

Mehr Sicherheit durch PKI-Technologie

Verschlüsselung allgemein

- Die 4 wichtigsten Bedingungen
 - 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.

Verschlüsselung allgemein

- **Authentifizierung**
 - Der Absender ist derjenige, der er vorgibt zu sein.
- **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 Protokoll
 - Digitale Unterschriften
 - Elektronische Signatur

Grundlegende Verschlüsselungsarten

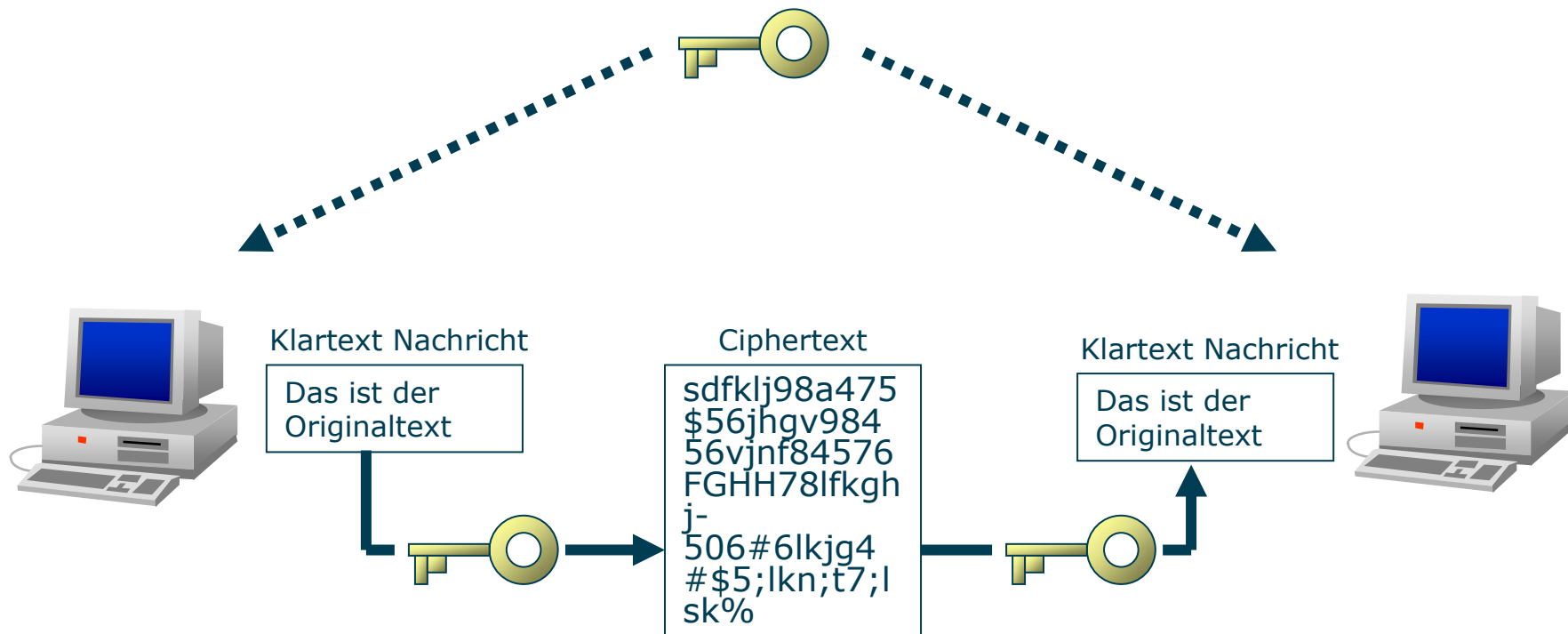
- Grundlegende Verschlüsselungsarten sind:
 - Symmetrische Verschlüsselung
 - Asymmetrische Verschlüsselung
 - Einweg-Verschlüsselungsfunktion (Hash)

Grundlegende Verschlüsselungsarten

- Symmetrische Verschlüsselung
 - Ein geheimer Schlüssel (Shared Secret Key) wird für die Ver- und Entschlüsselung benutzt.
- Vorteil
 - Sehr schnelle Verschlüsselung
 - Dadurch wird **Vertraulichkeit** erreicht
- Nachteil
 - Die Schlüssel müssen unbedingt sicher und geheim aufbewahrt und regelmäßig geändert werden.

Grundlegende Verschlüsselungsarten

- Symmetrische Verschlüsselung



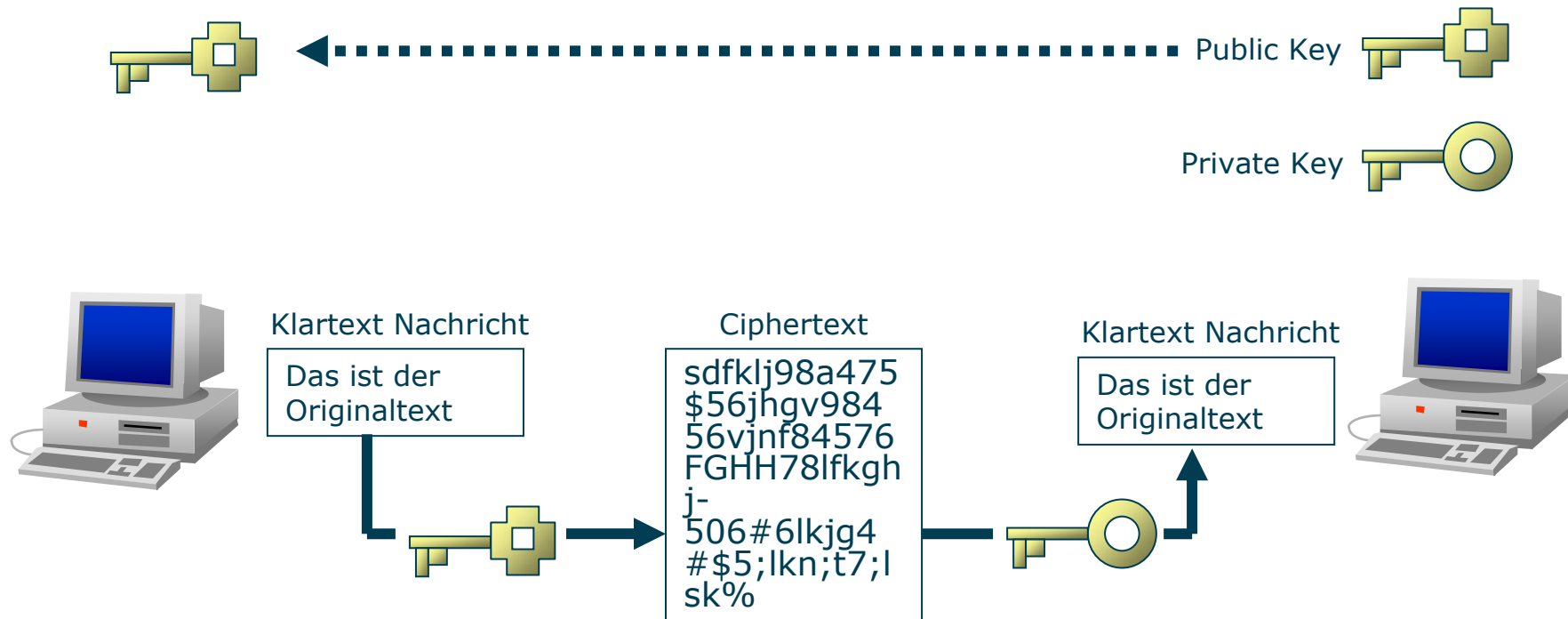
Grundlegende Verschlüsselungsarten

- Asymmetrische Verschlüsselung
 - Es werden zwei separate Schlüssel (Private/Public) für die Ver- und Entschlüsselung benutzt.
- Vorteil
 - Die Public Keys können 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

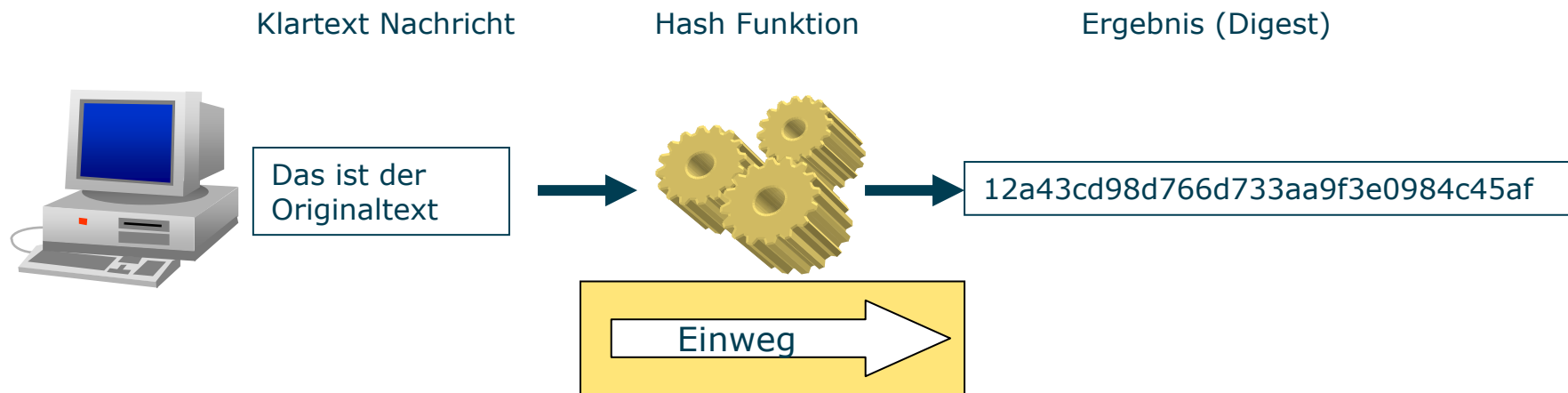
- **Einweg Hash Funktion**

- Die Einweg Hash 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 außerdem bei der digitalen Unterschrift mitverwendet.
- Dadurch wird **Integrität** erreicht.

Grundlegende Verschlüsselungsarten

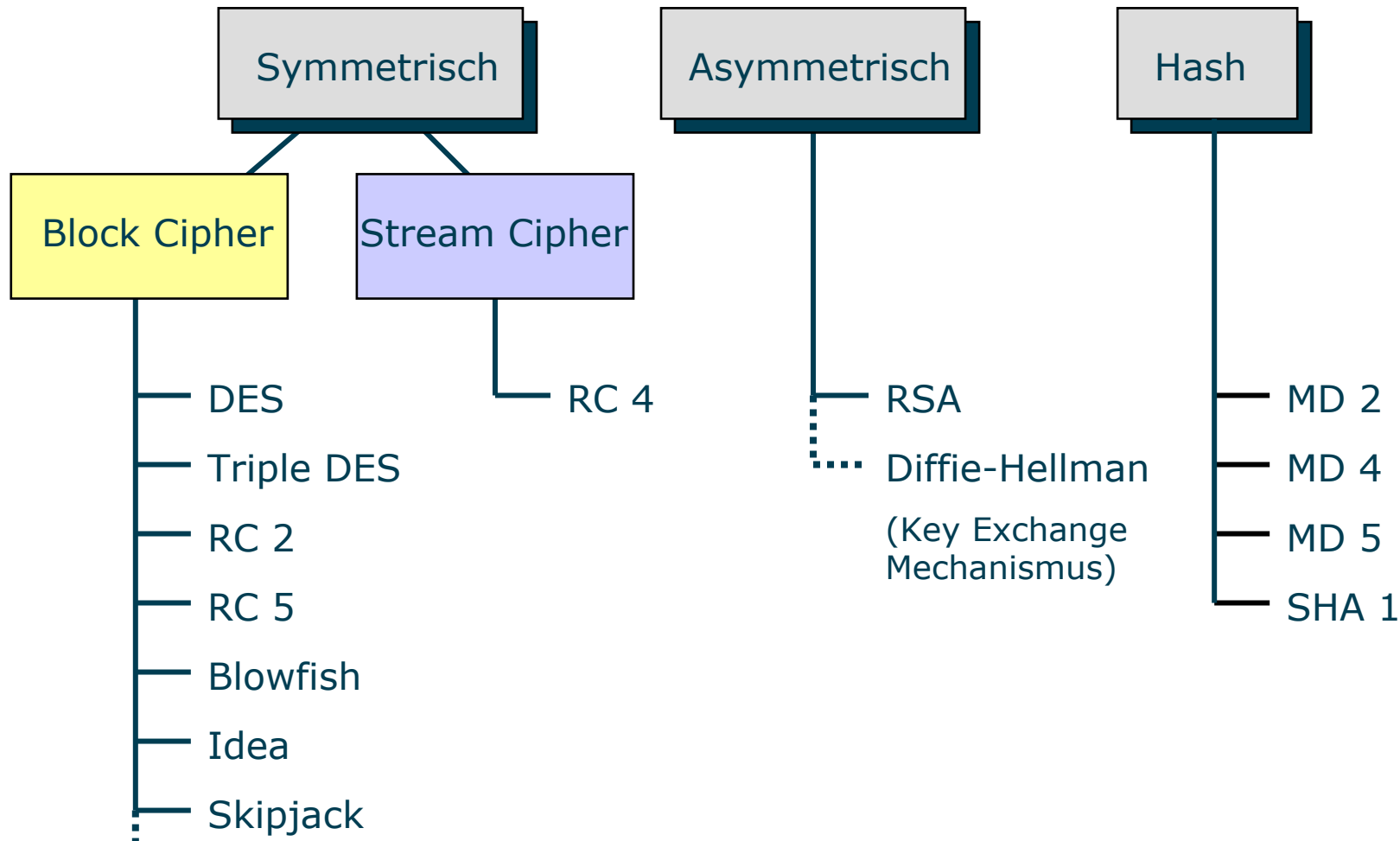


- **Einweg Hash Funktion**



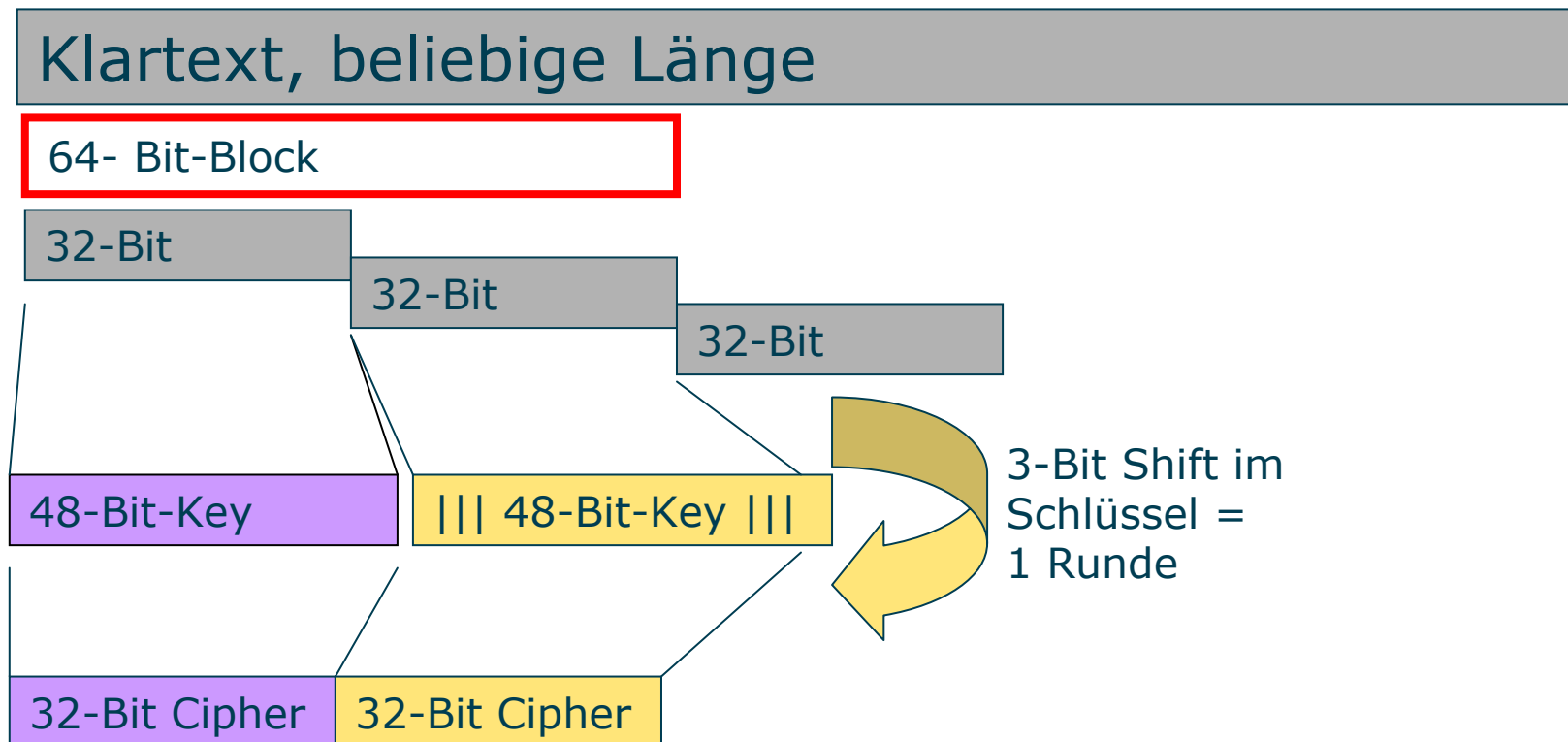
Grundlegende Verschlüsselungsarten

- Algorithmen



Grundlegende Verschlüsselungsarten **NTC**

- Algorithmen: Beispiel DES
 - 64-Bit Block Cipher, 48-Bit Schlüssel, 16 Runden



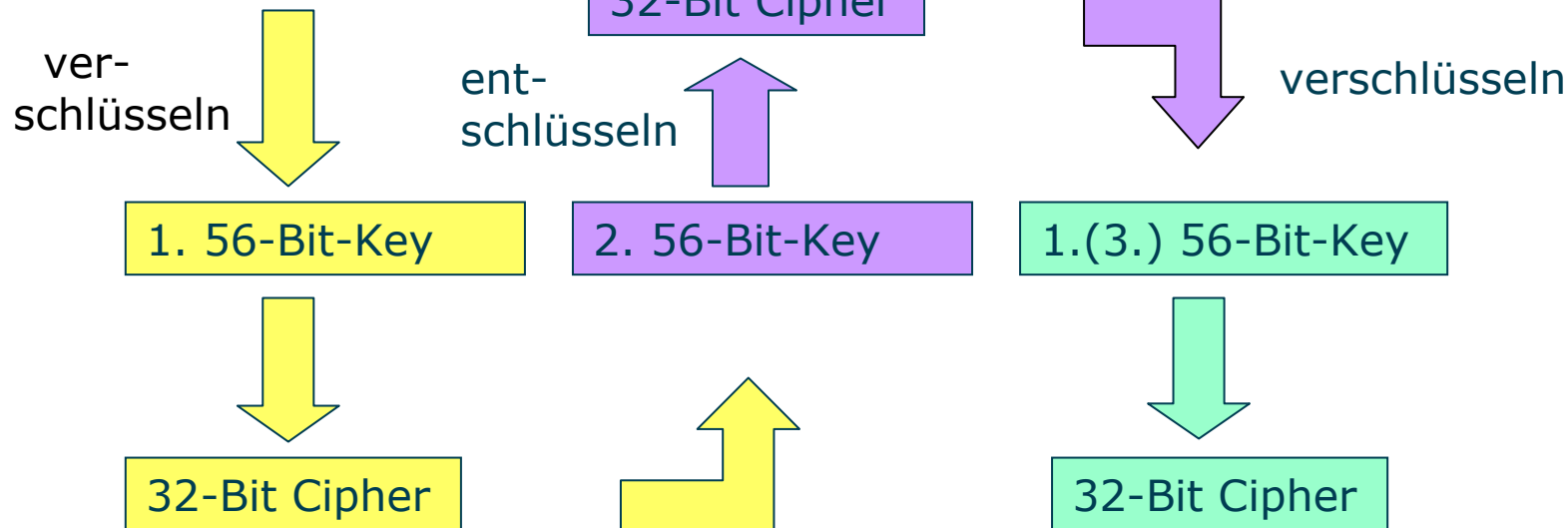
Grundlegende Verschlüsselungsarten **NTC**

- Algorithmen: Beispiel Triple DES
 - 64-Bit Block Cipher, 56-Bit Schlüssel, 2 [3] Schlüssel

Klartext, beliebige Länge

64- Bit-Block

32-Bit



Grundlegende Verschlüsselungsarten

- Standardimplementationen verschiedener Block Cipher Algorithmen

Cipher	Blocklänge	Schlüssellänge	Runden
DES	64	48	16
Triple DES	64	112 (168)	
RC2	64	variabel	12 bis 16
RC5	64	variabel	12 bis 16
Blowfish	variabel	max. 448	variabel
IDEA	variabel	128	variabel
Skipjack	variabel	80	variabel

Grundlegende Verschlüsselungsarten

- Standardimplementierungen von RSA, DH, Hash

Asymmetrisch	Schlüssellänge
RSA	512 - 2048
Key Management System	Schlüssellänge
Diffie Hellman Group I	512
Diffie Hellman Group II	1024
Diffie Hellman Group III	1536
Hash	Hashlänge
MD2	128
MD4	128
MD5	128
SHA-1	160

Verschlüsselungsarten angewandt



- Digitale Unterschrift
 - Die 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 ein Hash-Digest.
 - Er entschlüsselt das erhaltene Digest mit dem Public Key des Partners.
 - Er vergleicht die zwei Digest, bei Übereinstimmung ist der Sender verifiziert.

Verschlüsselungsarten angewandt

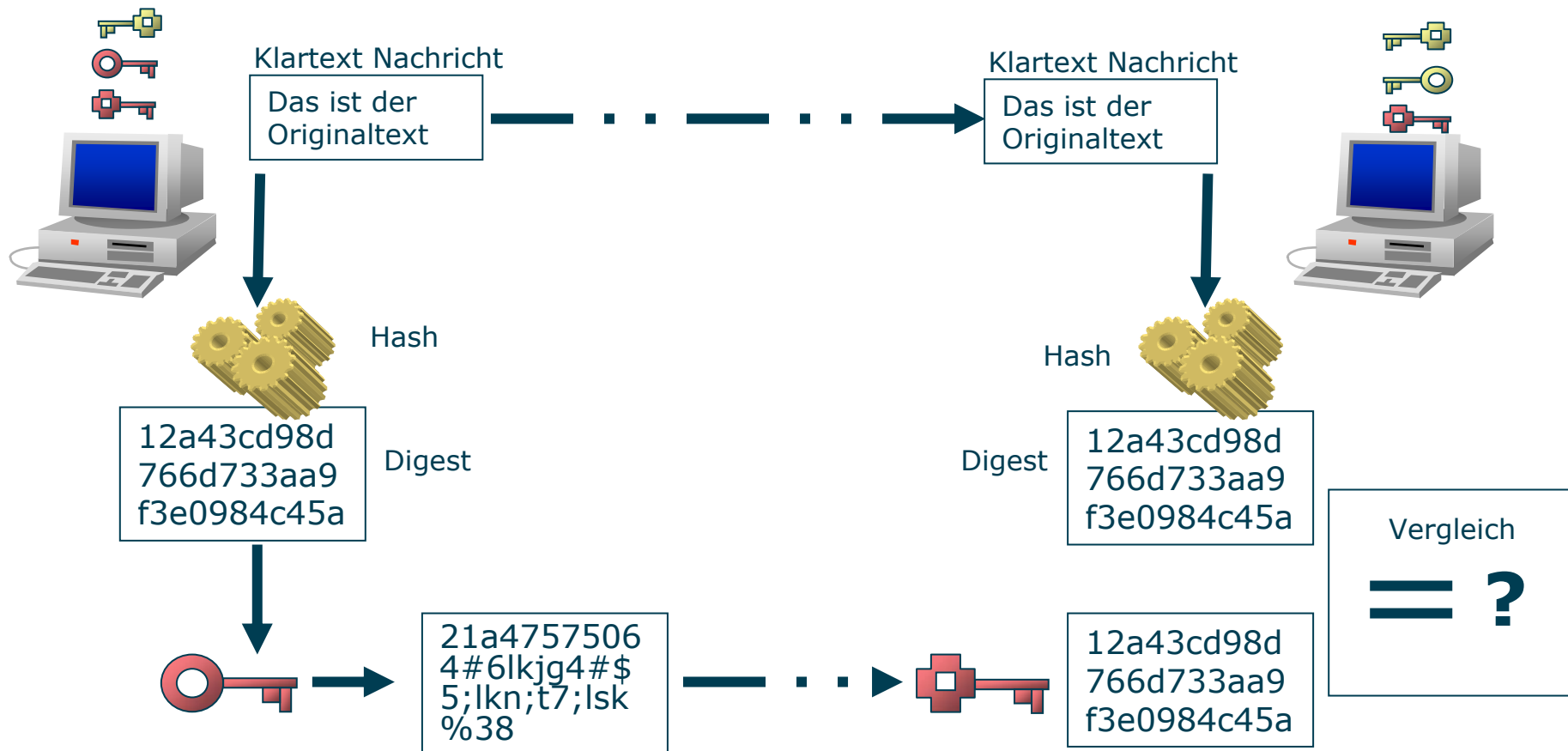


- Digitale Unterschrift
 - Voraussetzung ist, dass die Partner im Besitz des jeweiligen Public Keys des Partners sind.



Verschlüsselungsarten angewandt

- Digitale Unterschrift



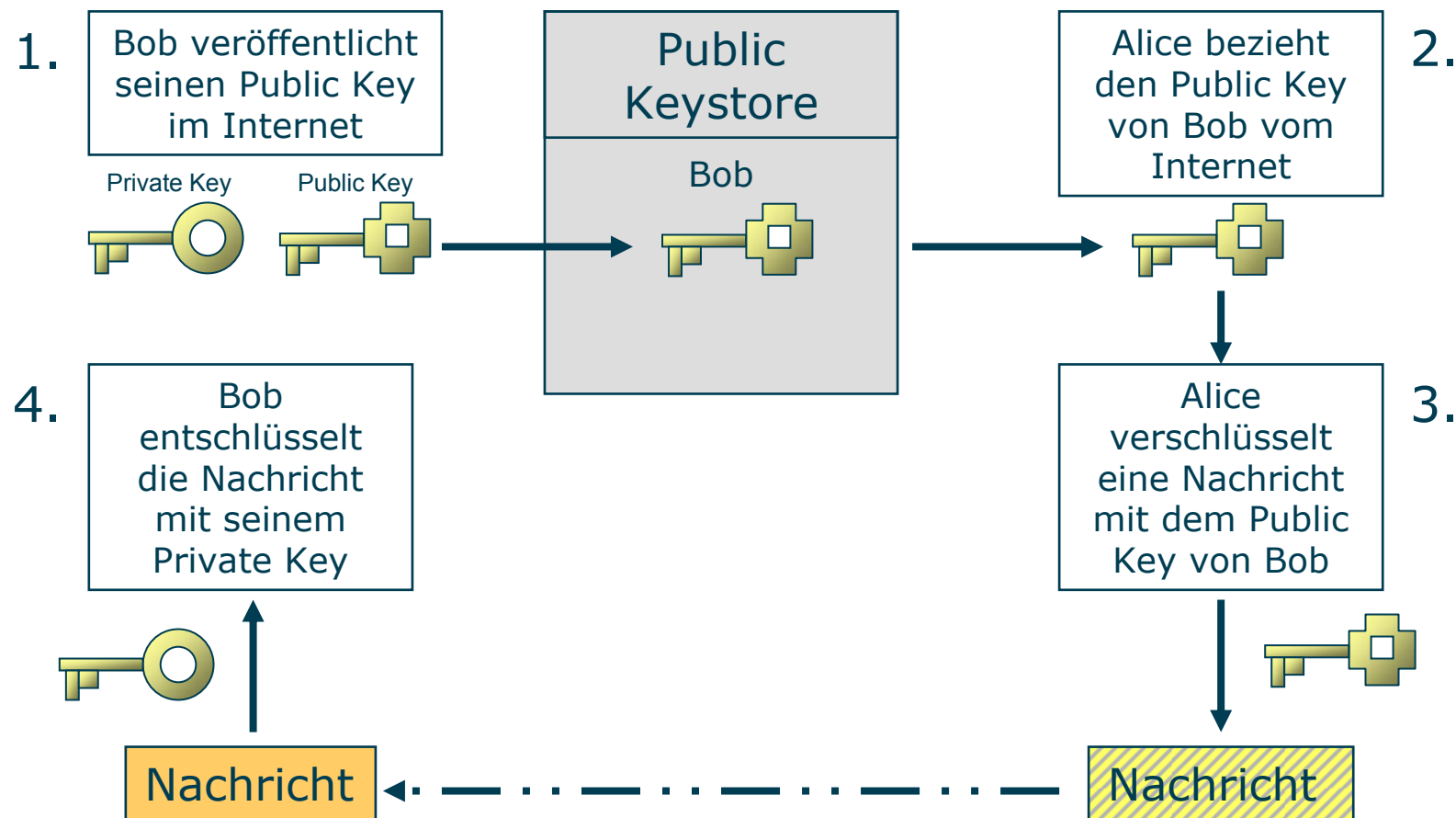
Verschlüsselungsarten angewandt



- 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.

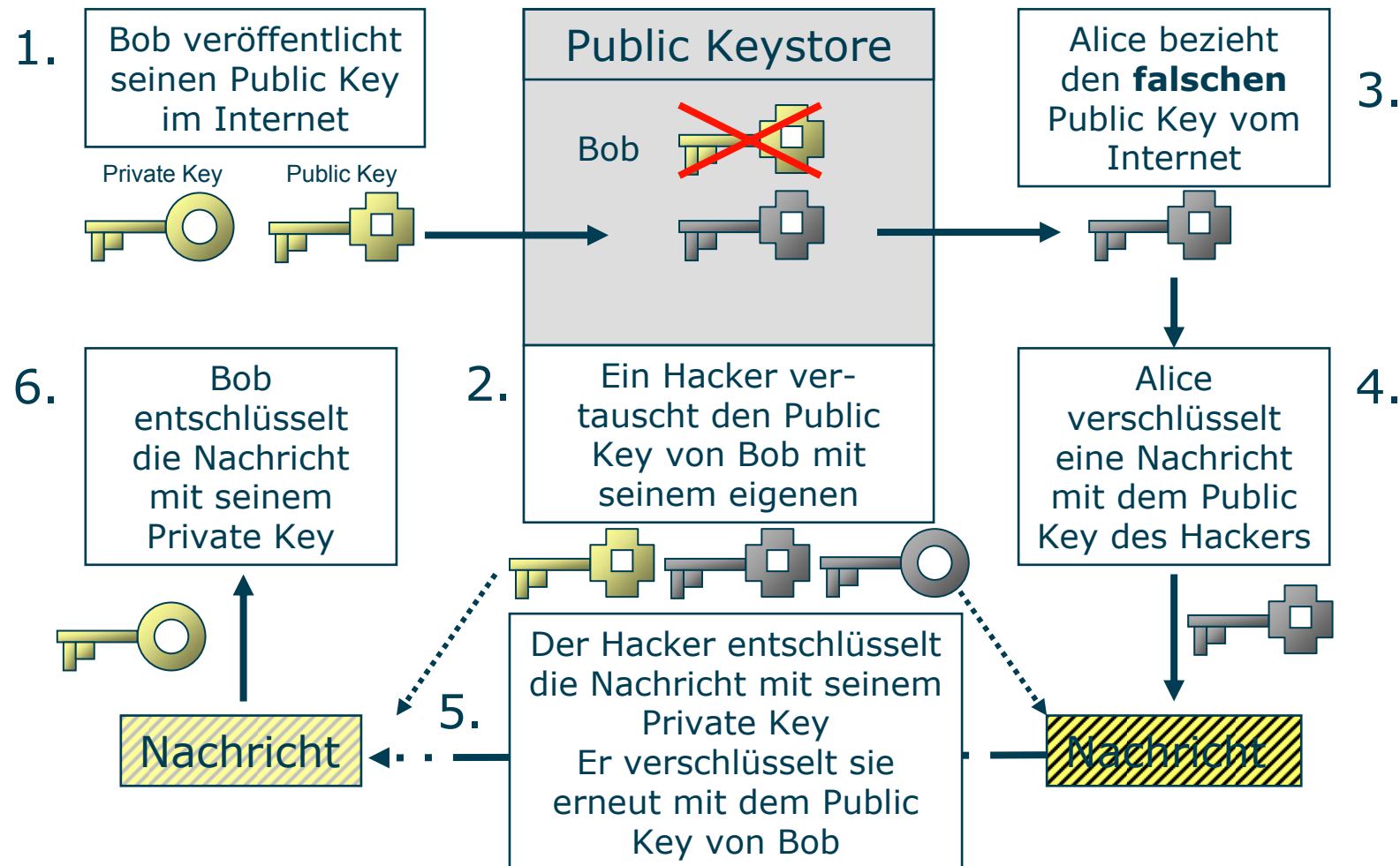
Verschlüsselungsarten angewandt

- Beispiel: Alice sendet Bob eine verschlüsselte Nachricht.



Verschlüsselungsarten angewandt

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



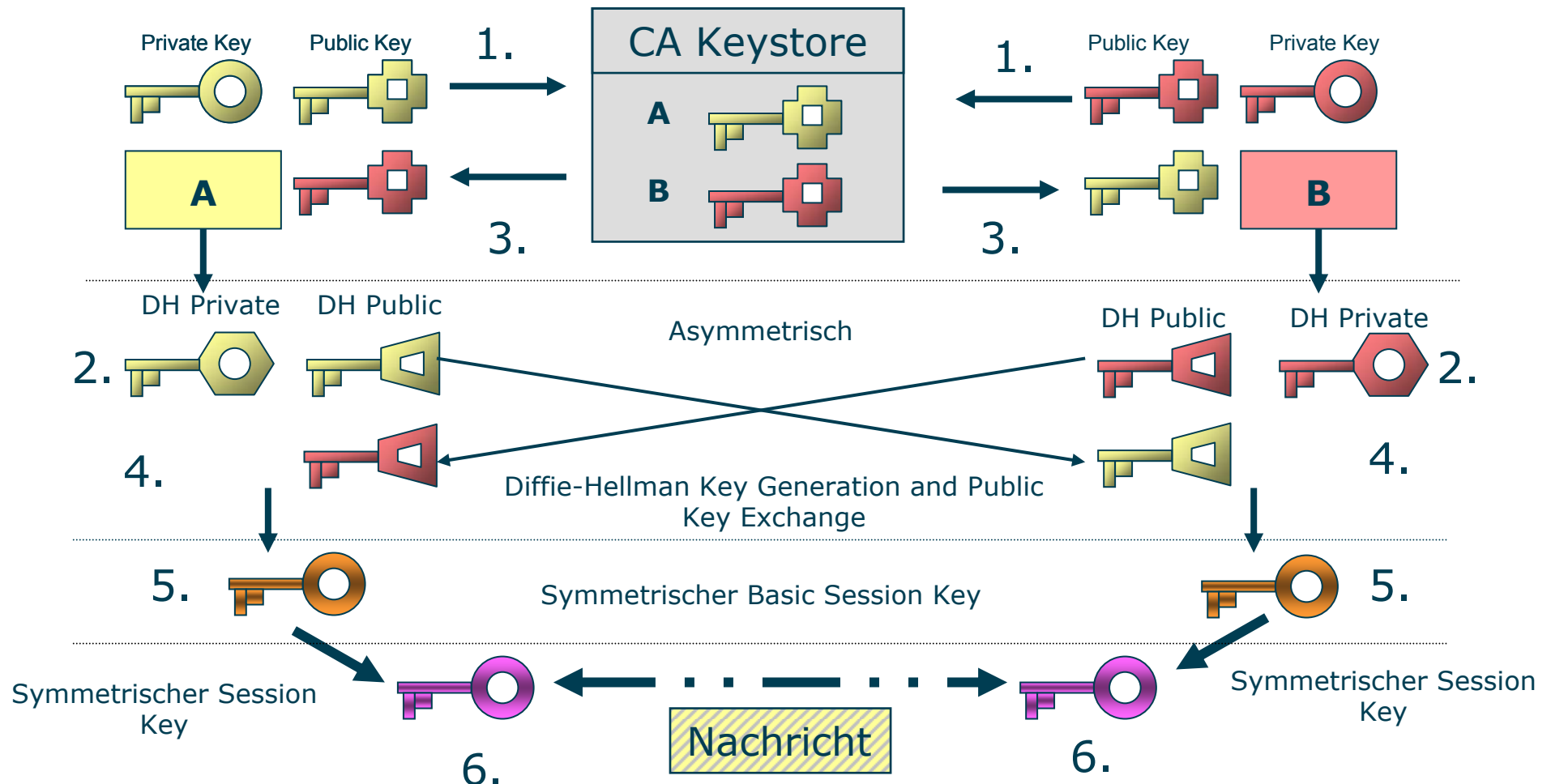
Verschlüsselungsarten angewandt



- 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 nach Diffie-Hellman

Verschlüsselungsarten angewandt

- Schlüsselaustauschverfahren nach Diffie-Hellman



Verschlüsselungsarten angewandt



- Schlüsselaustauschverfahren nach Diffie-Hellman
 - Ablauf
 - 1. 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.
 - 2. Diffie-Hellman Key Generation
 - Das Diffie-Hellman-Key-Pair wird gebildet.
 - 3. 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.
 - 4. Diffie-Hellman Public Key Austausch
 - Die DH-Public Keys werden zwischen den Partnern getauscht.

Verschlüsselungsarten angewandt



- Sicheres Schlüsselaustauschverfahren nach Diffie-Hellman
 - Ablauf
 - 5. Basic Session Key
 - Mittels der getauschten Diffie-Hellmann-Public Keys wird ein symmetrischer Schlüssel, der Basic Session Key, berechnet.
 - 6. 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-Hellman
 - Da sich die Diffie-Hellman 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.

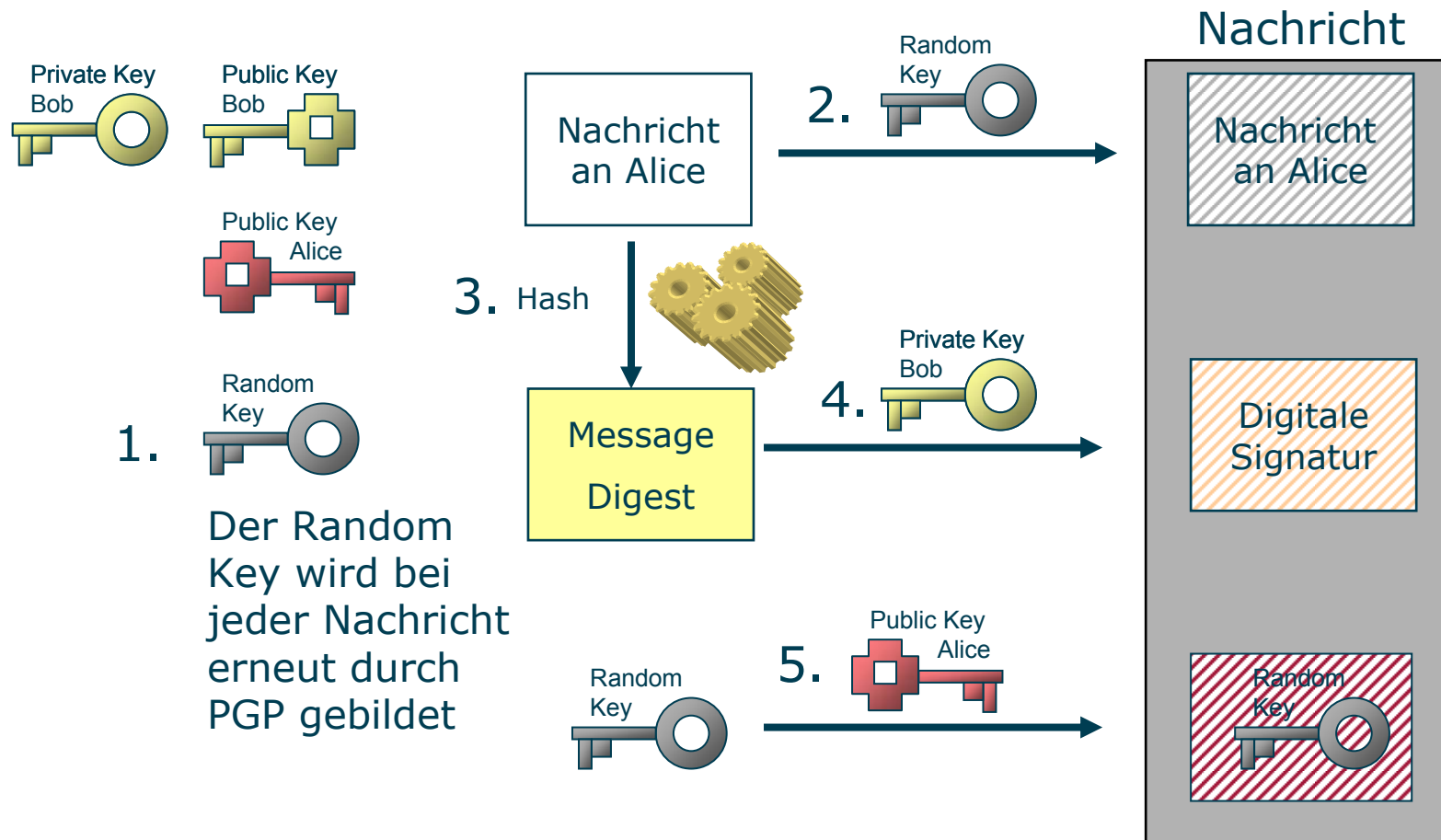
Kombinierte Verschlüsselungsverfahren



- 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 von seinem PC eine verschlüsselte Nachricht mittels PGP an Alice.



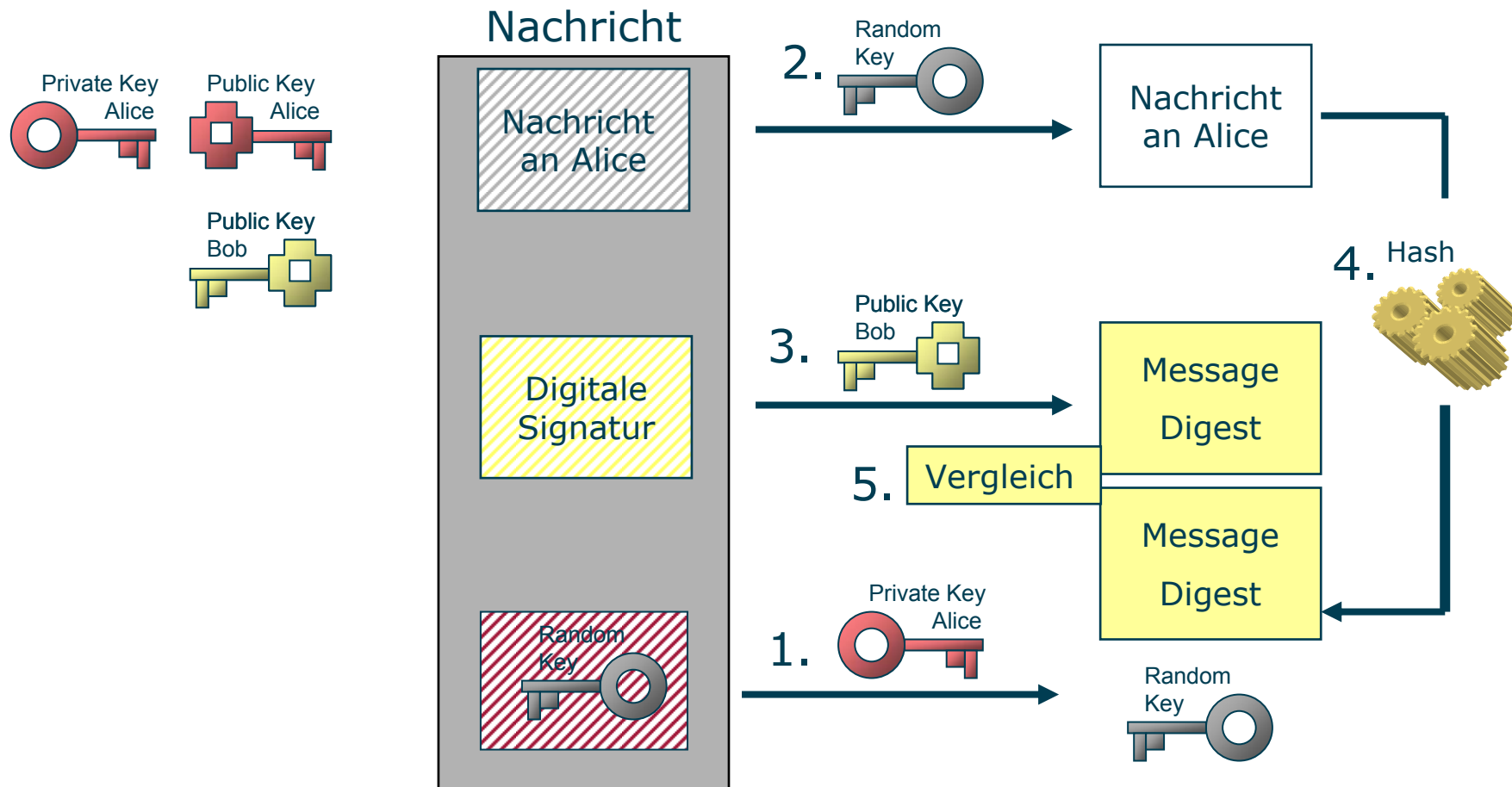
Kombinierte Verschlüsselungsverfahren



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

Kombinierte Verschlüsselungsverfahren

- Alice empfängt eine verschlüsselte Nachricht von Bob und entschlüsselt diese.



Kombinierte Verschlüsselungsverfahren



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

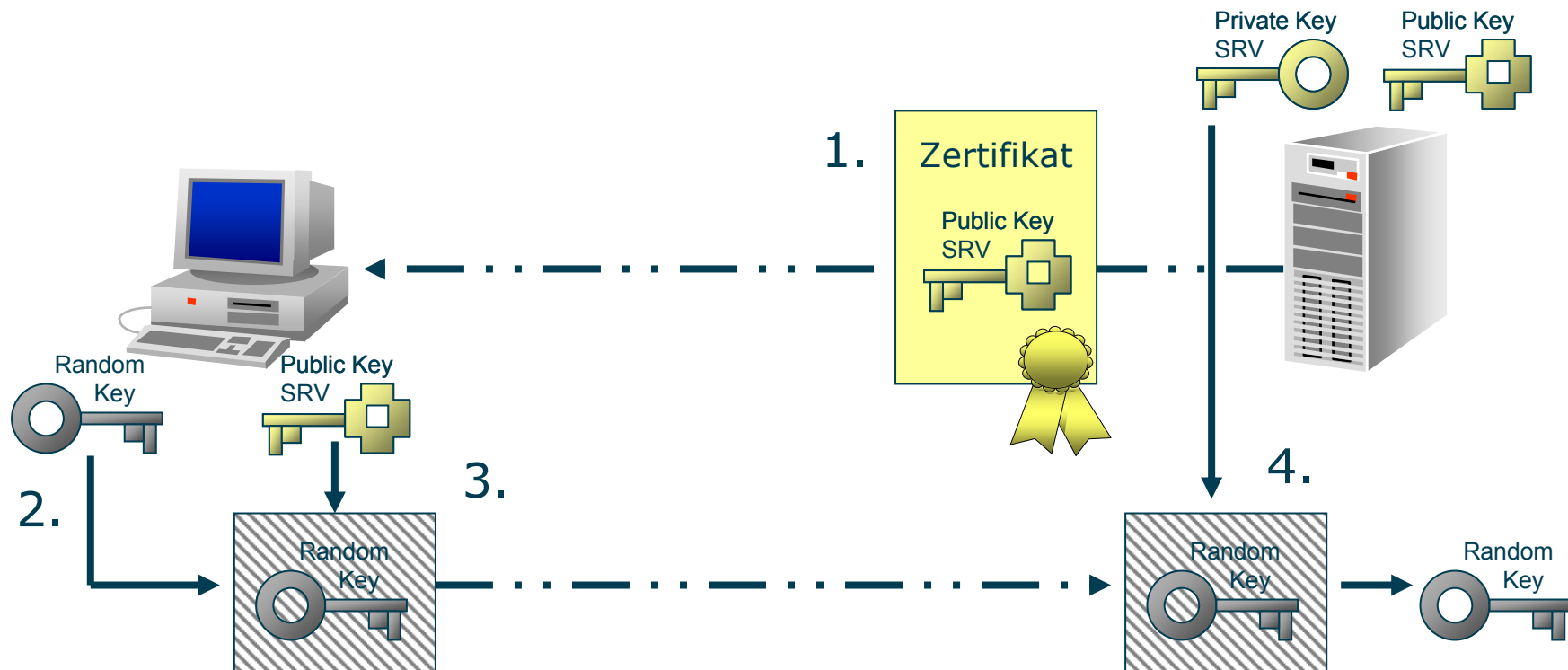
Kombinierte Verschlüsselungsverfahren



- Secure Sockets Layer (SSL)
 - 1995 durch Netscape entwickelt, hat sich gegen S-HTTP durchgesetzt.
 - Nicht protokollgebunden (HTTP, SMTP, NNTP, Telnet, FTP Implementationen)
 - Verwendet Port 443 mit HTTPS, Port 465 mit SSMTP, Port 563 mit SNNTP
 - 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-HTTP oder SSL
 - Ablauf
 - 1. Der Server sendet sein Zertifikat an den Client.
 - 2. Der Client bildet einen zufälligen, eindeutigen Schlüssel (Random Key).
 - 3. Der Client verschlüsselt den zufälligen Schlüssel mit dem öffentlichen Schlüssel (Public Key) des Servers aus dem Zertifikat.
 - 4. Der Client überträgt den Schlüssel zum Server.
 - 5. 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-Repudiation**
- Um diese Forderungen zu erfüllen werden digitale Zertifikate benötigt.

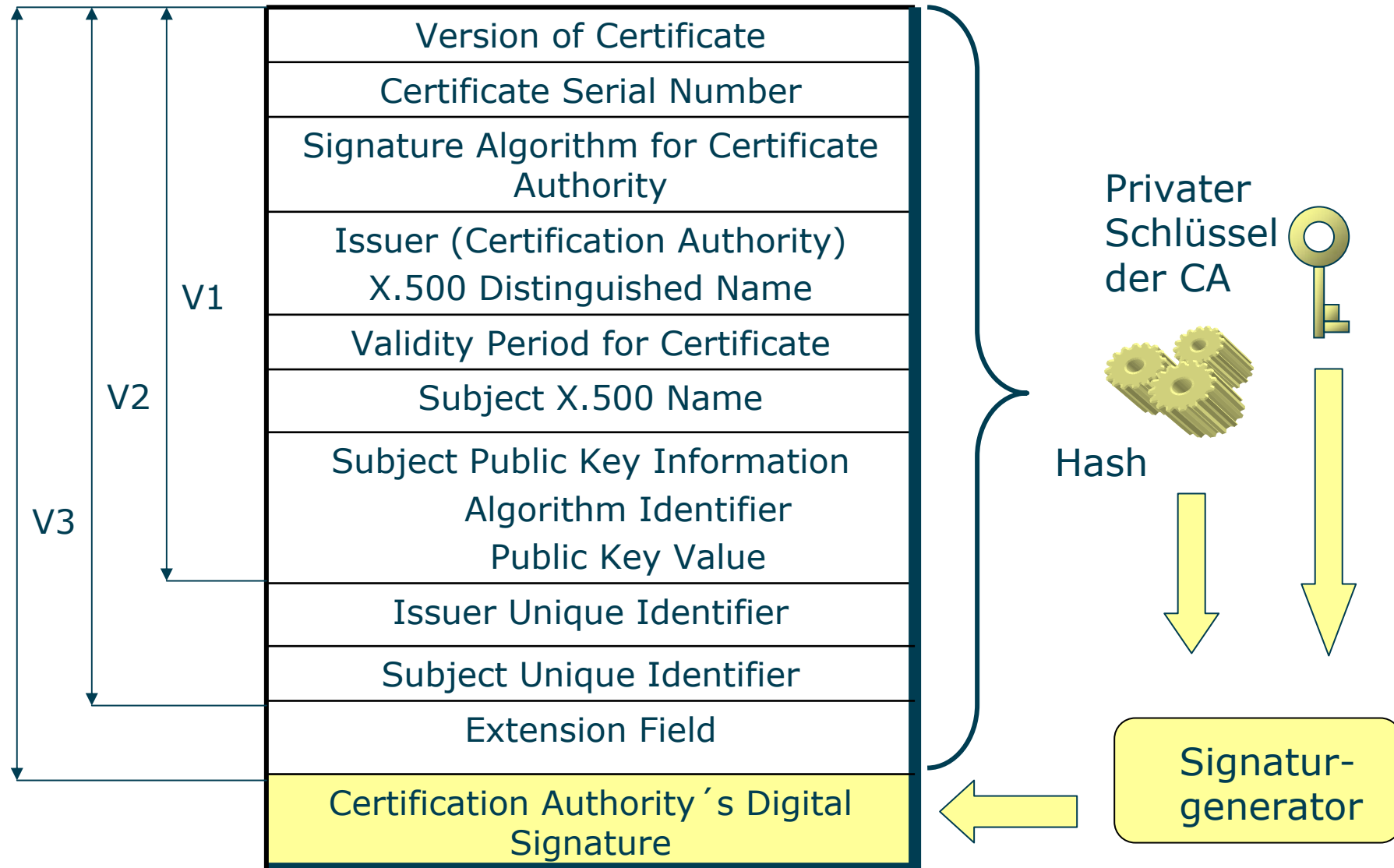
Digitale Zertifikate

- Warum Digitale Zertifikate?
 - Asymmetrische Schlüssel ermöglichen eine sichere Kommunikation mittels verteiltem Public Key.
 - Es könnten aber auch falsche Schlüssel verbreitet werden.
 - Deshalb muss die Echtheit eines öffentlichen Schlüssels (Public Key) bestätigt werden.
 - Die „Digitalen Zertifikate“ enthalten Public Keys, 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:
 - VeriSign (www.verisign.com)
 - D-Trust GmbH (www.d-trust.net)
 - TimeSafe TrustCenter (www.timesafe.de)
 - TC TrustCenter (www.trustcenter.de)
 - Ein Trust Center kann aber auch ein Zertifikatsserver innerhalb eines Unternehmens sein.
 - Ein Trust Center muss auf alle Fälle vertrauenswürdig sein!

Beispiel: Das Zertifikat nach X.509



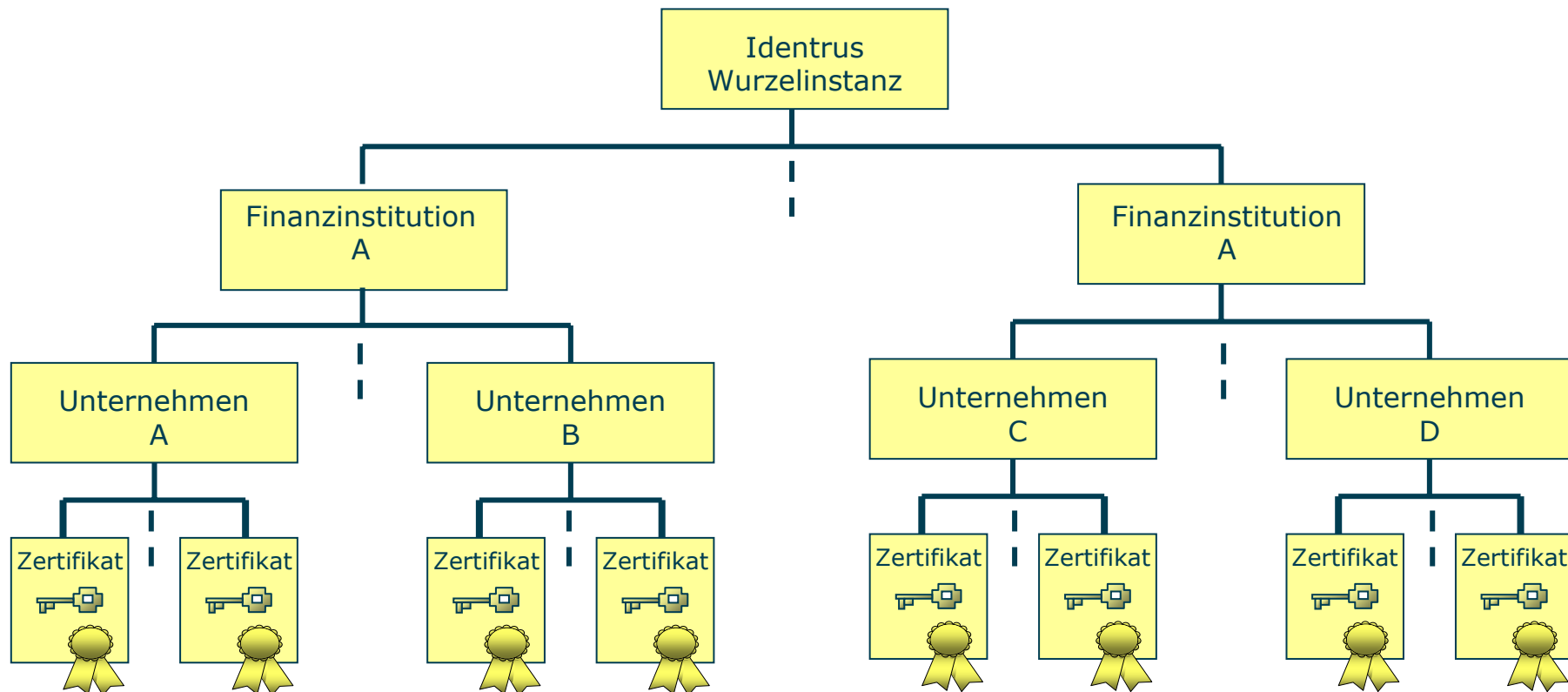
Digitale Zertifikate



- Trust Center
 - Da verschiedene Firmen oder Privatpersonen Mitglied bei verschiedenen Trust Centern sein können, muss eine Verbindung zwischen den Trustcentern bestehen.
 - Die Trust Center haben sich z. T. hierarchisch organisiert.
 - Das oberste Trustcenter ist das Root-Trust Center oder die Root-Certification Authority (CA root).
 - Verschiedene Branchen wie Banken, Rechtsanwälte unterhalten eigene Trust Center-Hierarchien.

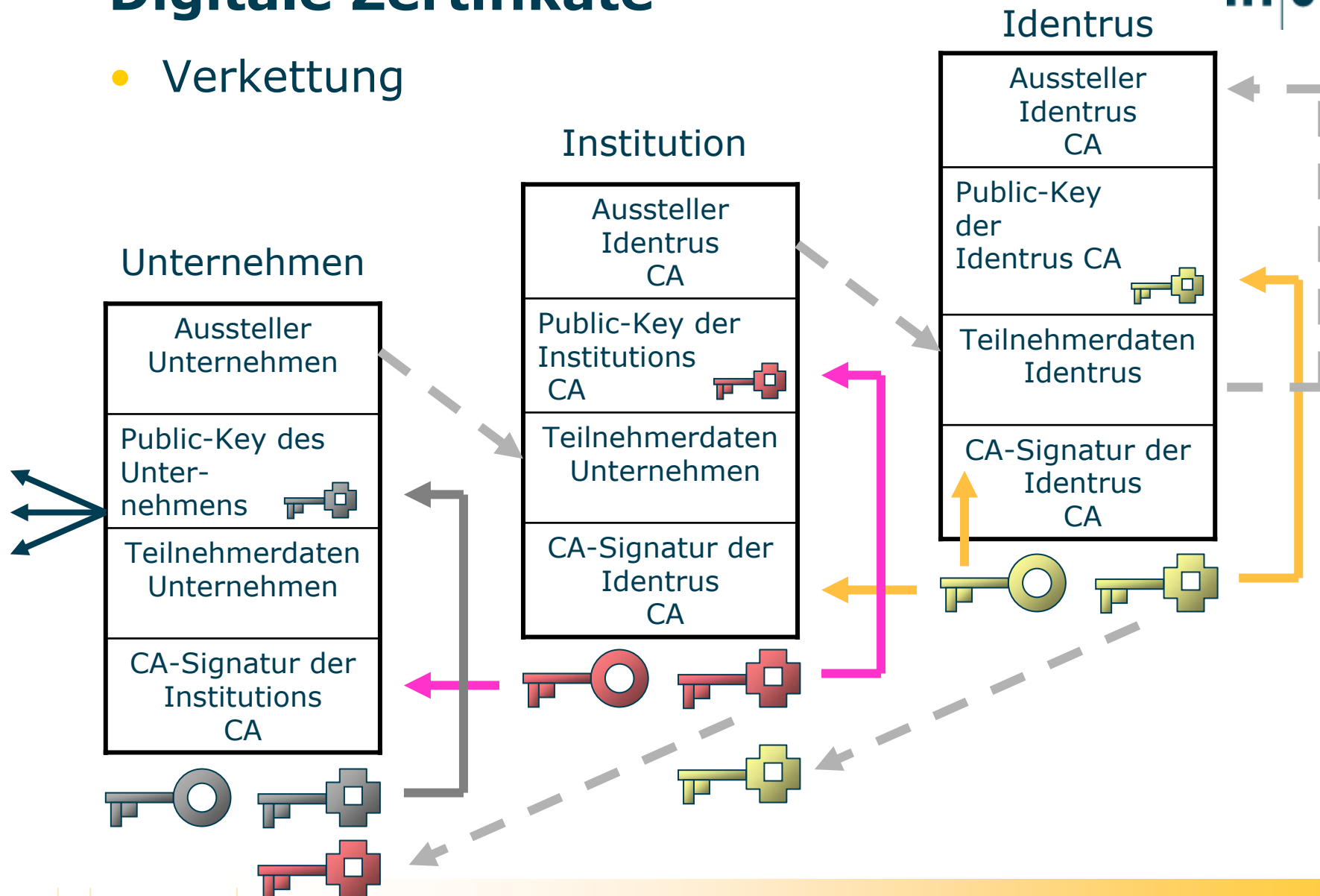
Digitale Zertifikate

- Beispiel: Zertifizierungshierarchie anhand des vierstufigen Identrus-Vertrauensmodell für Finanzinstitute



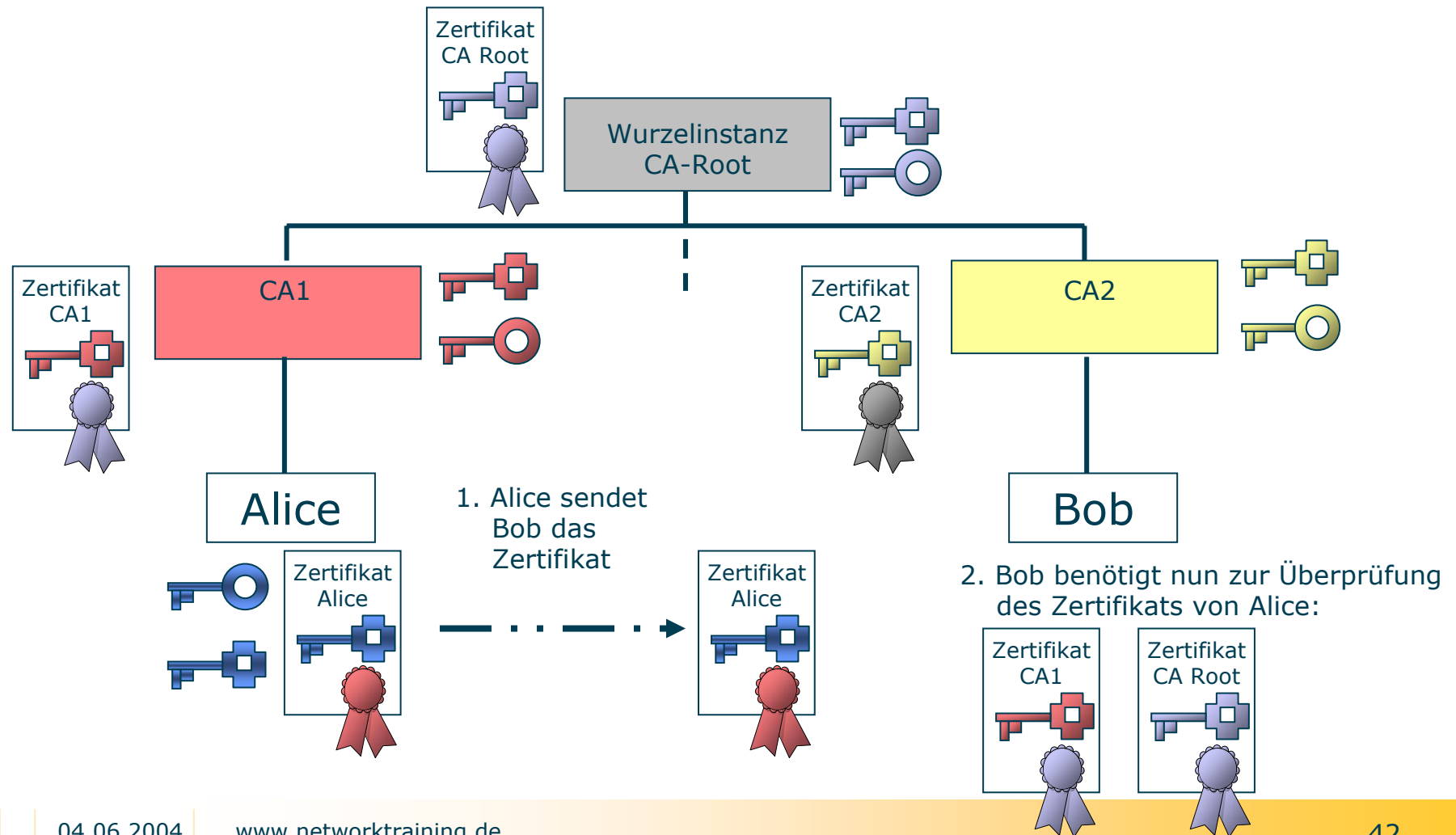
Digitale Zertifikate

- Verkettung



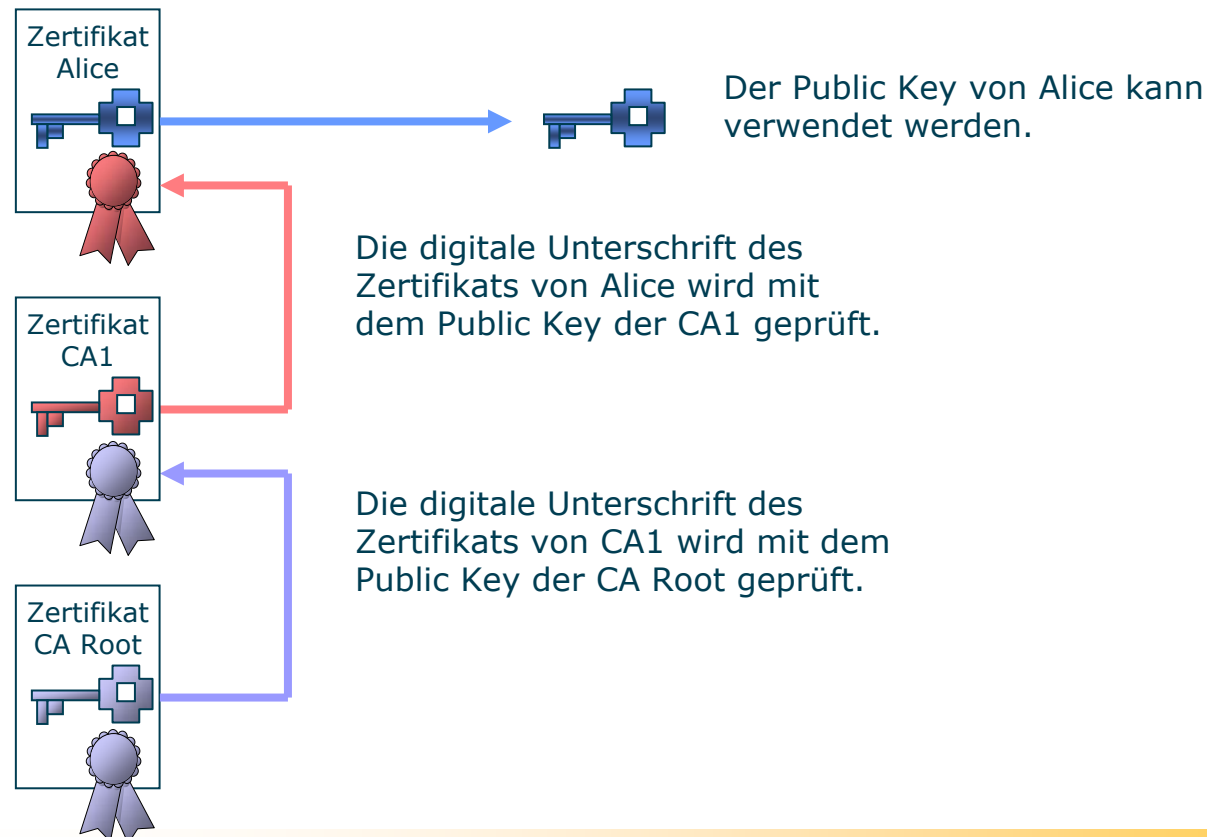
Digitale Zertifikate

- Beispiel einer Zertifikatsprüfung anhand einer zweistufigen CA-Hierarchie



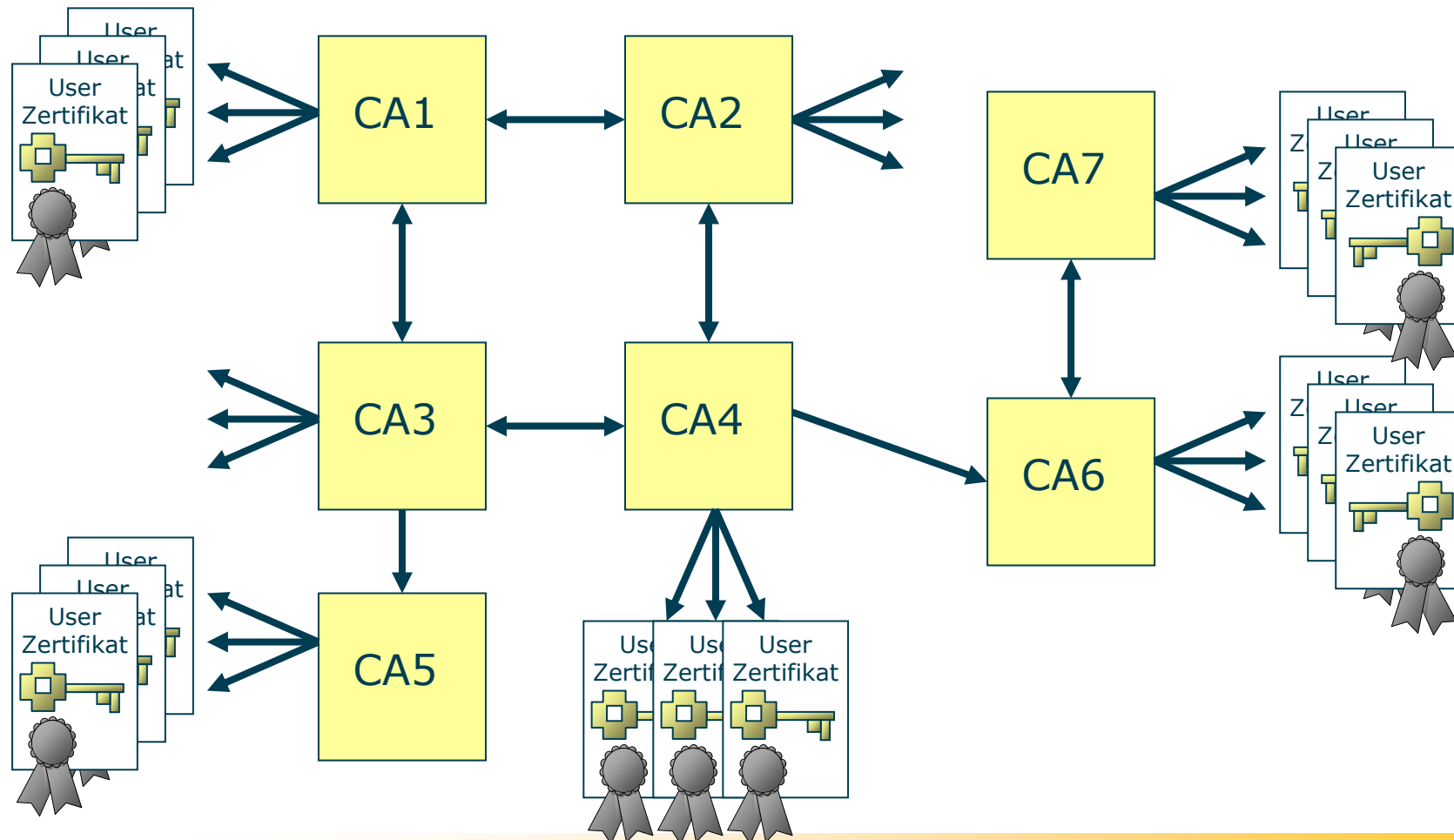
Digitale Zertifikate

- Beispiel einer Zertifikatsprüfung anhand einer zweistufigen CA-Hierarchie



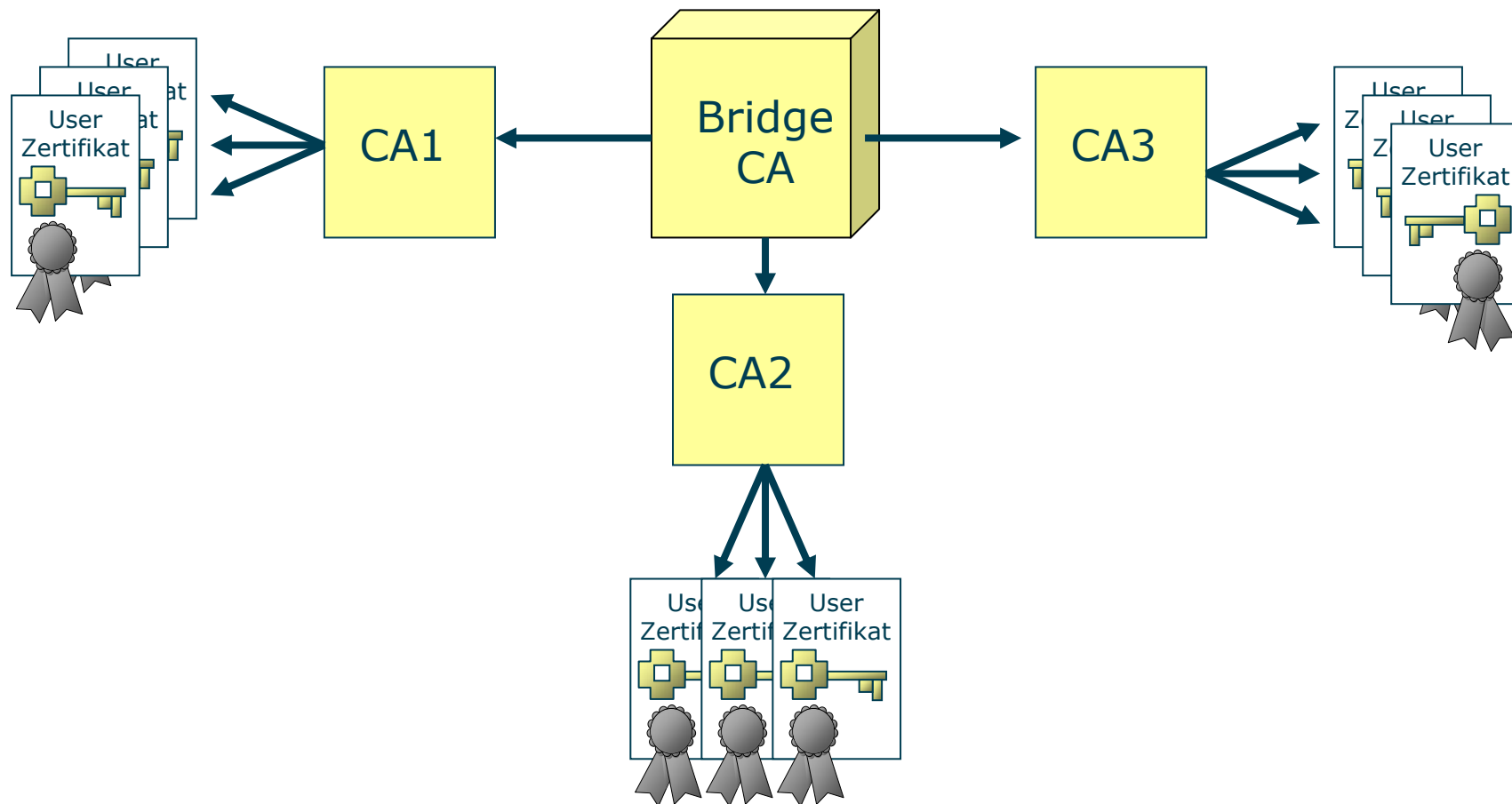
Digitale Zertifikate

- Hybrides Vertrauensmodell (ISO Banking)



Digitale Zertifikate

- Bridge Vertrauensmodell



Verschlüsselung und E-Commerce



- Elektronische Zahlungsmittel
 - E-Cash
 - Das Geld wird z.B. auf einem vertrauten Konto der Bank angelegt.
 - Danach werden elektronische Token an den Computer des Benutzers angeliefert und können abgebucht werden.
 - Dieses Zahlungsmittel ist einfach zu verstehen, aber schwierig zu implementieren.
 - Die Zahlung findet sofort statt.
 - Einige Banken bieten E-Cash an.
 - E-Schecks
 - Funktionieren ähnlich wie E-Cash aber die Zahlung findet nicht sofort statt (wie herkömmliche Schecks zu sehen)

Verschlüsselung und E-Commerce



- Elektronische Zahlungsmittel
 - Kreditkarten
 - Kreditkarten sind das meist benutzte Zahlungsmittel für Verbrauchertransaktionen.
 - Die Infrastruktur existiert schon seit Jahren.
 - Allerdings befürchtet der Verbraucher den Missbrauch seiner Karte.
 - EDI
 - EDI ist eine Standardisierung von elektronischen Formularen und Verfahren um die Automatisierung von Zahlungen zu ermöglichen (ANSI X12).
 - Vorteile:
 - Weniger Datenerfassung
 - Weniger Fehler
 - Kostensparend

Verschlüsselung und E-Commerce



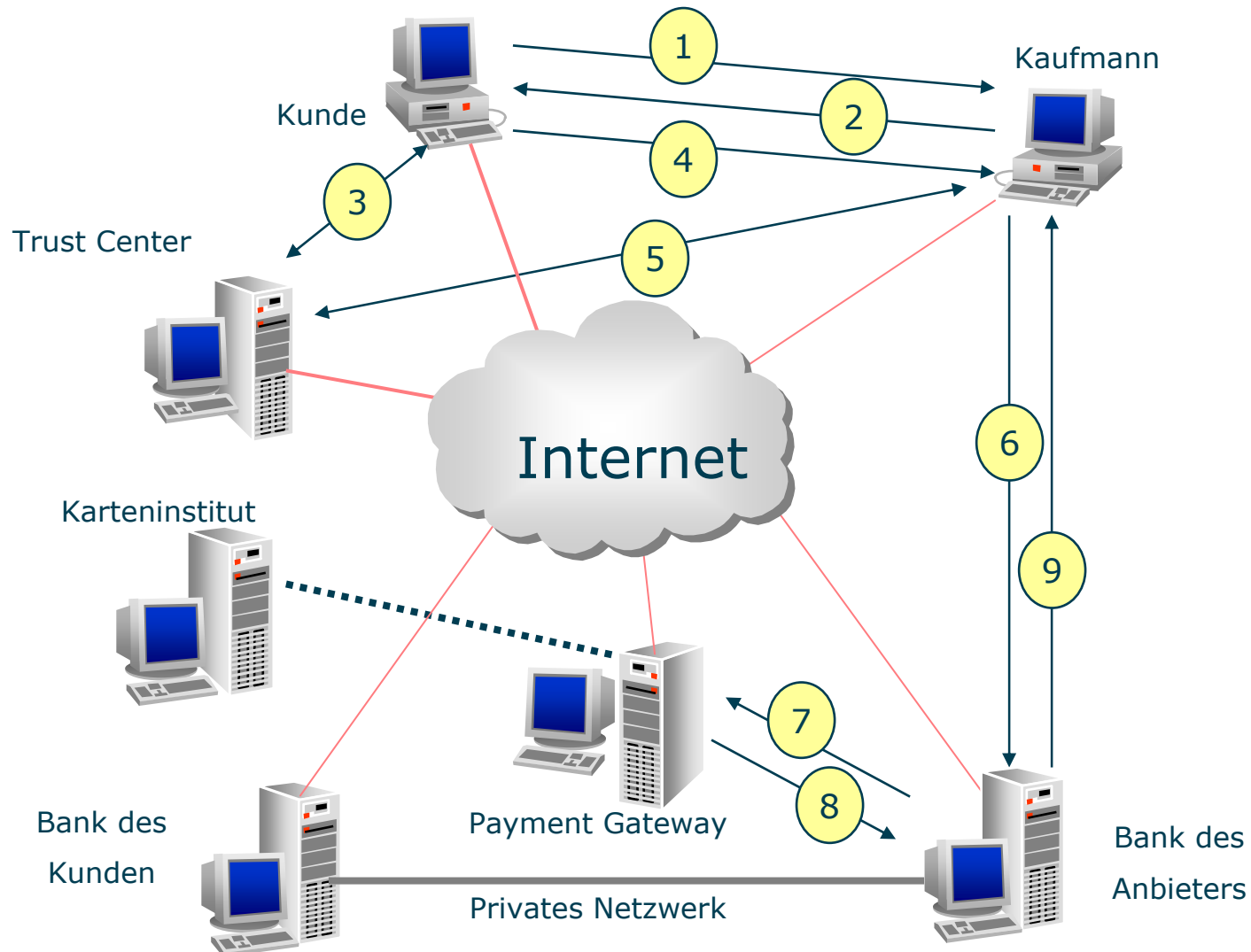
- Kosten
 - Kreditkarten
 - Die Kreditkarteninstitute verlangen eine Gebühr für jede Transaktion.
 - Es gibt 2 verschiedene Arten von Zahlungen.
 - 1. Karte anwesend
 - In der Regel wird eine Gebühr von 1% bis 3% verlangt, da die Zahlung relativ sicher ist.
 - 2. Karte abwesend
 - In der Regel wird eine Gebühr von 6% bis 12% verlangt, um mögliche Verluste zu decken, da die Zahlung relativ unsicher ist.

Verschlüsselung und E-Commerce



- Kreditkarten
 - Bisher sind telefonische oder Internet-Transaktionen als „Karte abwesend“ zu betrachten.
 - Mit Secure Electronic Transaction (SET von IBM) sind die Kreditkarteninstitute in der Lage, solche Transaktionen als „Karte anwesend“ zu betrachten.
 - Dadurch fallen weniger Gebühren an.

Verschlüsselung und E-Commerce



Verschlüsselung und E-Commerce



- Secure Electronic Transaction (SET)
 - 1. Der Kartenbesitzer (Kunde) möchte ein Produkt des Anbieters (Kaufmann) erwerben.
 - Der Kartenbesitzer sendet sein Zertifikat an den Kaufmann.
 - 2. Der Kaufmann schickt das Angebot, sein Zertifikat und das Zertifikat seiner Bank.
 - Beide Zertifikate sind mit dem Private Key des Trust Centers unterzeichnet.
 - 3. Der Kartenbesitzer entschlüsselt die Signaturen mit dem Public Key des Trust Centers.
 - 4. Der Kartenbesitzer schickt seine Bestellung an den Anbieter.
 - Diese ist mit dem Public Key des Anbieters verschlüsselt.
 - 5. Der Anbieter bestätigt das Kundenzertifikat über das Trust Center.

Verschlüsselung und E-Commerce



- Secure Electronic Transaction (SET)
 - 6. Der Kaufmann generiert eine Authentisierungsanfrage für den Kunden an seine Bank.
 - Diese wird mit dem Public Key seiner Bank verschlüsselt.
 - 7. Die Bank des Anbieters sendet eine Authentisierungsanfrage an das Payment Gateway.
 - Das Payment Gateway prüft die Gültigkeit der Karte über eine bankeigene Verbindung.
 - 8. Das Payment Gateway sendet eine Bestätigung oder eine Zurückweisung für die Karte an den Kaufmann zurück.
 - Dies kann mit oder ohne Rückfrage bei der Bank des Kunden geschehen.
 - 9. Bei Zustimmung sendet die Bank des Anbieters eine Bestätigung mit Identifizierung.
 - Diese wird mit dem Public Key des Kaufmanns verschlüsselt.

Wir freuen uns über Ihr Feedback



Network Training and Consulting GmbH
Weidenauer Straße 15
57078 Siegen
siegen@networktraining.de

Network Training and Consulting Südwest GmbH
Gutenbergstraße 13
70771 Leinfelden-Echterdingen
stuttgart@networktraining.de

Bundesweite Infoline: 0180 11 77 333
(Festnetz / Telekom 4,6 Cent / Minute)