PKI (public key infrastructure)

am Fritz-Haber-Institut

11. Mai 2015, Bilder: "Mehr Sicherheit durch PKI-Technologie", Network Training and Consulting

Verschlüsselung allgemein

- Bei einer Übertragung von sensiblen Daten über unsichere Netze müssen folgende Bedingungen erfüllt sein:

- **Vertraulichkeit**
  Die Daten dürfen nur vom Empfänger gelesen werden.

- **Integrität**
  Es ist sicher, dass die Daten während der Übertragung nicht verändert wurden.

- **Authentifizierung**
  Der Absender ist derjenige, der er vorgibt zu sein

- **Nicht-Abstreitbarkeit** (Non-Repudiation)
  Der Erhalt der Daten kann nicht geleugnet werden.

Verschlüsselung allgemein

- Um diese Bedingungen zu erfüllen, wird mittels Schemata verschlüsselt. Ein Verschlüsselungsschema besteht aus:

- **Schlüsseln**
  Beliebige Zeichenfolge mit bestimmter Länge (Keys)

- **Verschlüsselungsart**
  Algorithmus

- **Schlüsselverwaltung**
  Key Management Protocol

- **Digitale Unterschriften**
  Elektronische Signatur

Grundlegende Verschlüsselungsarten

- **Symmetrische Verschlüsselung**
- **Asymmetrische Verschlüsselung**
- **Einweg-Verschlüsselungsfunktion (Hash)**

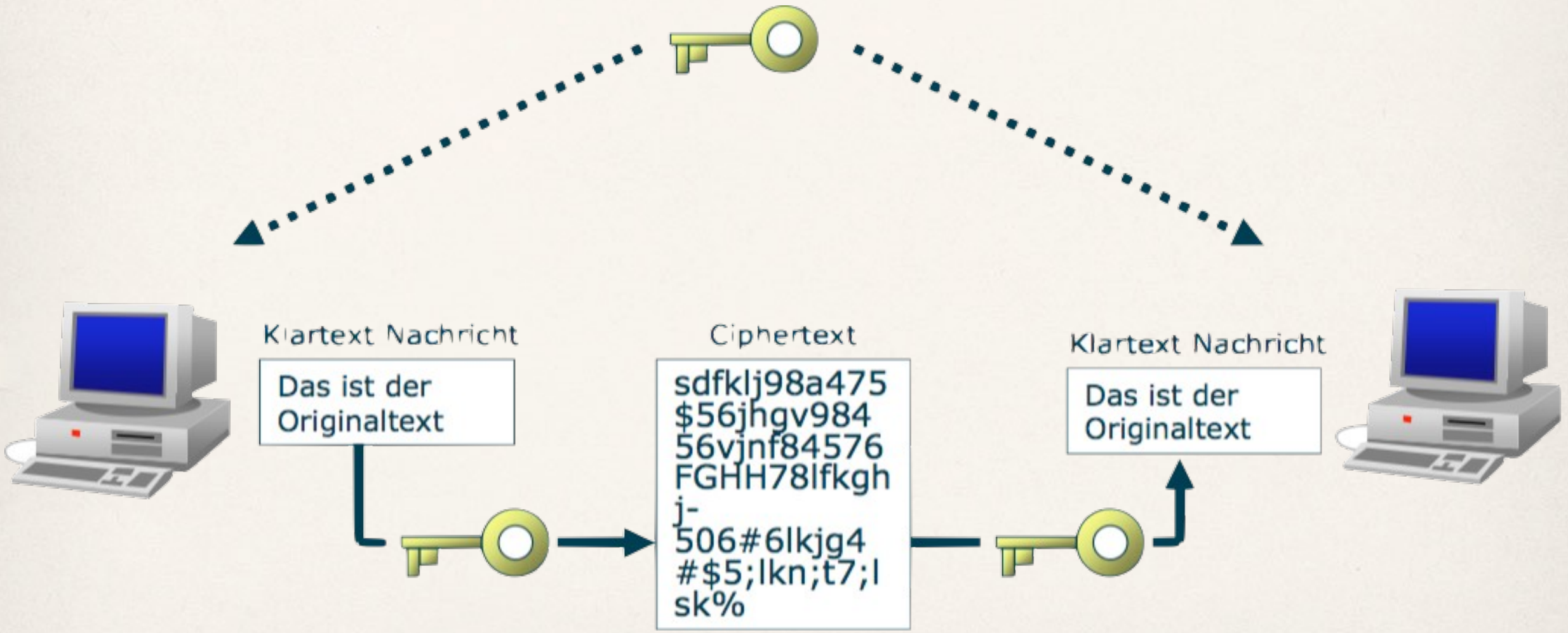
Grundlegende Verschlüsselungsarten

- **Symmetrische Verschlüsselung**
  Ein geheimer Schlüssel (*shared secret key*) wird für die Ver- und Entschlüsselung verwendet.

- Vorteil:
  - sehr schnelle Verschlüsselung
  - dadurch wird **Vertraulichkeit** gewährleistet
- Nachteil:
  - Die Schlüssel müssen unbedingt sicher und geheim aufbewahrt und regelmäßig geändert werden.

Grundlegende Verschlüsselungsarten

- **Symmetrische Verschlüsselung**

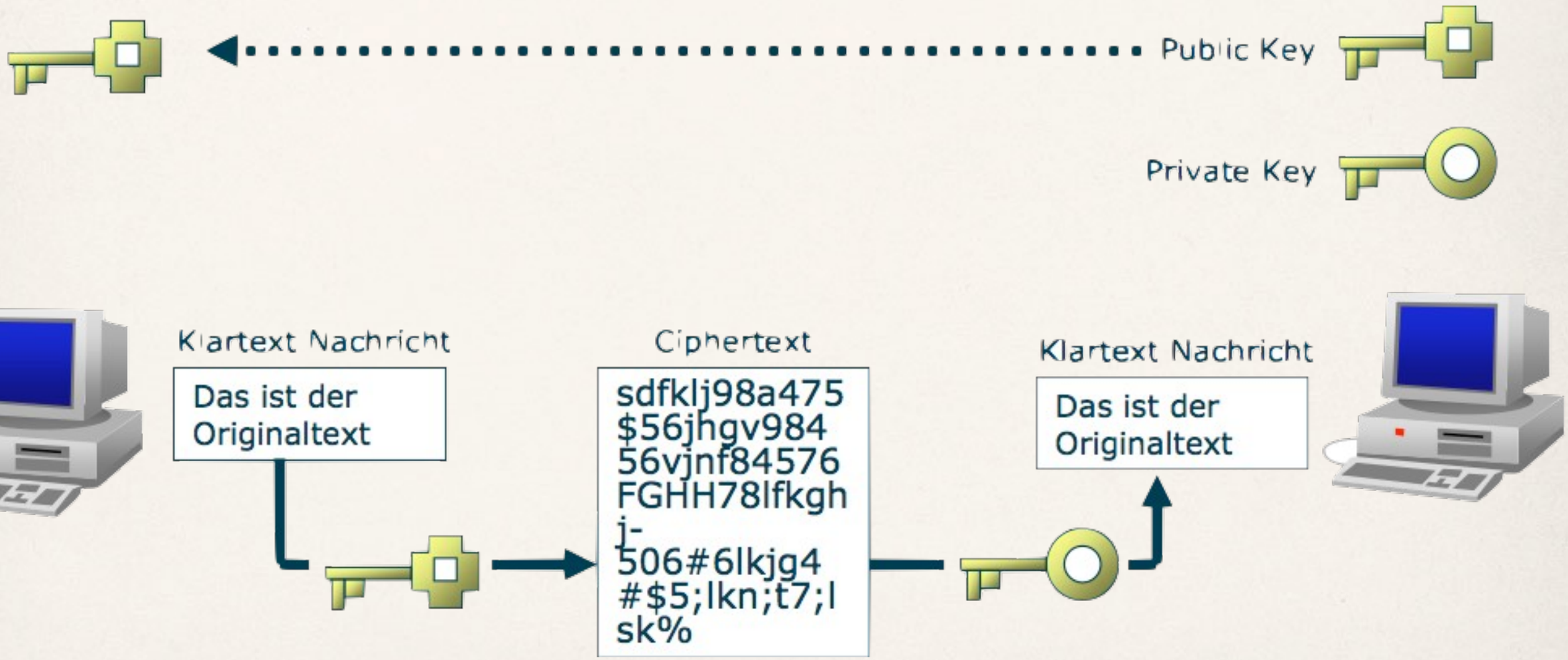


Grundlegende Verschlüsselungsarten

- **Asymmetrische Verschlüsselung**
  Es werden zwei separate Schlüssel (*private/public*) für die Ver- und Entschlüsselung verwendet.
- Vorteil:
  - der *public keys* kann öffentlich gemacht werden
  - der *private key* bleibt geheim
  - dadurch wird **Vertraulichkeit**, **Integrität** und **Authentifizierung** erreicht.
- Nachteil:
  - Langsam (ca. 1000 mal langsamer als symmetrische Verschlüsselung)

Grundlegende Verschlüsselungsarten

- **Asymmetrische Verschlüsselung**



Grundlegende Verschlüsselungsarten

- **Einweg Hash Funktion**
  Diese Funktion bildet aus einer Nachricht mit einer variablen Länge ein *Hash-Digest* mit fester Länge.

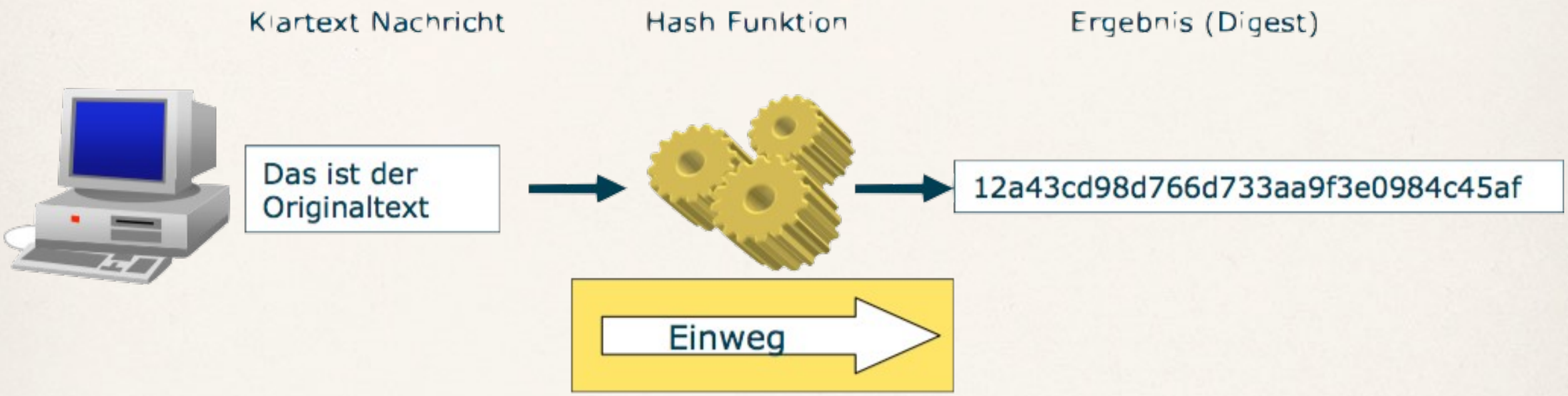
- Das *Hash-Digest* kann nicht wieder entschlüsselt werden.

- Dieses *Hash-Digest* wird bei der digitalen Unterschrift mit verwendet.

- dadurch wird **Integrität** erreicht.

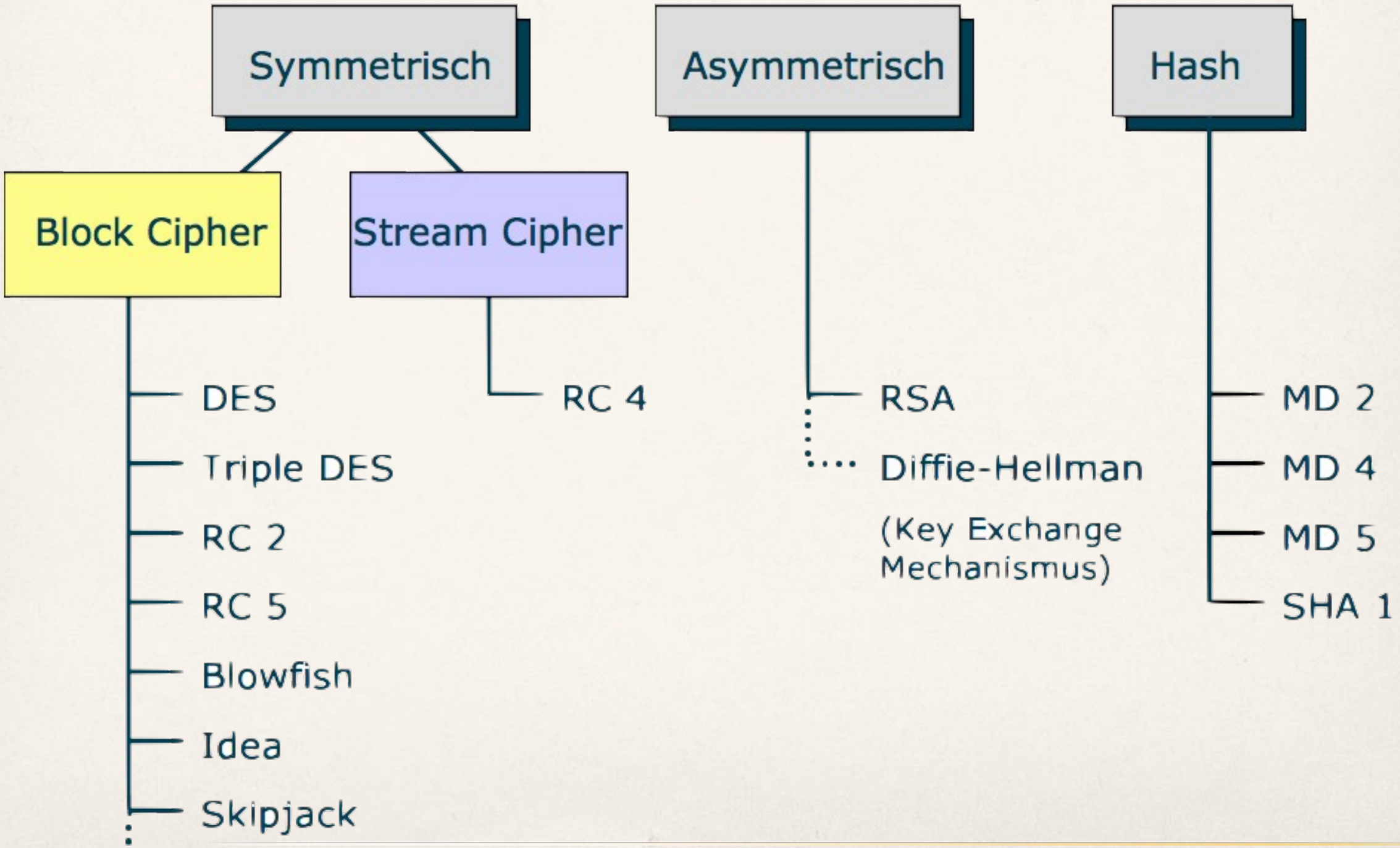
Grundlegende Verschlüsselungsarten

- **Einweg Hash Funktion**



Grundlegende Verschlüsselungsarten

- **Algorithmen**



Verschlüsselungsarten angewandt

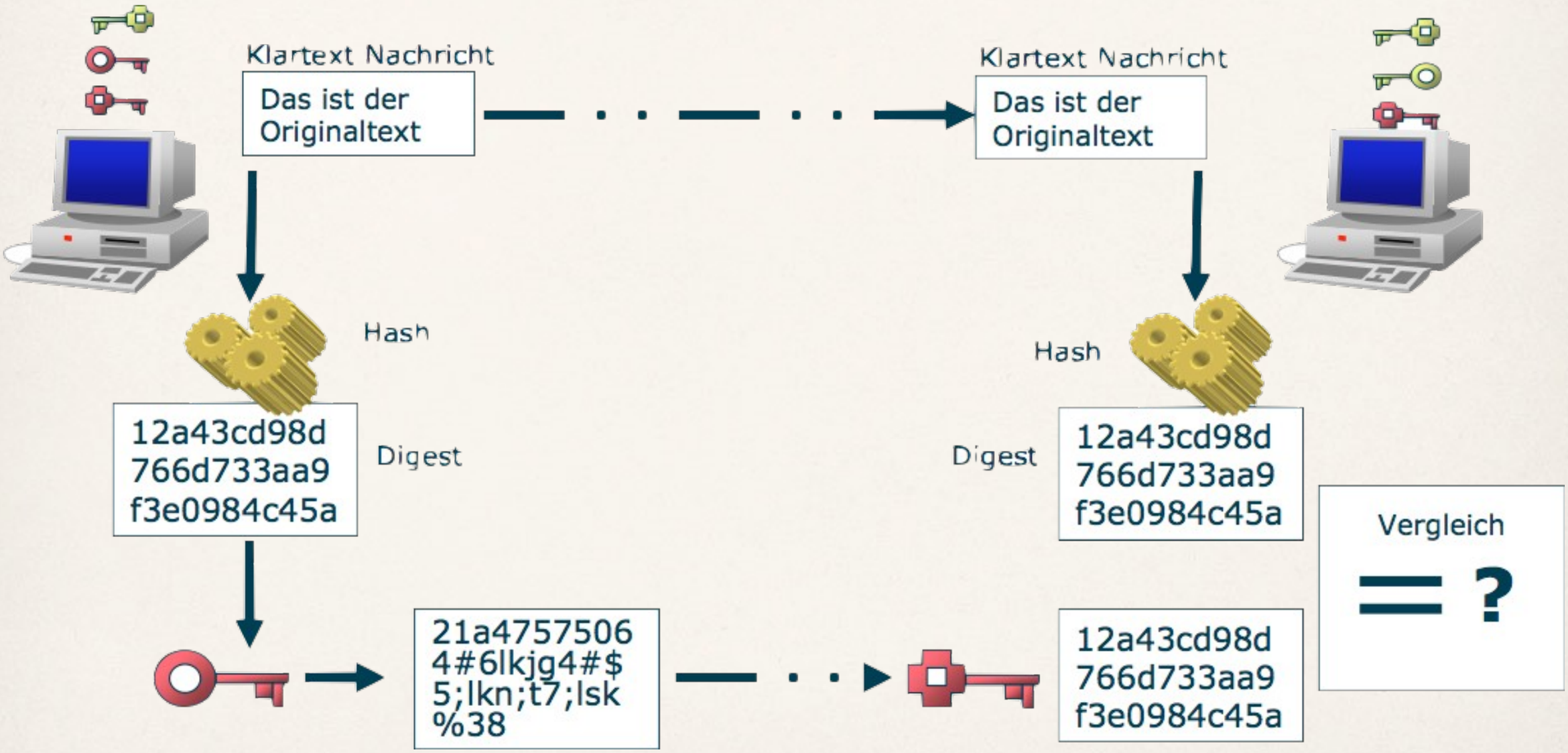
- **Digitale Unterschrift**
  dient zur:
  - Eindeutigen Identifikation des Absenders
  - Überprüfung der Datenintegrität
- Ablauf:
  - Aus der Originalnachricht wird beim Sender ein *Hash-Digest* gebildet.
  - Der Sender verschlüsselt das *Hash-Digest* mit seinem *Private key*.
  - Der Empfänger bildet aus der Originalnachricht ebenfalls einen *Hash-Digest*.
  - Er entschlüsselt das erhaltene *Digest* mit dem *Puplic Key* des Partners.
  - Er vergleicht die zwei *Digest*, bei deren Übereinstimmung ist der Sender verifiziert.

Verschlüsselungsarten angewandt

- **Digitale Unterschrift**
  Voraussetzung ist, dass die Partner im Besitz des jeweiligen *Public Key* des anderen Partners sind.

Verschlüsselungsarten angewandt

- **Digitale Unterschrift**

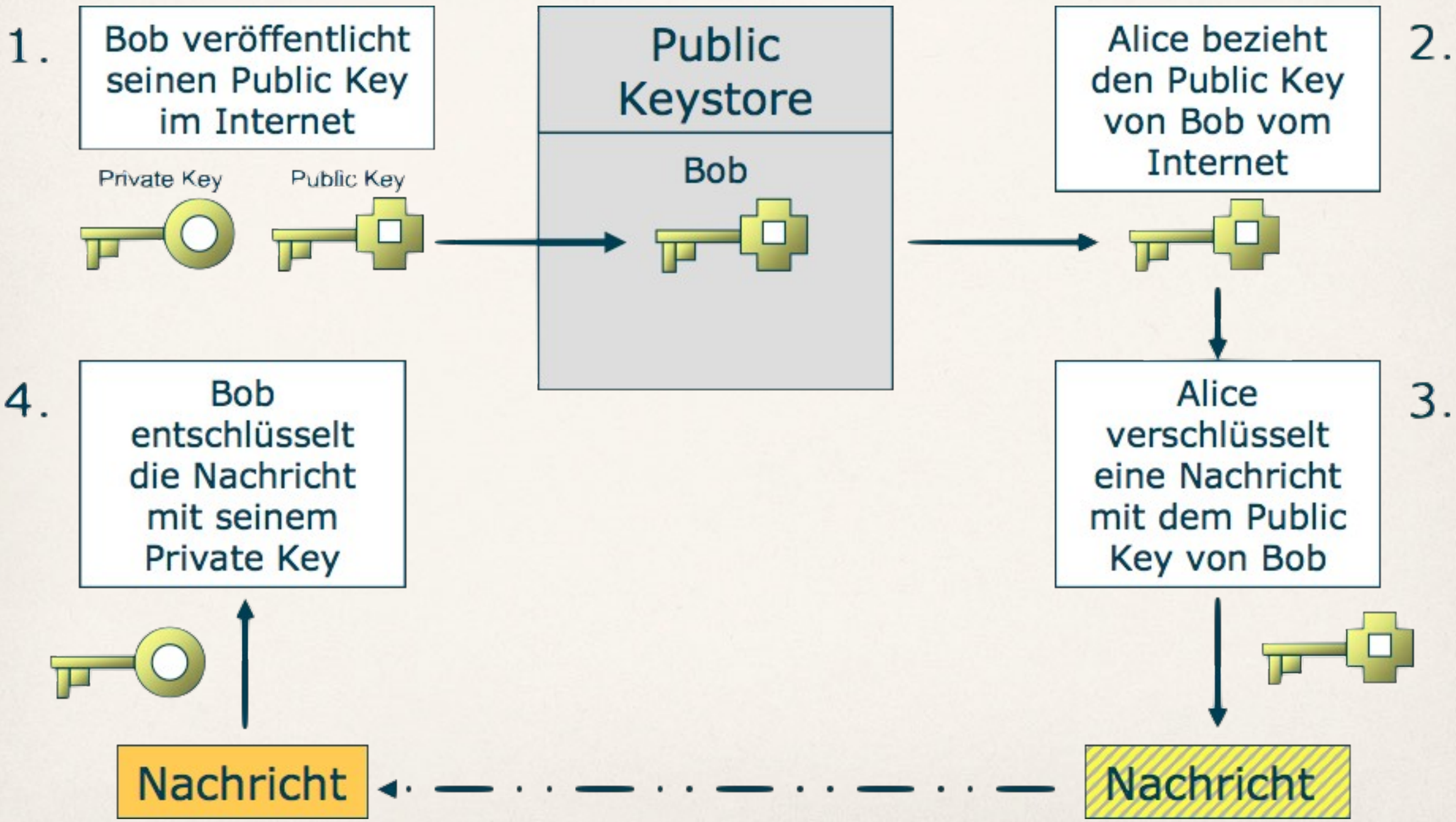


Verschlüsselungsarten angewandt

- **Problematik der grundlegenden Verschlüsselungsarten**
  - Symmetrische Verschlüsselung
    - Diese kann als sicher angesehen werden, solange der Schlüssel geheim bleibt.
    - Die Schlüsselübertragung ist aber kritisch
  - Asymmetrische Verschlüsselung
    - Löst das Austauschproblem, da die *Public Keys* veröffentlicht werden können.
    - Die übertragenen Daten sind gesichert, der Absender kann aber nicht verifiziert werden (*Man-in-the-Middle-Attack*).
    - Praktisch kann jeder seinen *Public Key* unter einer beliebigen Identität veröffentlichen.

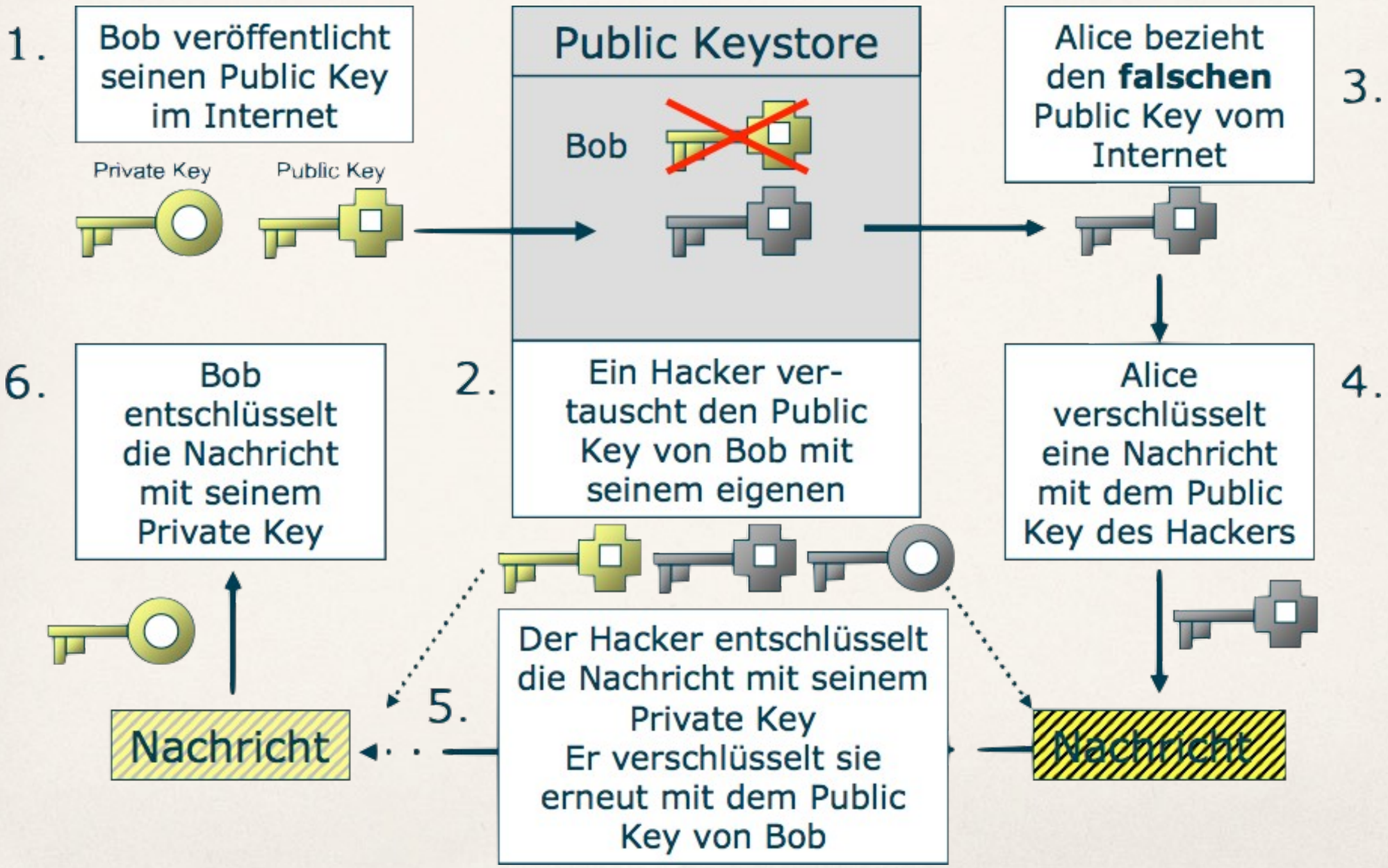
Verschlüsselungsarten angewandt

* **Beispiel:** Alice sendet Bob eine verschlüsselte Nachricht



Verschlüsselungsarten angewandt

- **Beispiel:** *Man-in-the-Middle-Attack*

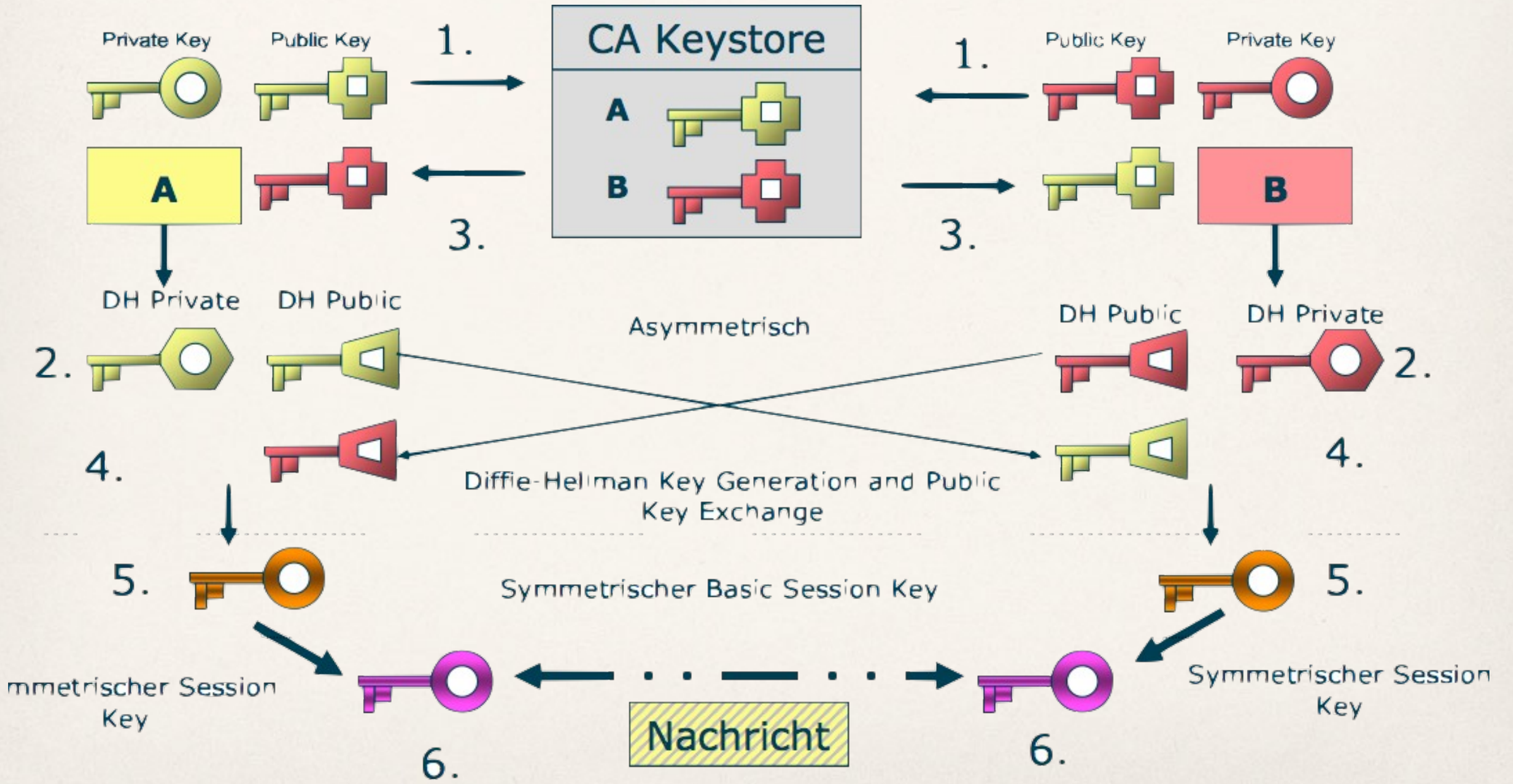


Verschlüsselungsarten angewandt

- **Sichere Schlüsselaustauschsysteme**
  - Schlüsselaustauschsysteme lassen einen sicheren Austausch eines *Public Key* über unsichere Netze wie z.B. das Internet zu.
  - Dazu werden die *Public Keys* mehrfach verändert und getauscht.
  - Ein sicheres Schlüsselaustauschsystem ist das Schlüsselaustauschprotokoll dach *Diffie-Hellmann*

Verschlüsselungsarten angewandt

- **Schlüsselaustauschverfahren nach *Diffie-Hellmann***



Verschlüsselungsarten angewandt

- **Schlüsselaustauschverfahren nach *Diffie-Hellmann***
  Ablauf:
  - *Public Key*
    - Der eigene *Public Key* wird über eine dritte Partei, der *CA* (*Certified Authority*), verifiziert und hinterlegt.
    - Der *Public Key* muss verifiziert sein, um eine *Man-in-the-Middle-Attack* auszuschließen.
  - *Diffie-Hellmann Key* Erzeugung
    - Das *Diffie-Hellmann-Key-Pair* wird gebildet.
  - *Public Key* Austausch
    - Die *Public Keys* werden von der *CA* bezogen.
    - Die *Public Keys* können auch direkt vom Partner bezogen werden, wenn diese durch die Partner selbst vertrauensvoll und über sichere Kanäle verifiziert werden.
  - *Diffie-Hellmann Public Key* Austausch
    - Die *DH-Public Keys* werden zwischen den Partnern getauscht.

Verschlüsselungsarten angewandt

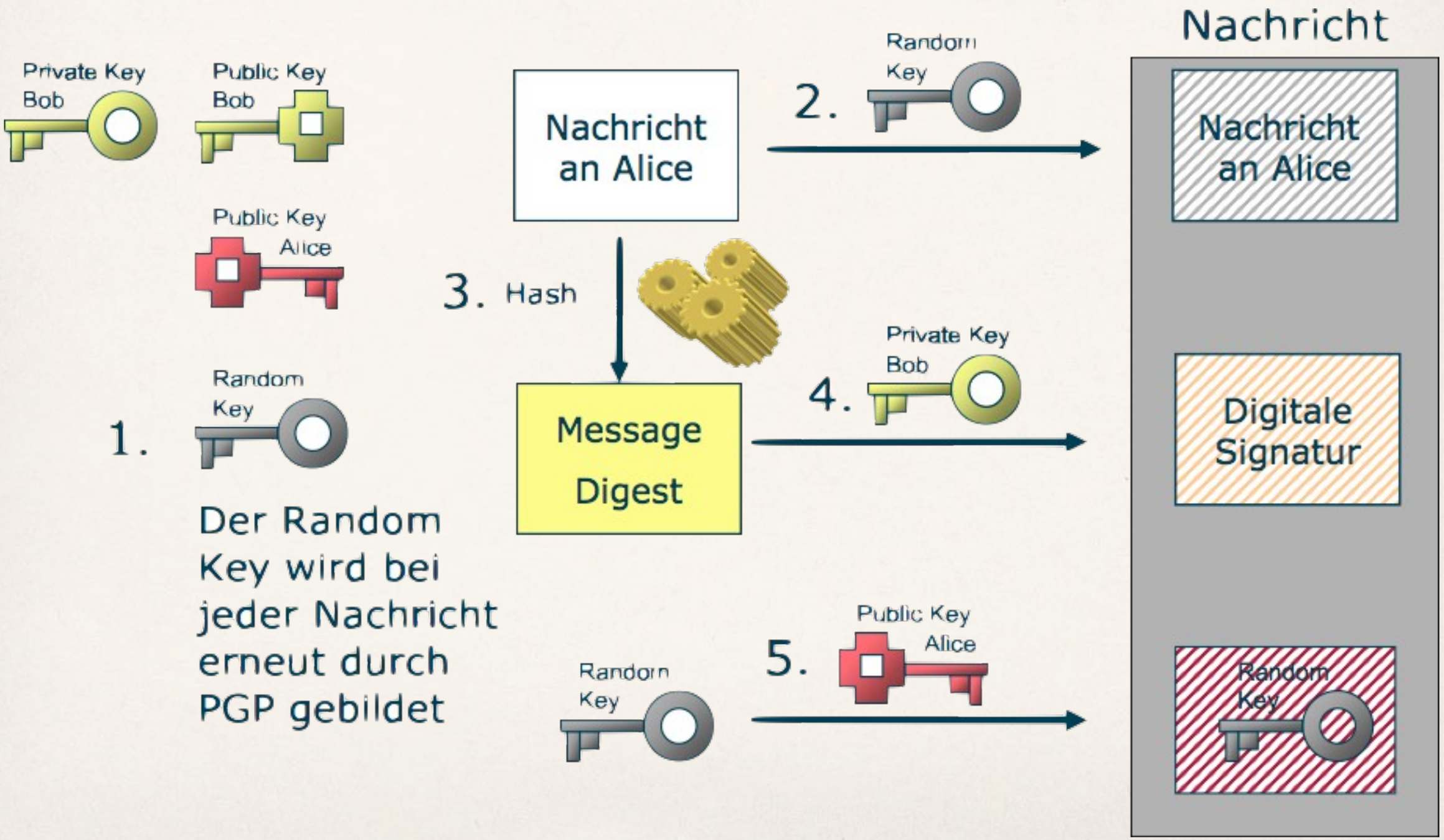
- **Schlüsselaustauschverfahren nach *Diffie-Hellmann***
  Ablauf:
  - *Basic Session Key*
    - Mittels der getauschten *Diffie-Hellmann-Public Keys* wird ein symmetrischer Schlüssel, der *Basic session Key*, berechnet.
  - *Session Key*
    - Aus dem *Basic Session Key* wird ein weiterer, symmetrischer Schlüssel abgeleitet, der zum Verschlüsseln der Nachricht verwendet wird (*Session Key*).
- Vorteile des Schlüsselaustauschverfahrens nach *Diffie-Hellmann*
  Da sich die *Diffie-Hellmann Keys* von den *CA-Keys* ableiten, können die *DH-Keys* von Zeit zu Zeit automatisch neu generiert, getauscht und sicher über ein unsicheres Netz, meist das Internet, übertragen werden.

Kombinierte Verschlüsselungsverfahren

- In kombinierten Verschlüsselungsverfahren werden die Vorteile der asymmetrischen und der symmetrischen Verschlüsselungsverfahren genutzt.
- Die symmetrische Verschlüsselung ist schneller und eignet sich für große Datenmengen, die Schlüsselverteilung ist kritisch.
- Die asymmetrische Verschlüsselung erlaubt den Austausch von *Public Keys* über das Internet, ist aber langsamer.
- Verfahren die dies anwenden sind z.B.:
  - *PGP* (*Pretty Good Privacy*)
  - *S-Mime* (*Secure-Mime*)

Kombinierte Verschlüsselungsverfahren

* **Beispiel:** Bob sendet an seinem PC eine verschlüsselte Nachricht mittels *PGP* an Alice

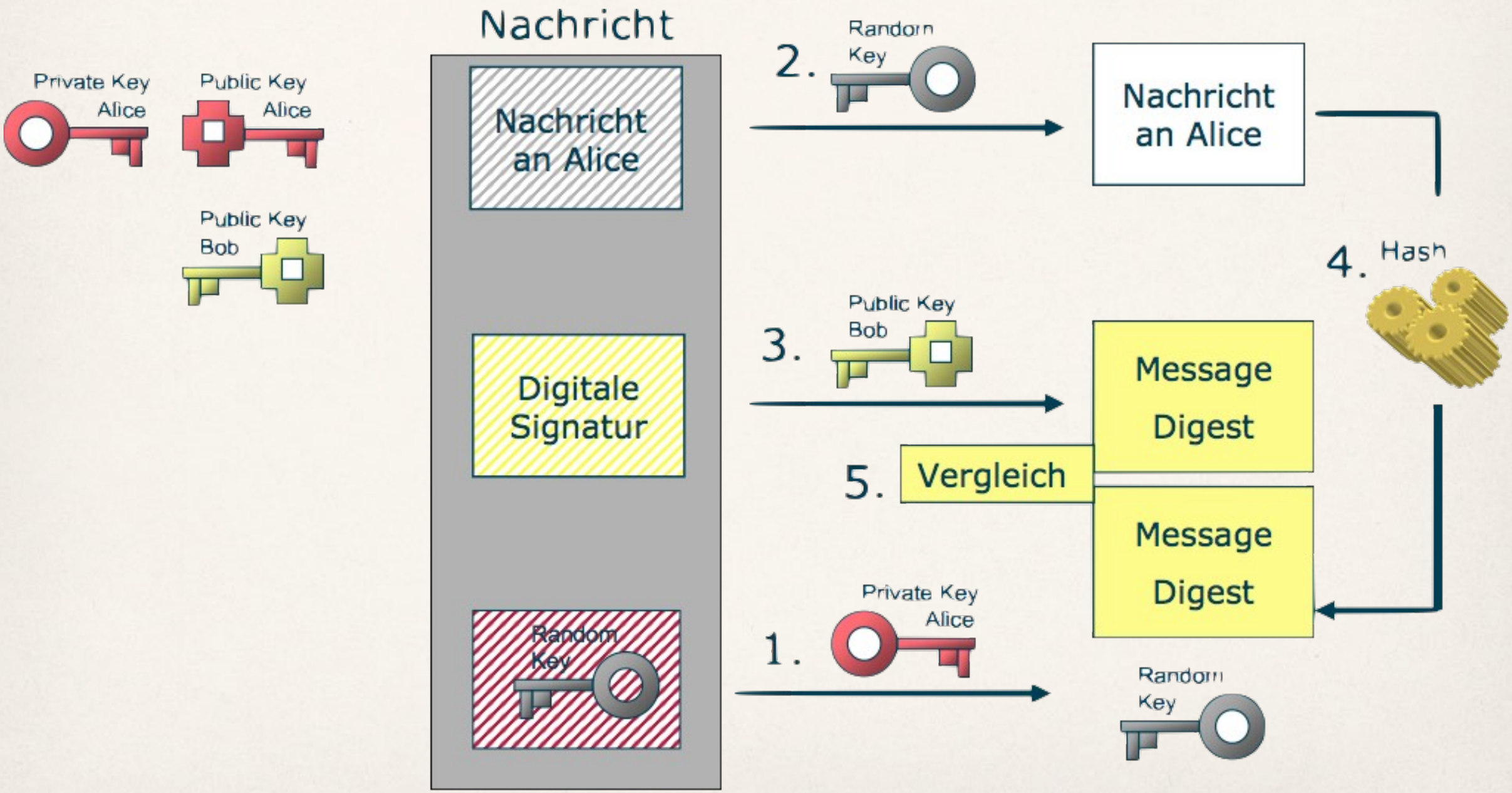


Kombinierte Verschlüsselungsverfahren

- **Bob sendet von seinem PC eine verschlüsselte Nachricht mittels *PGP* an Alice**
  Ablauf:
  - Ein zufälliger Schlüssel (*Random Key*) wird bei jeder Nachricht erneut durch *PGP* gebildet.
  - Mit dem *Random Key* wird die Nachricht verschlüsselt.
  - Aus der Nachricht wird mittels eines *Hash*-Algorithmus das *Message Digest* gebildet.
  - Das *Message Digest* wird mit dem *Private Key* des Senders verschlüsselt und so die Digitale Unterschrift gebildet, die der Nachricht beigefügt wird.
  - Der *Random Key* wird mit dem *Public Key* des Empfängers verschlüsselt und der Nachricht zugefügt.

Kombinierte Verschlüsselungsverfahren

* **Beispiel:** Alice empfängt eine verschlüsselte Nachricht von Bob und entschlüsselt diese



Kombinierte Verschlüsselungsverfahren

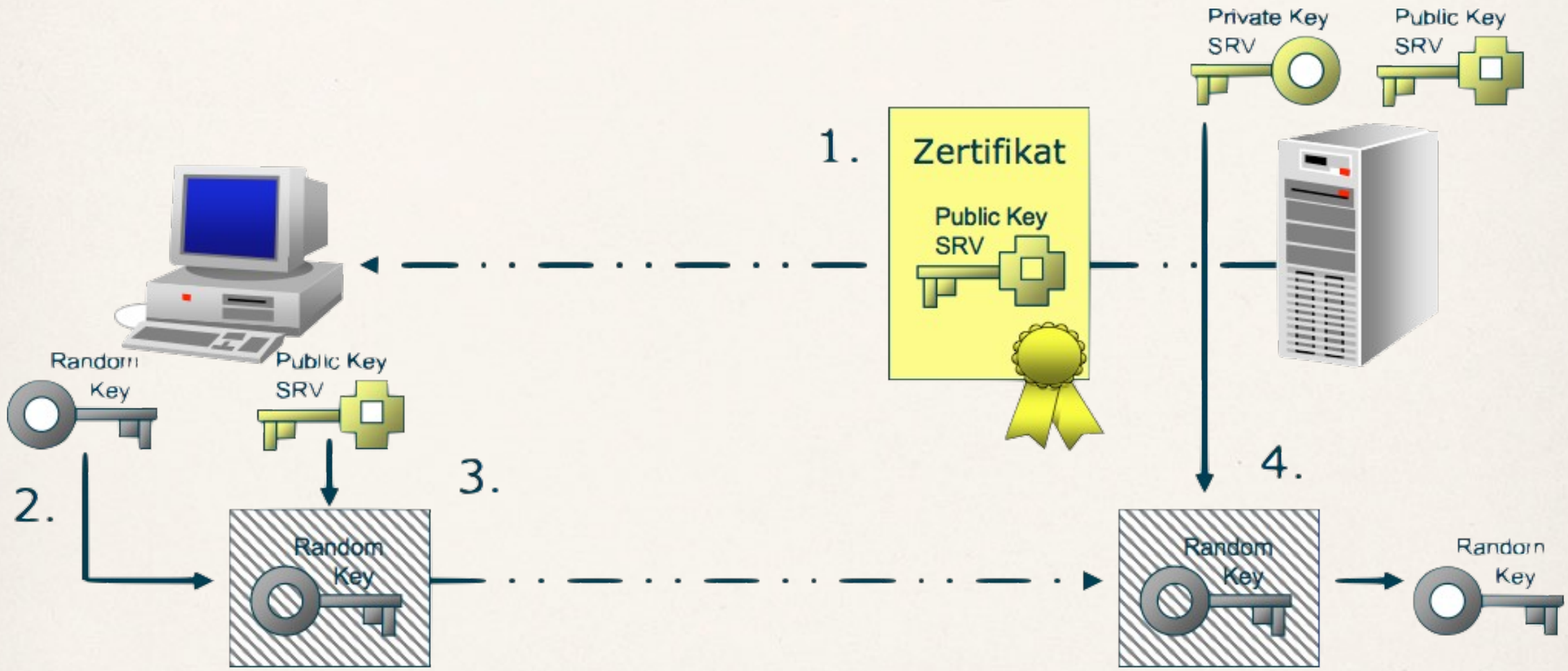
- **Alice empfängt eine verschlüsselte Nachricht von Bob und entschlüsselt diese**
  Ablauf:
  - Der verschlüsselte *Random Key* wird mit dem *Private Key* des Empfängers entschlüsselt
  - Der entschlüsselte *Random Key* wird zur Entschlüsselung der Nachricht verwendet.
  - Mit dem *Public Key* des Partners wird die digitale Unterschrift entschlüsselt, das Ergebnis ist das *Message Digest*.
  - Aus der Originalnachricht wird mittels eines *Hash*-Algorithmus das *Message Digest* erneut gebildet.
  - Die beiden *Message Digests* werden miteinander verglichen. Stimmen diese überein, ist der Absender verifiziert.

Kombinierte Verschlüsselungsverfahren

- ***Secure Sockets Layer* (*SSL*)**
  - 1995 durch Netscape entwickelt, hat sich gegen S-HTTP durchgesetzt.
  - Nicht protokollgebunden (*HTTP*, *SMTP*, *NNTP*, *Telnet*, *FTP*)
  - Verwendet *Port* 443 mit *HTTPS*, *Port* 465 mit *SSMTP*, ...
  - Nur für *TCP*-Dienste einsetzbar
- ***Secure HTTP* (*S-HTTP*)**
  - 1994 durch Teresia Systems (*RSA*) entwickelt
  - Protokollgebunden an *HTTP*
  - Verwendet *Port* 443

Kombinierte Verschlüsselungsverfahren

- **Verschlüsselung unter *S-HTTP* oder *SSL***



Kombinierte Verschlüsselungsverfahren

- **Verschlüsselung unter *S-HHTP* oder *SSL***
  Ablauf:
  - Der Server sendet sein Zertifikat an den Client.
  - Der Client bildet einen zufälligen, eindeutigen Schlüssel (*Random Key)*.
  - Der Client verschlüsselt den zufälligen Schlüssel mit dem öffentlichen Schlüssel (*Public Key*) des Servers aus dem Zertifikat.
  - Der Client überträgt den Schlüssel zum Server.
  - Der Server entschlüsselt den zufälligen Schlüssel mit seinem privaten Schlüssel (*Privat Key*)

Digitale Zertifikate

- Zwei der vier wichtigsten Bedingungen wurden durch die bisherigen Verfahren erreicht:
  - **Vertraulichkeit** durch Verschlüsselung der Daten
  - **Integrität** durch das *Hash*-Prüfzeichen
- Nur teilweise erfüllt wurde:
  - **Authentifizierung** durch digitale Unterschrift
- Nicht erfüllt wurde:
  - **Non-Repudation**
- Um diese Forderungen zu erfüllen werden **digitale Zertifikate** benötigt.

Digitale Zertifikate

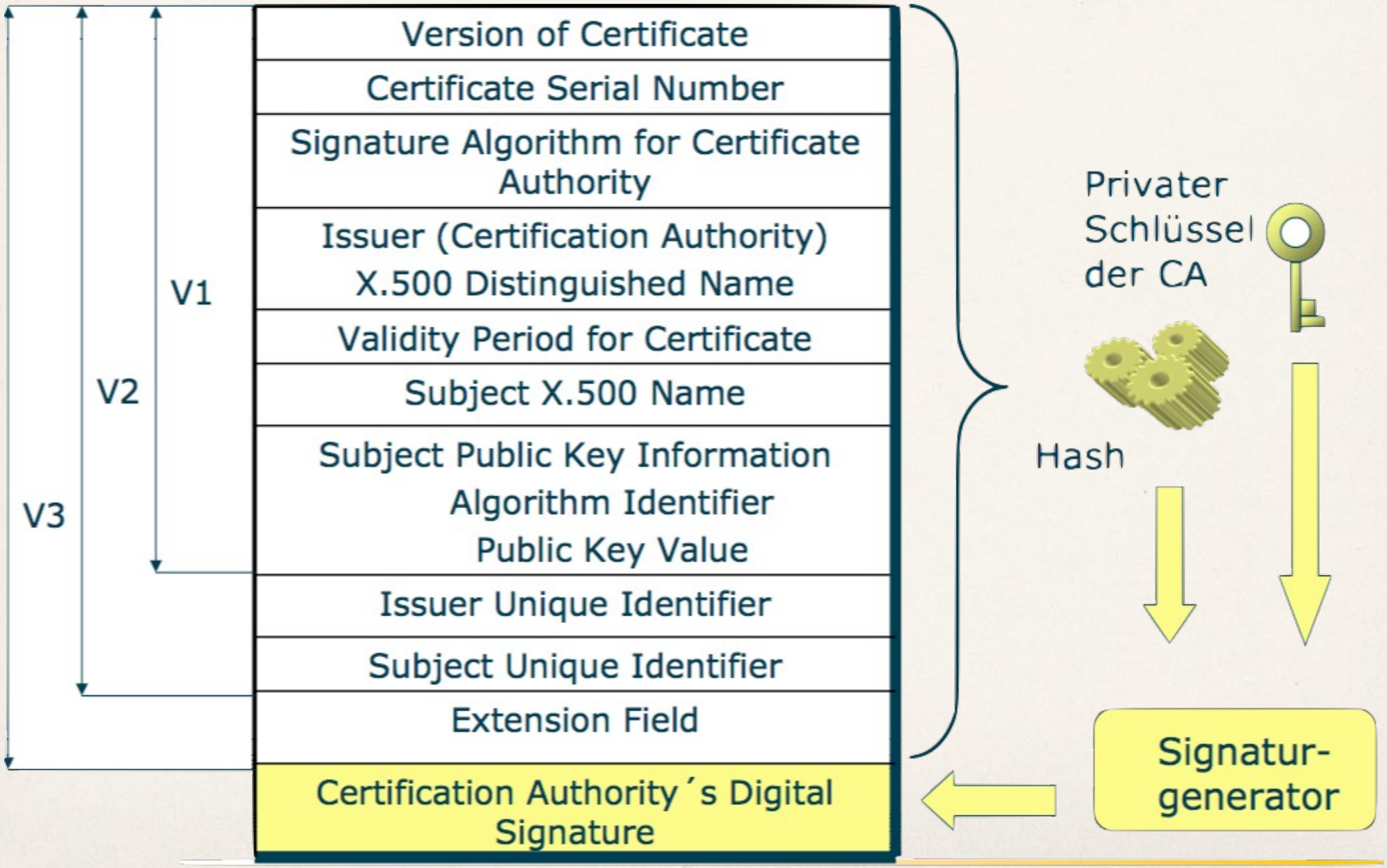
- Warum Digitale Zertifikate?
  - Asymmetrische Schlüssel ermöglichen eine sichere Kommunikation mittels verteiltem *Public Key.*
  - Es können aber auch falsche Schlüssel verbreitet werden.
  - Deshalb muss die Echtheit eines öffentlichen Schlüssels (*Public Key*) bestätigt werden.
  - Die **Digitalen Zertifikate** enthalten *Public Key*, die von einer oder mehreren vertrauten Parteien (*CA, Trust Center*) elektronisch unterschrieben sind.

Digitale Zertifikate

- *Trust Center*
  - Ein *Trust Center* ist als Notar für Digitale Zertifikate zu sehen.
  - Nur die Zertifikate von beglaubigten Besitzern werden publiziert.
  - Die Zertifikate können beim *Trust Center* geprüft werden.
  - *Trust Center* verwalten die Zertifikate und publizieren gesperrte Zertifikate.
  - Ein *Trust Center* kann eine öffentliche Einrichtung sein:
    - Deutsche Telekom Root CA 2 (*http://www.t-systems-zert.com/*)
  - Ein *Trust Center* kann aber auch ein Zertifikatsserver innerhalb eines Unternehmens sein:
    - FHI CA (*https://pki.pca.dfn.de/fhi-ca/cgi-bin/pub/pki*)
  - Ein *Trust Center* muss auf alle Fälle vertrauenswürdig sein!

Digitale Zertifikate

- **Beispiel:** Das Zertifikat nach X.509

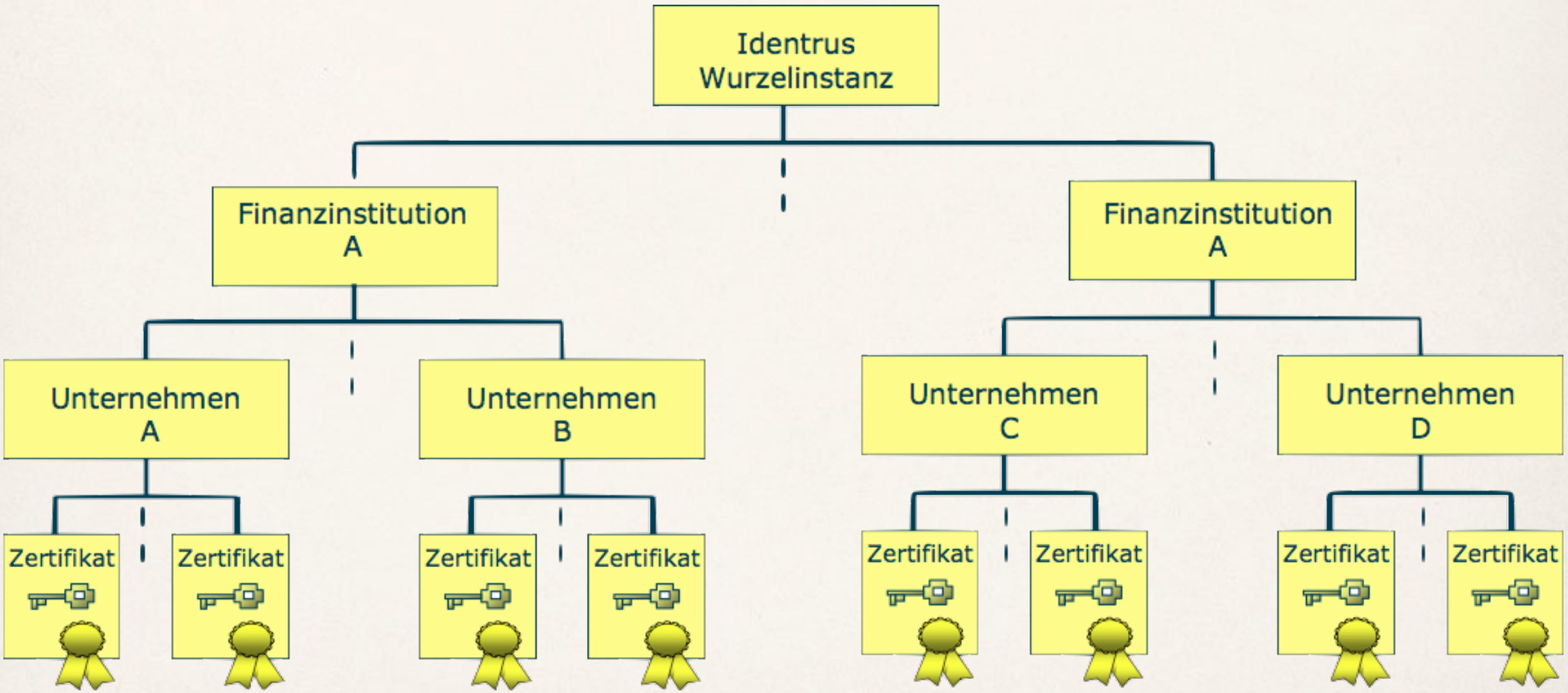


Digitale Zertifikate

- *Trust Center*
  - Da verschiedene Firmen oder Privatpersonen Mitglied bei verschiedenen *Trust Centern* sein können, muss eine Verbindung zwischen den *Trust Centern* bestehen.
  - Die *Trust Center* haben sich z.T. hierarchisch organisiert.
  - Die Zertifikate können beim *Trust Center* geprüft werden.
  - Das oberste *Trust Center* ist das *Root-Trust Center* oder die *Root-Certification Authority* (*CA root)* (in unserem Fall *Telekom Root CA*).
  - Verschiedene Branchen wie Banken, Rechtsanwälte unterhalten eigene *Trust Center*-Hierarchien. Auch die Forschung in Deutschland mit dem *DFN-PKI (http://www.pki.dfn.de/)*.

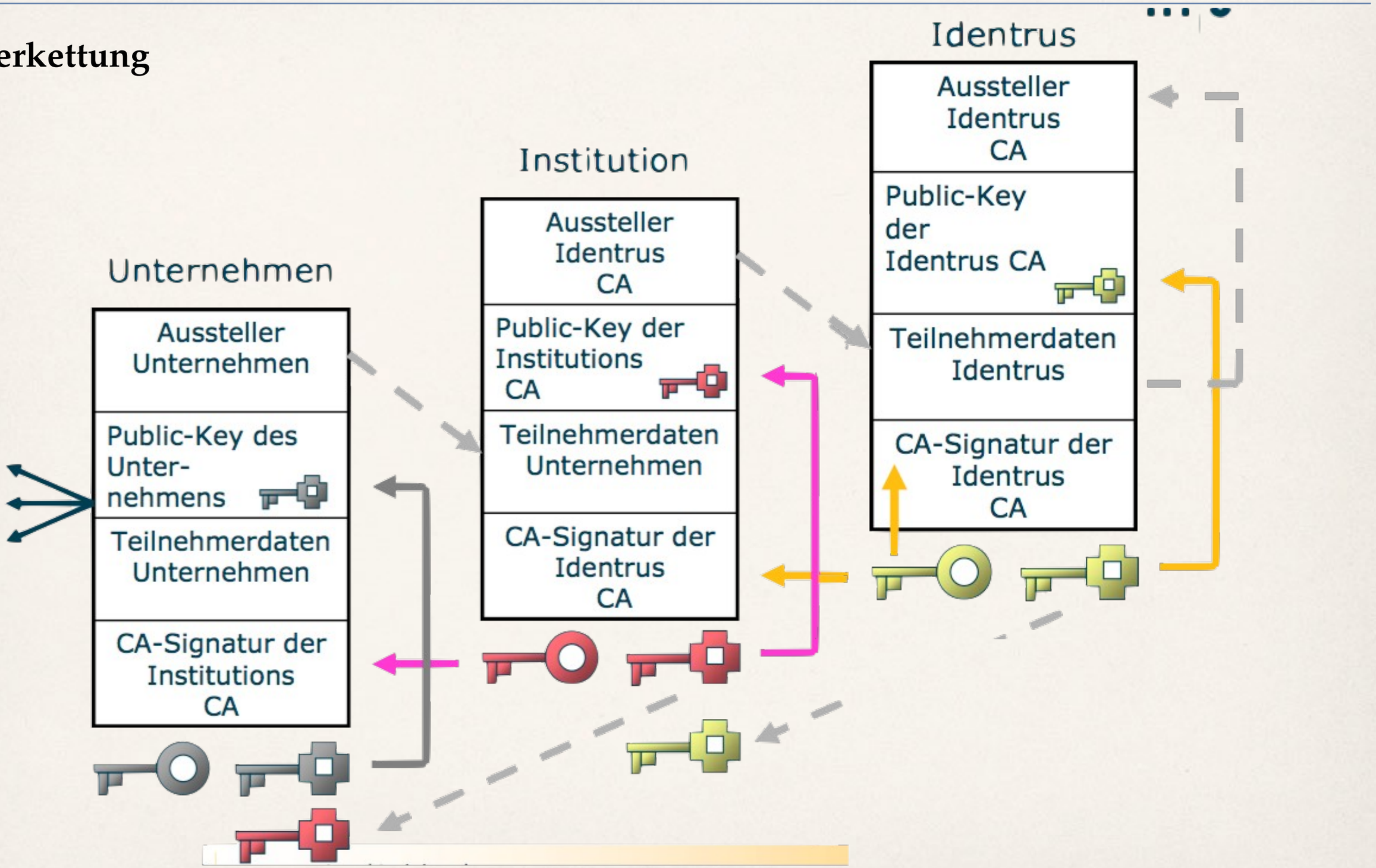
Digitale Zertifikate

- **Beispiel:** Zertifizierungshierarchie anhand des vierstufigen Identrus-Vetrauensmodell für Finanzinstitute



Digitale Zertifikate

- **Verkettung**



Digitale Zertifikate

subject= /C=DE/ST=Berlin/L=Berlin/O=Fritz-Haber-Institut der Max-Planck-Gesellschaft/OU=PPB/CN=Fritz-Haber-Institut CA/emailAddress=pki@fhi-berlin.mpg.de

-----BEGIN CERTIFICATE-----
MIIFUjCCBDqgAwIBAgIEDWWuVjANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJE
RTETMBEGA1UEChMKREZOLVZlcmVpbjEQMA4GA1UECxMHREZOLVBLSTEkMCIGA1UE
AxMbREZOLVZlcmVpbiBQQ0EgR2xvYmFsIC0gRzAxMB4XDTA4MTIxNTEwMjYxNFoX
DTE5MDYzMDAwMDAwMFowgcAxCzAJBgNVBAYTAkRFMQ8wDQYDVQQIEwZCZXJsaW4x
DzANBgNVBAcTBkJlcmxpbjE5MDcGA1UEChMwRnJpdHotSGFiZXItSW5zdGl0dXQg
ZGVyIE1heC1QbGFuY2stR2VzZWxsc2NoYWZ0MQwwCgYDVQQLEwNQUEIxIDAeBgNV
BAMTF0ZyaXR6LUhhYmVyLUluc3RpdHV0IENBMSQwIgYJKoZIhvcNAQkBFhVwa2lA
ZmhpLWJlcmxpbi5tcGcuZGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCdbKsulcWodpHUmz9/G/gblsCpY3rYzPochxiDDfGi88+tlFygZRlHq0A88uWi
gtrPu4sRwFJ0spAC9UKFmRLIrKnRQMEJK+Xcca73HqR57g8NmRjaKmgDx9YuRUxO
C8OuAYPST9S7dWVp9vqYfHXT7lEqKCddEfOAR1jj5LLVMwbSGrXxVGGs3J2KnQ+X
yKjx6B7jckobN/8+Ze3wRCxl4cd9rq2vAcGMKvOq65GkCs7TKi8g5AmoT+iqqIMA
vIyL9Rr+ayYvrCT5hML9evxPh+COYlp+u9gCKeVdKfUXUpfzUDs4/Pw5RuPtcZGv
cJwAfuUY7ermoZ2SlXQPv+gBAgMBAAGjggG3MIIBszASBgNVHRMBAf8ECDAGAQH/
AgEBMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQU/GNEzTzQhWLWzQZoa0I6HyMtSXww
HwYDVR0jBBgwFoAUSbfGz+g9H3/qRHsTKffxCnA+3mQwHwYDVR0RBBkwF4EVcGtp
QGZoaS1iZXJsaW4ubXBnLmRlMIGIBgNVHR8EgYAwfjA9oDugOYY3aHR0cDovL2Nk
cDEucGNhLmRmbi5kZS9nbG9iYWwtcm9vdC1jYS9wdWIvY3JsL2NhY3JsLmNybDA9
oDugOYY3aHR0cDovL2NkcDIucGNhLmRmbi5kZS9nbG9iYWwtcm9vdC1jYS9wdWIv
Y3JsL2NhY3JsLmNybDCBogYIKwYBBQUHAQEEgZUwgZIwRwYIKwYBBQUHMAKGO2h0
dHA6Ly9jZHAxLnBjYS5kZm4uZGUvZ2xvYmFsLXJvb3QtY2EvcHViL2NhY2VydC9j
YWNlcnQuY3J0MEcGCCsGAQUFBzAChjtodHRwOi8vY2RwMi5wY2EuZGZuLmRlL2ds
b2JhbC1yb290LWNhL3B1Yi9jYWNlcnQvY2FjZXJ0LmNydDANBgkqhkiG9w0BAQUF
AAOCAQEA3Mae5E2LQhAlQtvBh8BZtYtaaIARR5dLVXQiOGr11oV74zM1E9jvHGtQ
Nb8RXXiKRnvOl7Pj9vtSUqXeYez9is6MWrzxskyw7Rzc3O/egHJC0bIkByOEbWCM
GwNfURrlKL2ZPyyYciAlwseP7YF/WBWOFzEmN6XlpQJtraBVuIiDdBfxo/ep/yYh
Kpeb5gvStvEDWe0H2AwHzXtHRnKICDU2A+VEN6BGvKGnqEMnGs6HjbO8D/ltc7Yd
X2mplyEc9mlncqI0prk1QnKbK9lGjpDs3J8/0qXhS3PgJif/crO6jzeSVZ6SqSAM
sYDy30SLblWMde/NUuJhVjn8Pc20eA==
-----END CERTIFICATE-----

subject= /C=DE/O=DFN-Verein/OU=DFN-PKI/CN=DFN-Verein PCA Global - G01

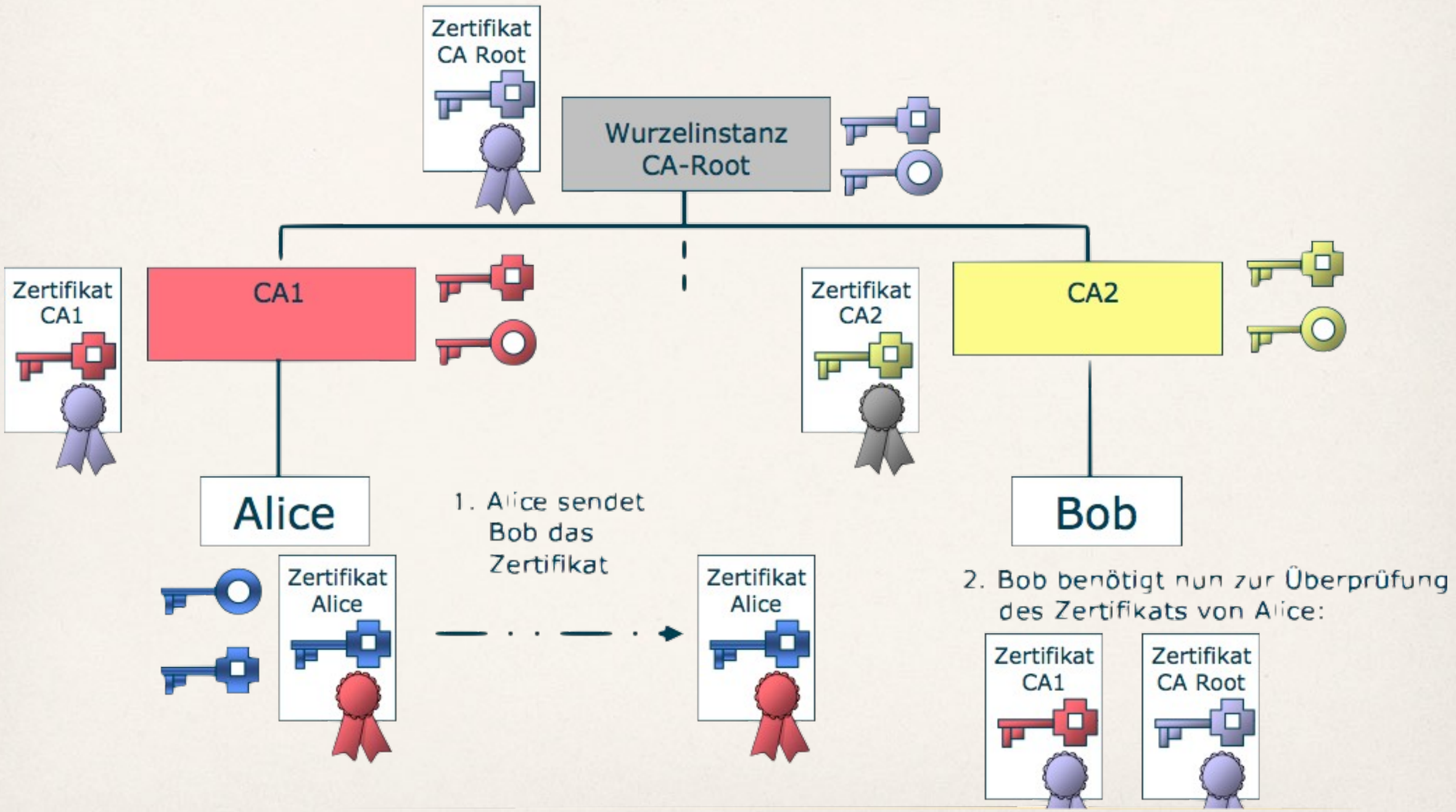
-----BEGIN CERTIFICATE-----
MIIEITCCAwmgAwIBAgICAMcwDQYJKoZIhvcNAQEFBQAwcTELMAkGA1UEBhMCREUx
HDAaBgNVBAoTE0RldXRzY2hlIFRlbGVrb20gQUcxHzAdBgNVBAsTFlQtVGVsZVNl
YyBUcnVzdCBDZW50ZXIxIzAhBgNVBAMTGkRldXRzY2hlIFRlbGVrb20gUm9vdCBD
QSAyMB4XDTA2MTIxOTEwMjkwMFoXDTE5MDYzMDIzNTkwMFowWjELMAkGA1UEBhMC
REUxEzARBgNVBAoTCkRGTi1WZXJlaW4xEDAOBgNVBAsTB0RGTi1QS0kxJDAiBgNV
BAMTG0RGTi1WZXJlaW4gUENBIEdsb2JhbCAtIEcwMTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAOmbw2eF+Q2u9Y1Uw5ZQNT1i6W5M7ZTXAFuVInTUIOs0
j9bswDEEC5mB4qYU0lKgKCOEi3SJBF5b4OJ4wXjLFssoNTl7LZBF0O2gAHp8v0oO
GwDDhulcKzERewzzgiRDjBw4i2poAJru3E94q9LGE5t2re7eJujvAa90D8EJovZr
zr3TzRQwT/Xl46TIYpuCGgMnMA0CZWBN7dEJIyqWNVgn03bGcbaQHcTt/zWGfW8z
s9sPxRHCioOhlF1Ba9jSEPVM/cpRrNm975KDu9rrixZWVkPP4dUTPaYfJzDNSVTb
yRM0mnF1xWzqpwuY+SGdJ68+ozk5SGqMrcmZ+8MS8r0CAwEAAaOB2TCB1jBwBgNV
HR8EaTBnMGWgY6Bhhl9odHRwOi8vcGtpLnRlbGVzZWMuZGUvY2dpLWJpbi9zZXJ2
aWNlL2FmX0Rvd25sb2FkQVJMLmNybD8tY3JsX2Zvcm1hdDlYXzUwOSYtaXNzdWVy
PURUX1JPT1RfQ0FfMjAdBgNVHQ4EFgQUSbfGz+g9H3/qRHsTKffxCnA+3mQwHwYD
VR0jBBgwFoAUMcN5G7r1U9cX4I16LRdsCrMrnTMwDgYDVR0PAQH/BAQDAgEGMBIG
A1UdEwEB/wQIMAYBAf8CAQIwDQYJKoZIhvcNAQEFBQADggEBADvhWnfASBfcqRjs
ga9aifC9KJKmylkYEnDsKPLnrn+WLOfyXRkx9hMrdL29gLK592fJOaJ5O+EREe5r
eJEzfjtfJidlU2WOM2Puz3PDsJIjSSFQdSOhHxjilIU9PzPpdyCNor3moYUpQPY/
czJYDQlrptqFbMA/u41mZFYkTq4NPzI1AVvpjILZcllPsYaF8XSFVuXD+Fzzje5H
s1MFcOflTYppgyjhEwmGnl7I6lgeDB/5pNRaBGj9KD6LArZYtfahLDdXAGerI2iN
Y6XvmWtc/UtW9qtAhzTUEZJs7IfFCgsHM3K0bwwdVCzYUcfMvzDTQ3LxMr+Mzklj
qAD38hw=
-----END CERTIFICATE-----

subject= /C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2

-----BEGIN CERTIFICATE-----
MIIDnzCCAoegAwIBAgIBJjANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEwJERTEc
MBoGA1UEChMTRGV1dHNjaGUgVGVsZWtvbSBBRzEfMB0GA1UECxMWVC1UZWxlU2Vj
IFRydXN0IENlbnRlcjEjMCEGA1UEAxMaRGV1dHNjaGUgVGVsZWtvbSBSb290IENB
IDIwHhcNOTkwNzA5MTIxMTAwWhcNMTkwNzA5MjM1OTAwWjBxMQswCQYDVQQGEwJE
RTEcMBoGA1UEChMTRGV1dHNjaGUgVGVsZWtvbSBBRzEfMB0GA1UECxMWVC1UZWxl
U2VjIFRydXN0IENlbnRlcjEjMCEGA1UEAxMaRGV1dHNjaGUgVGVsZWtvbSBSb290
IENBIDIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCrC6M14IspFLEU
ha88EOQ5bzVdSq7d6mGNlUn0b2SjGmBmpKlAIoTZ1KXleJMOaAGtuU1cOs7TuKhC
QN/Po7qCWWqSG6wcmtoIKyUn+WkjR/Hg6yx6m/UTAtB+NHzCnjwAWav12gz1Mjwr
rFDa1sPeg5TKqAyZMg4ISFZbavva4VhYAUlfckE8FQYBjl2tqriTtM2e66foai1S
NNs671x1Udrb8zH57nGYMsRUFUQM+ZtV7a3fGAigo4aKSe5TBY8ZTNXeWHmb0moc
QqvF1afPaA+W5OFhmHZhyJF81j4A4pFQh+GdCuatl9Idxjp9y7zaAzTVjlsB9WoH
txa2bkp/AgMBAAGjQjBAMB0GA1UdDgQWBBQxw3kbuvVT1xfgiXotF2wKsyudMzAP
BgNVHRMECDAGAQH/AgEFMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQUFAAOC
AQEAlGRZrTlk5ynrE/5aw4sTV8gEJPB0d8Bg42f76Ymmg7+Wgnxu1MM9756Abrsp
tJh6sTtU6zkXR34ajgv8HzFZMQSyzhfzLMdiNlXiItiJVbSYSKpk+tYcNthEeFpa
IzpXl/V6ME+un2pMSyuOoAPjPuCp1NJ70rOo4nI8rZ7/gFnkm0W09juwzTkZmDLl
6iFhkOQxIY40sfcvNUqFENrnijchvllj4PKFiDFT1FQUhXB59C4Gdyd1Lx+4ivn+
xbrYNuSD7Odlt79jWvNGr4GUN9RBjNYj1h7P9WgbRGOiWrqnNVmh5XAFmw4jV5mU
Cm26OWMohpLzGITY+9HPBVZkVw==
-----END CERTIFICATE-----

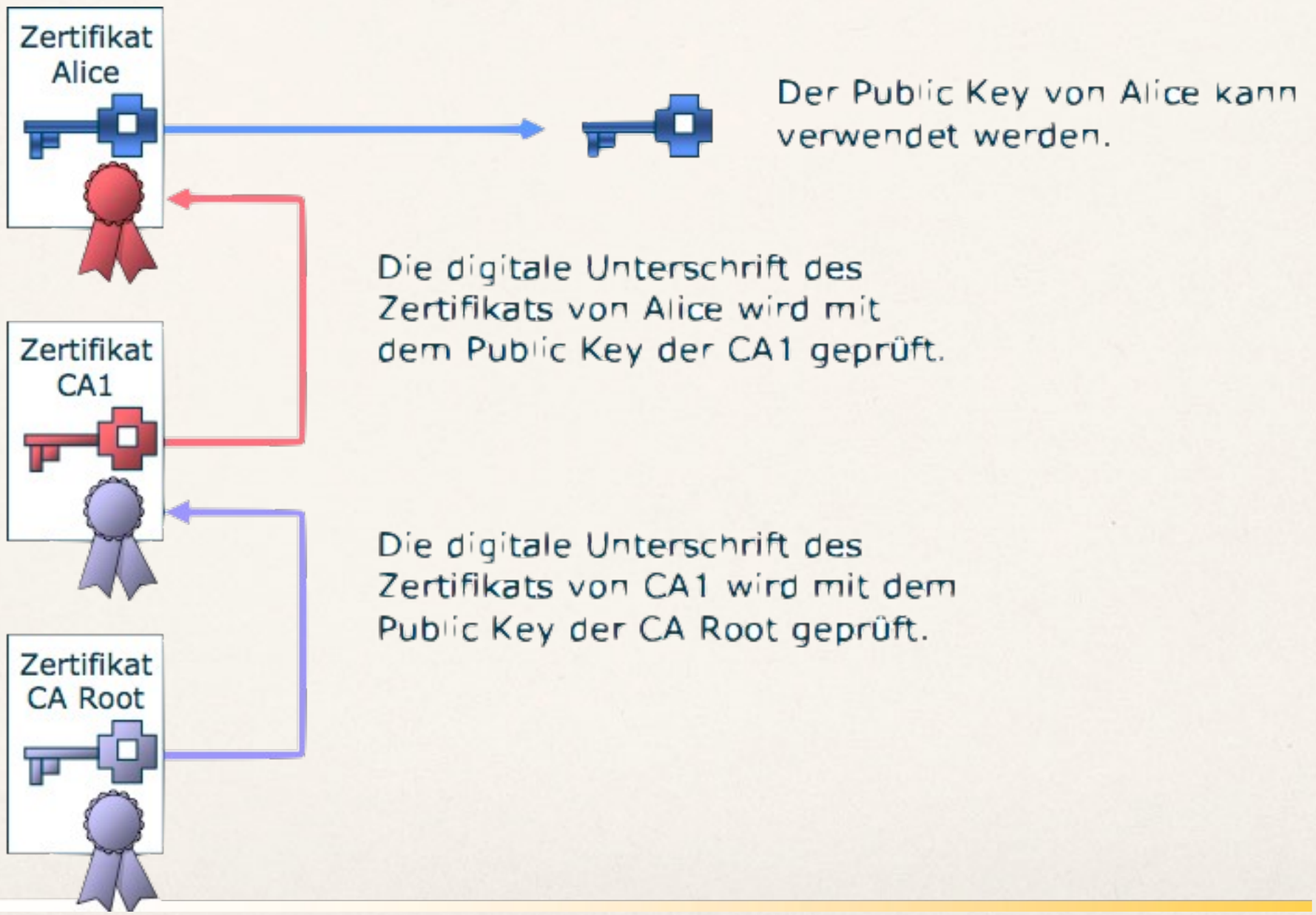
Digitale Zertifikate

- **Beispiel:** Zertifikatsprüfung anhand einer zweistufigen *CA*-Hierarchie



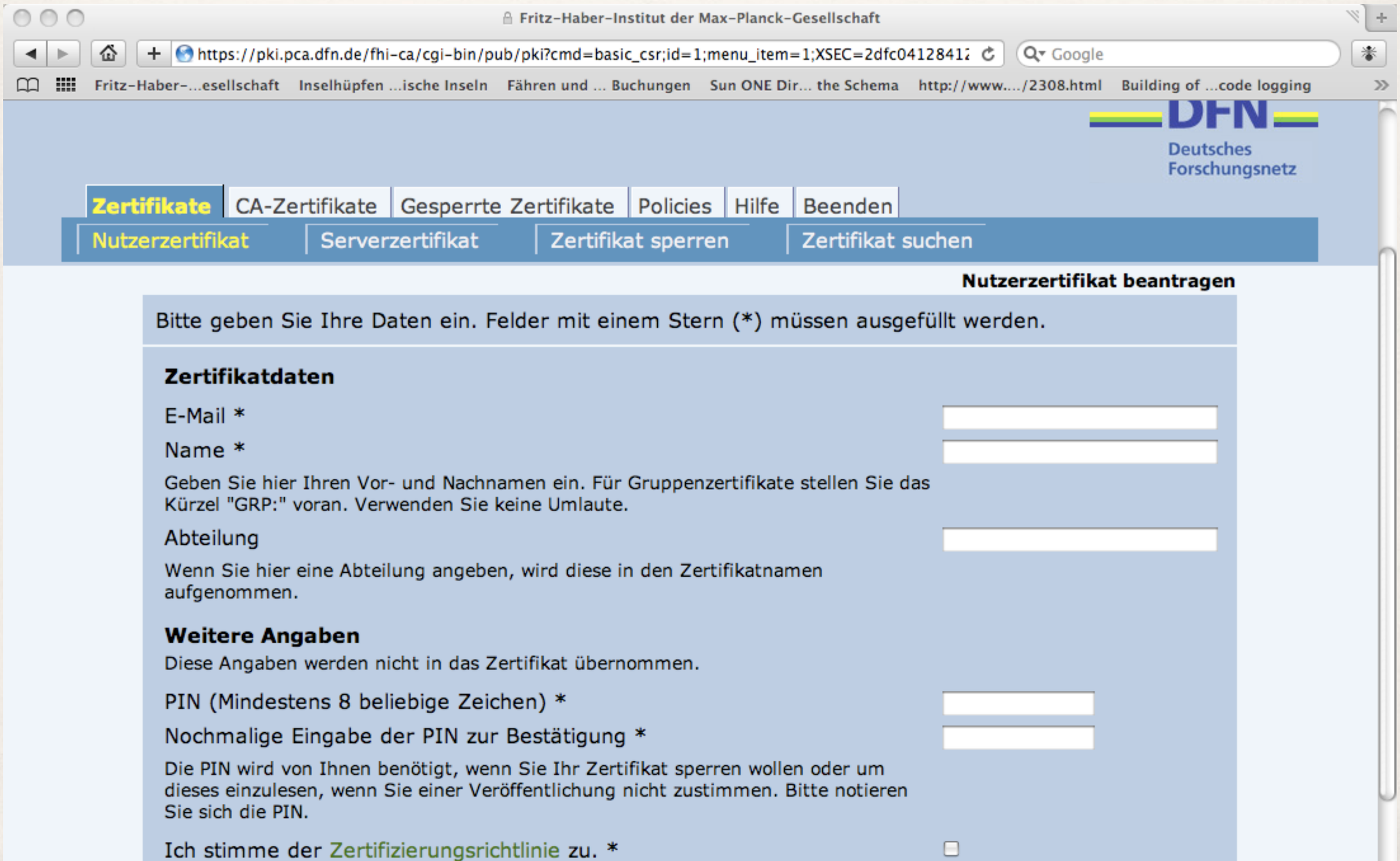
Digitale Zertifikate

- **Beispiel:** Zertifikatsprüfung anhand einer zweistufigen *CA*-Hierarchie



Digitale Zertifikate

- **Beispiel:** FHI-*CA* (*https://pki.pca.dfn.de/fhi-ca/cgi-bin/pub/pki*)



Zum Nachlesen

- *Der kleine Fermat und die Schlüssel*
  - http://www.linslernet.de/crypt.htm
- Cryptool
- http://www.cryptool-online.org/index.php?lang=de