeinfrei)

15.03.2024, 13:12 Uhr | Lesezeit: 3 Min. | Security

Von Dr. Christopher Kunz

Die großen Browserhersteller und Zertifikats-Aussteller ziehen einen vorläufigen Schlusstrich unter ihre Unterstützung für Online Certificate Status Protocol (OCSP) und setzen künftig wieder voll auf regelmäßig, aber nicht in Echtzeit aktualisierte Sperrlisten (Certificate Revocation List, CRL). Diese, so die Selbstverpflichtung der im "CA/Browser Forum" organisierten Stellen, werden künftig schneller auf den neuesten Stand gebracht.

<https://www.heise.de/news/Digitale-Zertifikate-Online-Sperrung-wird-optional-Sperrlisten-zur-Pflicht-9655904.html> , online 15.03.24

Siehe auch:

<https://www.heise.de/news/HTTPS-Zertifikate-Die-Rueckkehr-der-Sperrlisten-7257554.html>, online 08.09.22

## **Fragen zur Ungültigkeitserklärung**

- Warum muss der Antrag für die Revokation eines Zertifikats ebenso sorgfältig geprüft werden, wie der Antrag für ein neues Zertifikat?
- Wie könnte eine Identitätsprüfung des Antragsstellers der Revokation durchgeführt werden?
- Warum muss die Aktualisierung der Revokationsliste möglichst schnell erfolgen?
- Welche Anforderung an die Gültigkeitsdauer der Revokationsliste ergibt sich daraus?

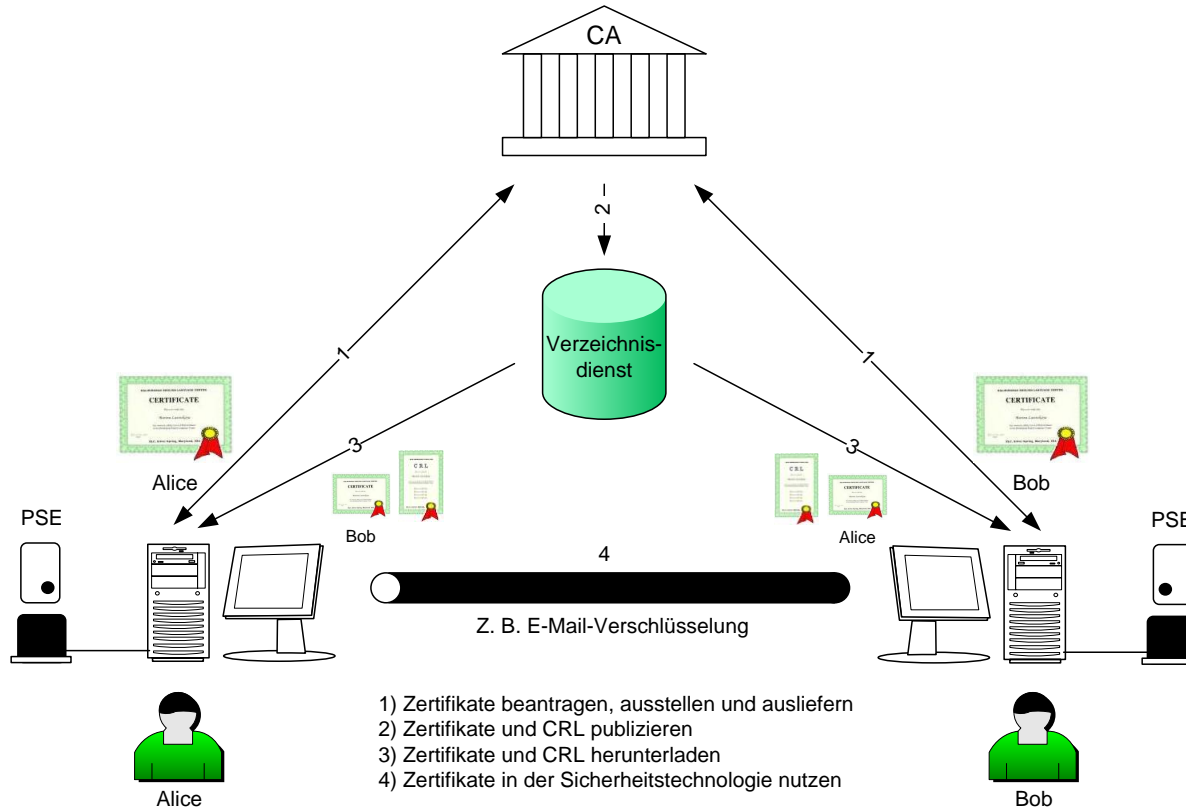
# **Bausteine einer Public Key Infrastruktur**



## **Überblick Grundbausteine**

- Certification Authority (CA)
- Personal Security Environment (PSE)
- Directory Service (Verzeichnisdienst)
- Sicherheitsapplikation

## Wechselwirkung, Abhängigkeiten



## Personal Security Environment

- Ablagemedium für Geheimelemente (private Schlüssel)
- Ausprägungen (Versuch einer Klassifizierung)
  - Passwort-geschützte Datei  
→ **Soft-Token**
  - Plastikkarte mit Speicherchip mit Krypto-Prozessor  
→ **Chip-Karte, Hard-Token, besser Smart-Card, Crypto-Card oder Krypto-Token**
  - USB-Stecker mit Speicherchip mit Krypto-Prozessor  
→ **Hard-Token, besser USB-Token oder Krypto-Token**
  - Erweiterungskarte für Computer-Mainboards mit Krypto-Prozessor  
→ **Hardware Security Module (HSM)**

## **Personal Security Environment mit oder ohne Krypto-Prozessor?**

- Nachteil aller PSEs ohne Krypto-Prozessor: Sicherheitsapplikation muss kryptographische Operationen ausführen (anstatt PSE)
- Für die Ausführung dieser Operationen (z.B. Signaturerstellung) muss das Geheimelement in der Sicherheitsapplikation im Klartext vorliegen
- Sicherheitsapplikation läuft aber oftmals im unsicheren PC-Betriebssystem-Umfeld
- Geheimelement kann dort durch Malware ausspioniert werden

## **Personal Security Environment mit oder ohne Krypto-Prozessor?**

- Lösung dieses Problems: PSEs mit Krypto-Prozessor verwenden
- Alle kryptographischen Operationen werden auf dem PSE vom Krypto-Prozessor ausgeführt (evtl. sogar die initiale Berechnung des Schlüsselpaars)
- Geheimelement verlässt deshalb das PSE nie
- Wenn auch das Schlüsselpaar auf dem PSE berechnet wurde, ist der private Schlüssel nur genau einmal vorhanden

## **Diskussion PSE mit Krypto-Prozessor**

- Wie läuft die Signatur einer Datei unter Verwendung eines PSEs mit Krypto-Prozessor ab?
- Wie die Entschlüsselung einer Datei?
- Warum ist die Schlüsselerzeugung auf dem PSE sicherheitstechnisch die beste Lösung?
- Welchen Nachteil erkaufte man sich mit dieser Lösung?
- Davon abgeleitet: Schlüsselpaare für welche Anwendung (Signatur, Verschlüsselung) können ohne weiteres auf einem PSE berechnet werden? Warum?

## Crypto-Card, HSM, USB-Token und RFID-Karte



Crypto-Card



HSM



USB-Token



RFID-Karte

## **Directory Service**

- Ist Ablageort der ausgestellten Zertifikate und der ausgestellten CRL
- Wird von der Sicherheitsapplikation angesprochen
- Kommuniziert zum Zwecke des Datenabgleichs evtl. mit anderen Verzeichnisdiensten
- Lagert nicht nur Zertifikate und CRLs, sondern auch andere Personendaten. Bsp. Globales Adressbuch von Microsoft Exchange



## **Sicherheitsapplikation**

Das Funktionieren einer Sicherheitsapplikation ist an die folgenden Bedingungen geknüpft:

- Direkter Zugriff auf den Private Key (bei Soft-Token) oder Kommunikation mit Krypto-Prozessor (bei Crypto-Card) ist möglich
- Zugriff auf das eigene Zertifikat, das Zertifikat des Kommunikationspartners und die CRL ist möglich
- Und deshalb: Zugriff auf den Verzeichnisdienst ist möglich (da Zertifikate und CRLs in der Regel dort abgelegt sind)

## Sicherheitsapplikation

Sicherheitsprotokolle, die in Sicherheitsapplikationen häufig implementiert sind:

- IPSEC (Layer 3)
- TLS (Layer 4)
- SSH
- FTPS
- S/MIME oder PGP (Sichere E-Mail)
- POP3S, IMAPS, SMTPS
- LDAPS
- EAP-TLS (Extensible Authentication Protocol)

# **Prüfen der Gültigkeit von Zertifikaten**

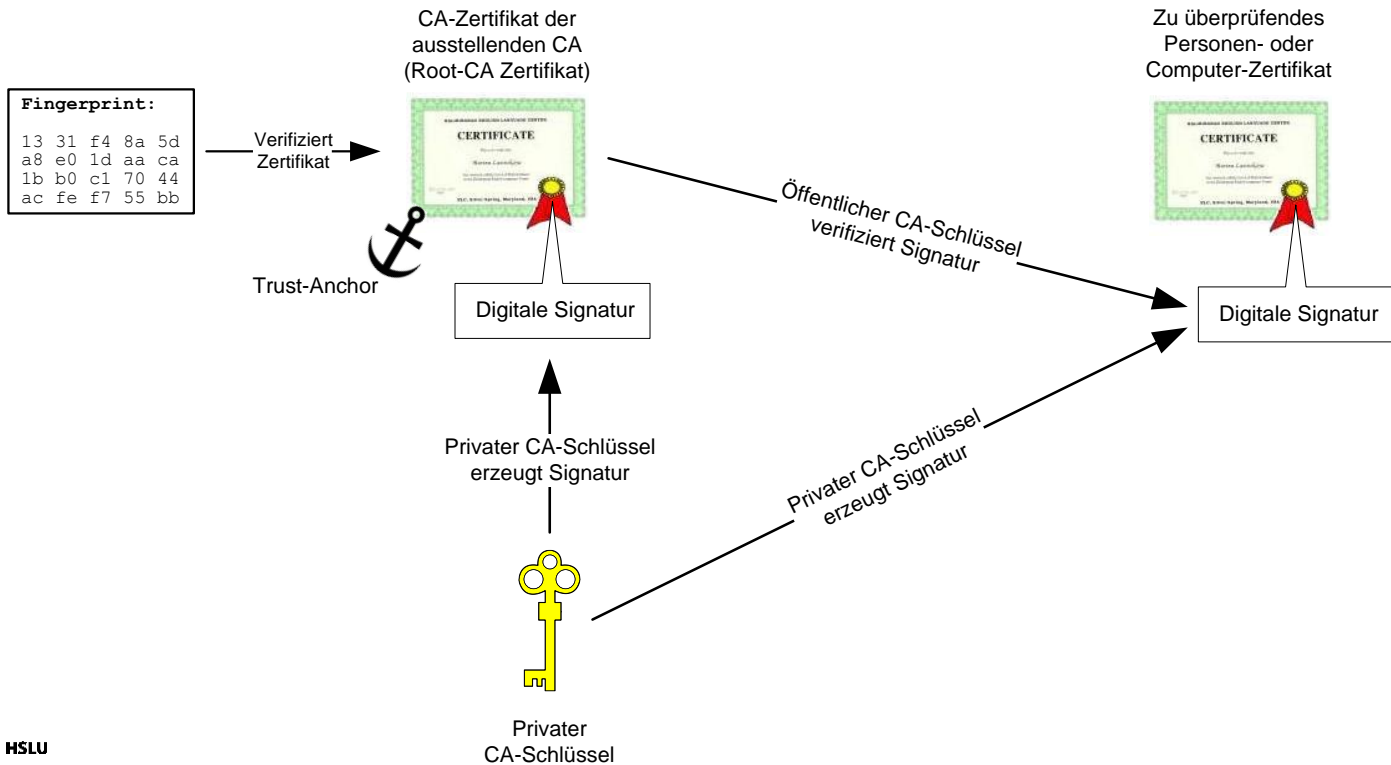
## Prüfkriterien

Die Prüfung der Gültigkeit eines Zertifikats beinhaltet die folgenden Kriterien:

- Gültigkeitsdauer: Aktuelles Datum liegt im Gültigkeitsbereich des Zertifikats
- Ungültigerklärung: Zertifikat wurde nicht revoziert, d.h. vor Ablauf für ungültig erklärt
- Zertifikatssignatur: Zertifikat wurde von der CA gültig signiert und gilt somit als echt

Frage: Welche weiteren Kriterien müssen gegebenenfalls bei der Verwendung von Zertifikaten überprüft werden? (Sie haben nichts mit der Zertifikatsgültigkeit selber zu tun.)

## Prüfung der Zertifikatsechtheit



## Prüfung der Zertifikatsechtheit

- CA-Zertifikate, die nicht von einer übergeordneten CA ausgestellt worden sind, werden als **Root-CA Zertifikate** bezeichnet
- Sie sind der Aufhänger der Sicherheit und werden deshalb oft auch als **Trust-Anchor** bezeichnet
- Root-CA Zertifikate können nicht über die Signatur überprüft werden, sondern nur mithilfe des Fingerprints (Warum?)
- Personen- oder Computer-Zertifikate lassen sich mithilfe des Zertifikats der ausstellenden CA überprüfen (Signaturverifikation) oder mithilfe des Fingerprints

## Prüfung der Zertifikatsechtheit

- Generell kann die Echtheit eines *jeden* Zertifikats durch einen Vergleich von dessen Fingerprint mit dem Fingerprint des Original-Zertifikats überprüft werden
- Wie muss eine korrekte Überprüfung des Fingerprints ablaufen?
- Was fällt Ihnen bei der Betrachtung des folgenden von Windows ausgegebenen Zertifikats*inhalts* auf?

Feld	Wert
Alternativer Ausstellername	Verzeichnisadresse:O=ZertES ...
Stellenschlüsselkennung	Schlüssel-ID=21 f0 05 b5 f8 a...
Sperrlisten-Verteilungspunkte	[1]Sperrlisten-Verteilungspunk...
Schlüsselkennung des Antra...	75 24 9d 6f 5c 5b ff 00 1a 1e ...
Schlüsselverwendung	Digitale Signatur, Zugelassen (...)
Fingerabdruckalgorithmus	sha1
Fingerabdruck	31 11 66 3d 5b f0 31 9a 81 cd ...

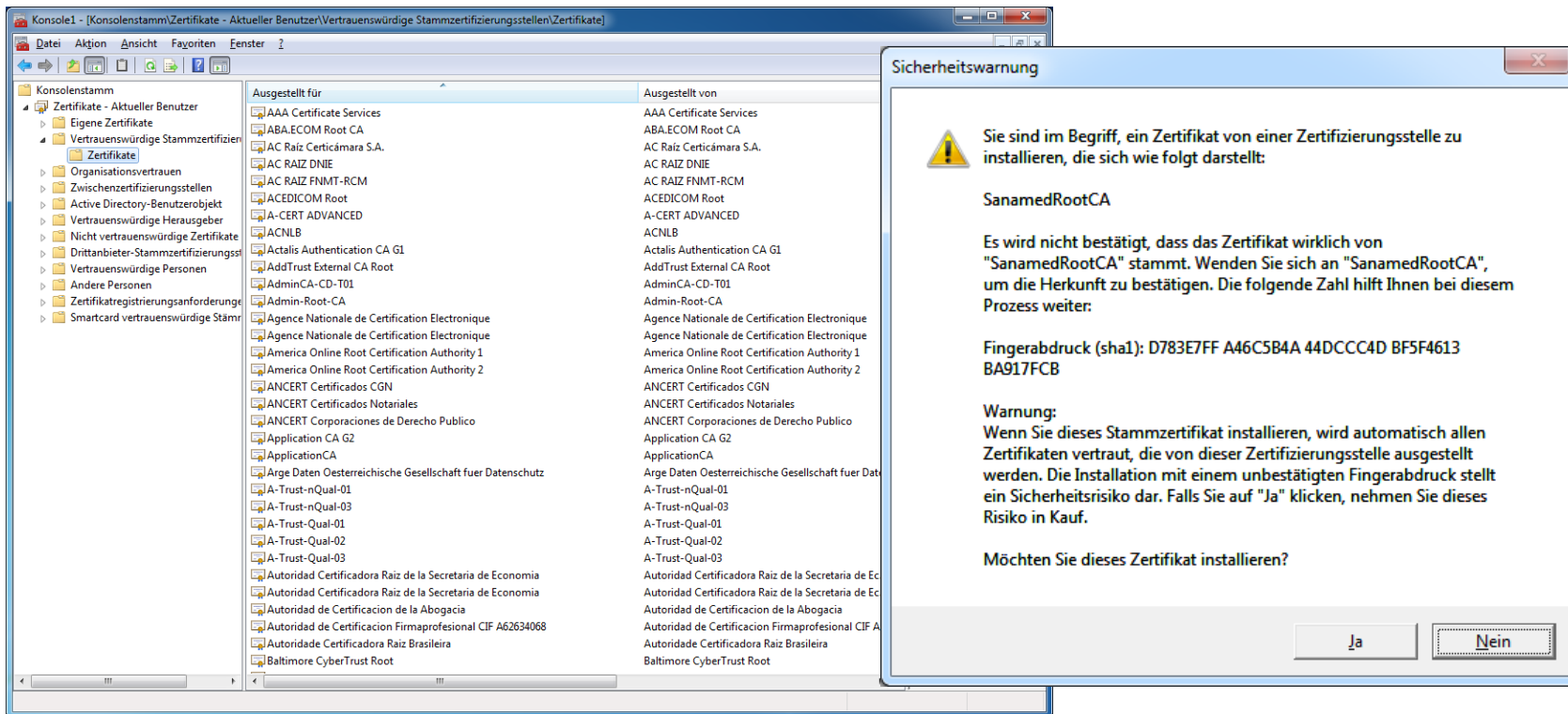
```
31 11 66 3d 5b f0 31 9a 81 cd 5b 58 6d 93 6f
01 2f f6 9a 9b
```

## Prüfung von Root-CA Zertifikaten

- Die automatische Prüfung von Personen- oder Computer-Zertifikaten über die Signatur setzt das Vorhandensein von echten (d.h. überprüften) Root-CA Zertifikaten voraus
- Betriebssystem- und Browser-Hersteller liefern mit ihren Produkten vorinstallierte Root-CA Zertifikate mit (Vertrauensfrage!)
- Nicht installierte Root-CA Zertifikate können manuell nachinstalliert werden (oder werden z.T. automatisch nachinstalliert)
- Durch die Installation wird dem Zertifikat Echtheit attestiert (heikler Vorgang! Warum?)



## Prüfung von Root-CA Zertifikaten – Beispiel Windows



# Webbrowser: Googles Chrome bekommt eigenen Root-CA-Speicher

Künftig will Internetriese selbst bestimmen, wessen Zertifikaten der hauseigene Browser vertraut und das nicht mehr Microsoft und Apple überlassen.

Lesezeit: 2 Min.  In Pocket speichern

   18



(Bild: monticello / Shutterstock.com)

23.09.2022 14:14 Uhr | Security

Von Jürgen Schmidt

Bislang verwendet Google Chrome für die Überprüfung von HTTPS-Zertifikaten das Betriebssystem als Vertrauensanker. Konkret lässt der Browser alle Zertifikate gelten, deren digitale Unterschrift sich auf eines der vom Betriebssystem installierten Root-CA-Zertifikate zurückführen lässt; also die von Microsoft installierten auf Windows, die von Apple auf macOS und so weiter. Jetzt will Google einen eigenen Root-CA-Store aufbauen, den Chrome dann standardmäßig verwendet.

Dieser Root-CA-Store soll dann die Wurzelzertifikate aller Zertifizierungsstellen enthalten, denen Chrome standardmäßig vertraut. Für die Aufnahme hat das Chrome-Team bereits eine Policy erstellt, die Bedingungen formuliert, denen die CAs genügen müssen. Mozilla betreibt bereits ein ähnliches Programm für den Root-CA-Store von Firefox. Denn anders als Chrome verwendet Firefox traditionell seine eigenen Zertifikate und nicht die des Betriebssystems.

<https://www.heise.de/news/Google-Chrome-bekommt-eigenen-Root-CA-Speicher-7273841.html>, online 23.09.22

## **Prüfung von Root-CA Zertifikaten – Beispiel DigiCert**

- Öffentliche Zertifizierungsstellen wie DigiCert publizieren die Fingerprints ihrer Root-CA Zertifikate im Web
- Selbstverständlich muss die Authentizität von Webseiten, die Fingerprints publizieren, absolut gewährleistet sein

## Prüfung von Root-CA Zertifikaten – Beispiel DigiCert

The screenshot shows a web browser window displaying the DigiCert website's root certificates page. A red arrow points from the 'Fingerabdruck' (Fingerprint) field in the Windows Certificate Manager window to the SHA-1 Thumbprint of the VeriSign Universal Root Certification Authority.

**VeriSign Class 3 Public PCA - Generation 5 (G5)**

Subject DN: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5  
Operational Start Date: Nov 8 00:00:00 2006 GMT  
Operational End Date: Jul 16 23:59:59 2036 GMT  
Key Size: 2048 bit  
Signature Algorithm: sha1WithRSAEncryption  
Serial Number: 18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a  
SHA-1 Thumbprint: 4E B6 D5 78 49 9B 1C CF 5F 58 1E AD 56 BE 3D 9B 67 44 A5 E5  
Hierarchy: Public TLS / SSL, CodeSigning, Client Auth/Email  
Root Download  
Link: <https://www.websecurity.digicert.com/content/dam/websecurity/digitalassets/desktop/pdfs/roots/VeriSign-Class%203-Public-Primary-Certification-Authority-G5.pem>

**VeriSign Universal Root Certification Authority**

Subject DN: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority  
Operational Start Date: Apr 2 00:00:00 2008 GMT  
Operational End Date: Dec 1 23:59:59 2037 GMT  
Key Size: 2048 bit  
Signature Algorithm: sha256WithRSAEncryption  
Serial Number: 40 1a c4 64 21 b3 13 21 03 0e bb e4 12 1a c5 1d  
SHA-1 Thumbprint: 36 79 CA 35 66 87 72 30 4D 30 A5 FB 87 3B 0F A7 7B B7 0D 54  
Hierarchy: Public TLS / SSL, CodeSigning, Client Auth/Email  
Root Download  
Link: <https://www.websecurity.digicert.com/content/dam/websecurity/digitalassets/desktop/pdfs/roots/VeriSign-Universal-Root-Certification-Authority.pem>

**Symantec Class 1 Public PCA - Generation 4 (G4)**

Subject DN: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 1 Public Primary Certification Authority - G4  
Operational Start Date: Oct 5 00:00:00 2011 GMT  
Operational End Date: Jan 18 23:59:59 2038 GMT  
Key Size: 384 bit  
Signature Algorithm: ecdsa-with-SHA384  
Serial Number: 21 6e 33 a5 cb d3 88 a4 6f 29 07 b4 27 3c c4 d8  
SHA-1 Thumbprint: 84 F2 E3 DD 83 13 3E A9 1D 19 52 7F 02 D7 29 BF C1 5F E6 67

**Zertifikat**

Allgemein Details Zertifizierungspfad

Anzeigen: <Alle>

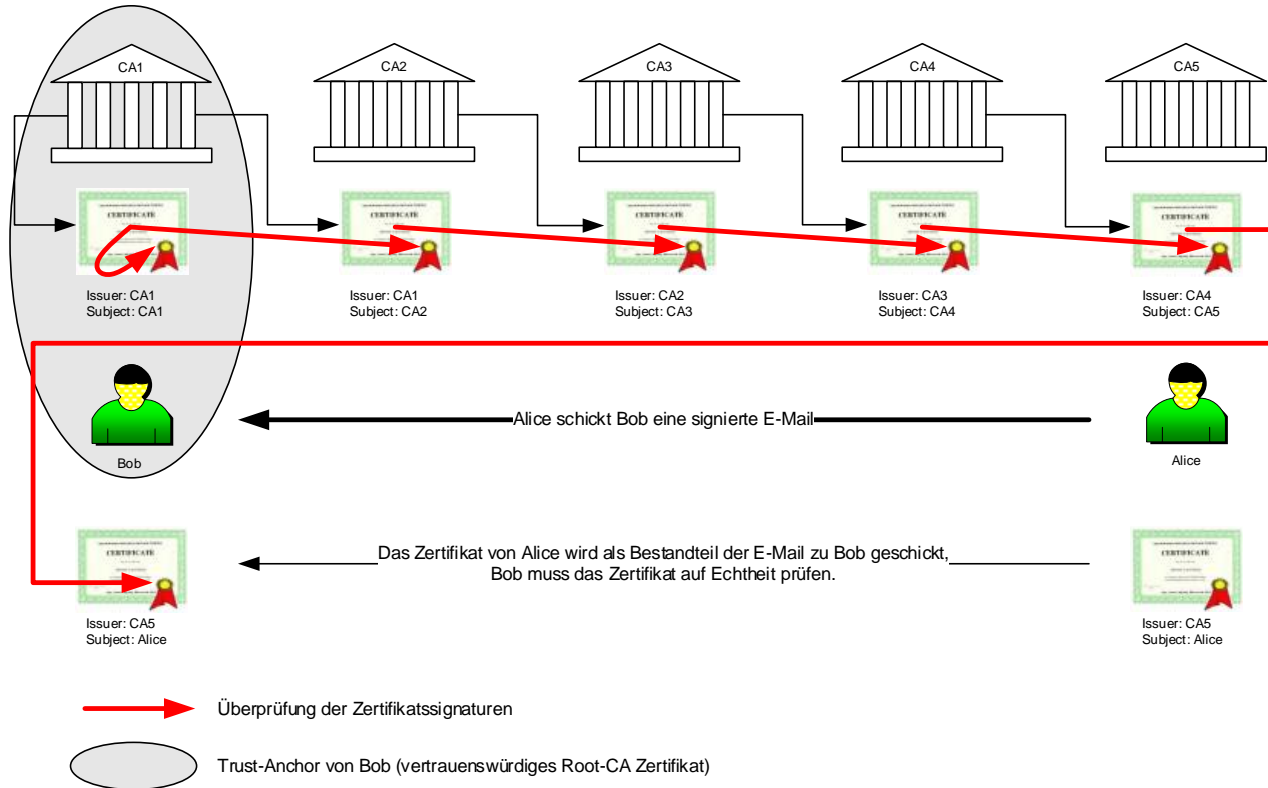
Feld	Wert
Schlüsselkennung des Antrags	7fd365a7c2ddcebf03009f34...
Basiseinschränkungen	Typ des Antragstellers=Zertifi...
Schlüsselverwendung	Zertifikatsignatur, Offline Signi...
Fingerabdruck	4eb6d578499b1ccf5f581ead5...
Anzeigename	VeriSign
Erweiterte Schlüsselverwen...	Clientauthentifizierung, Codesi...
Erweiterte Überprüfung	[1]Zertifikatrichtlinie:Richtlinie...

4eb6d578499b1ccf5f581ead56be3d9b6744a5e5

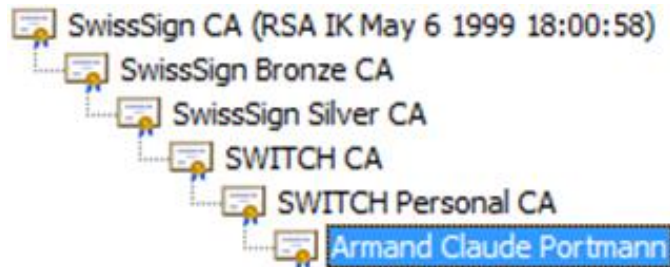
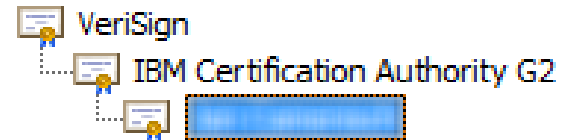
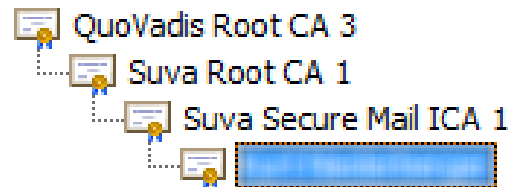
Eigenschaften bearbeiten... In Datei kopieren...

OK

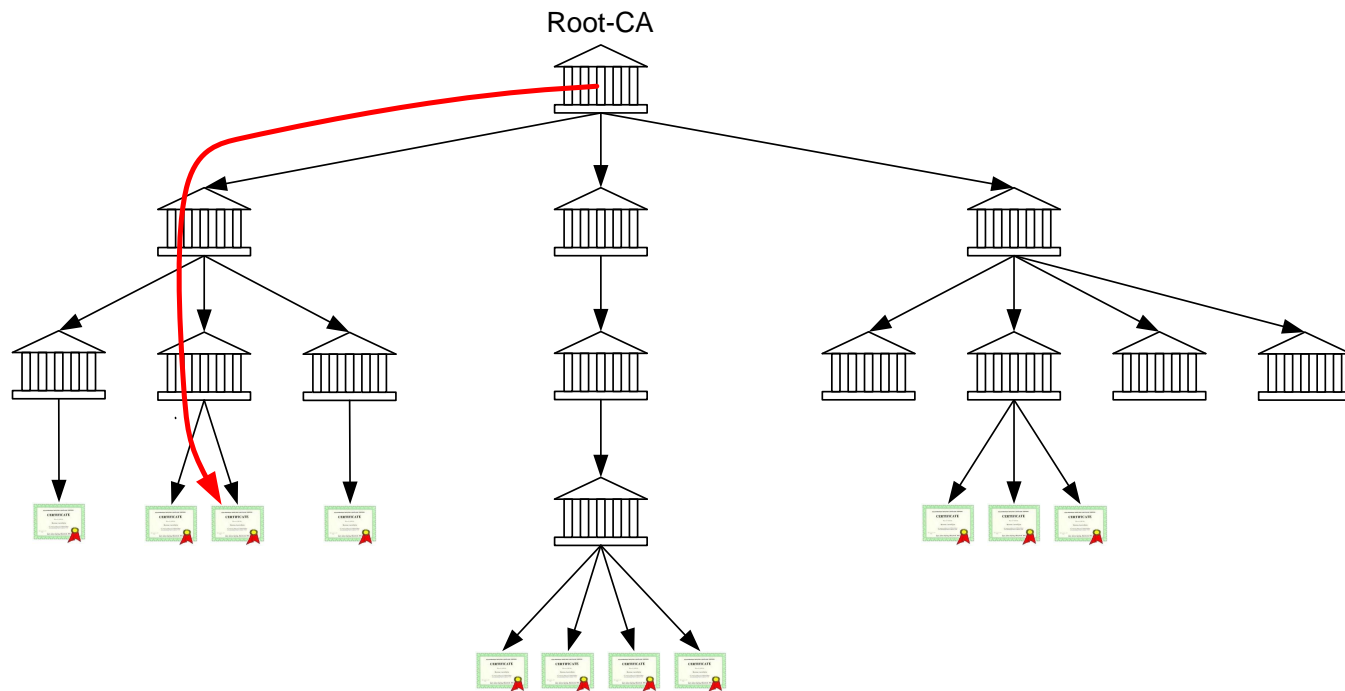
# Zertifikatskette



## Beispiele für Zertifikatsketten



## Hierarchische Vernetzung von CAs – Anwendung von Zertifikatsketten



## Quellenangaben

[1] An Introduction to Cryptography, PGP Corporation

<https://archive.org/details/pgp-70-intro-to-crypto>, online 31.10.23

[2] All-in Signing Service, Swisscom (White Paper)



Danke!

**Hochschule Luzern**  
**Informatik**  
Weiterbildung  
**Prof. Armand Portmann**  
Leiter Programm

T direkt +41 41 757 68 57  
armand.portmann@hslu.ch