Kapitel 9: Informationssicherheit und Datenschutz

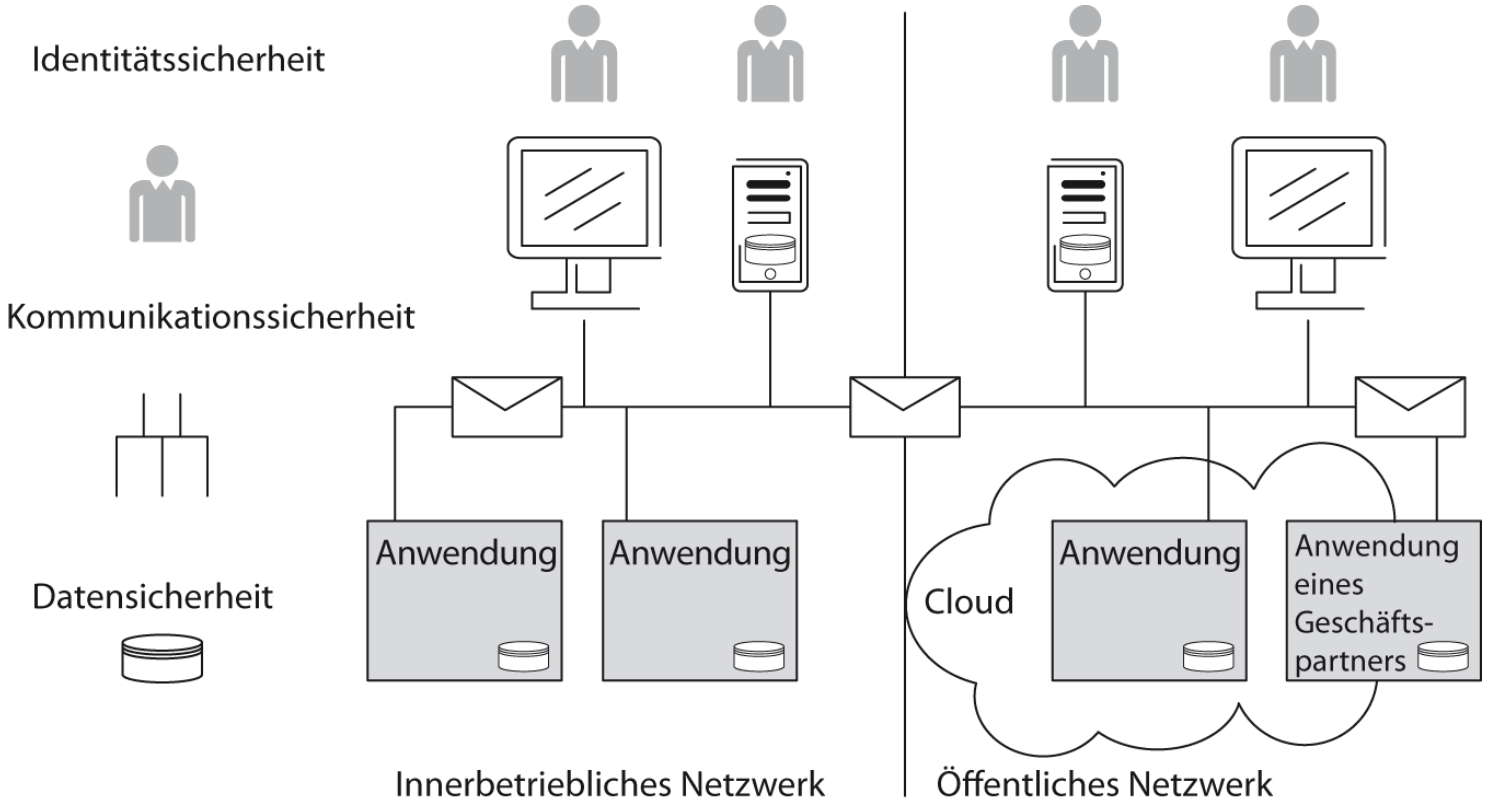
9. Informationssicherheit und Datenschutz

1. IS-Betrieb und Informationssicherheit
2. Sicherheitstechnische Grundlagen
3. Sicherheitstechnische Anwendungen
4. Sicherheitsmanagement
5. Umgang mit sensiblen Daten (Datenschutz)

9.1 IS-Betrieb und Informationssicherheit

Aufgaben der Informationssicherheit

- Sicherung der Identität der Benutzer (Identitätssicherheit)
- Sicherung der gespeicherten Daten (Datensicherheit) und
- Sicherung der Interaktion (Kommunikationssicherheit).

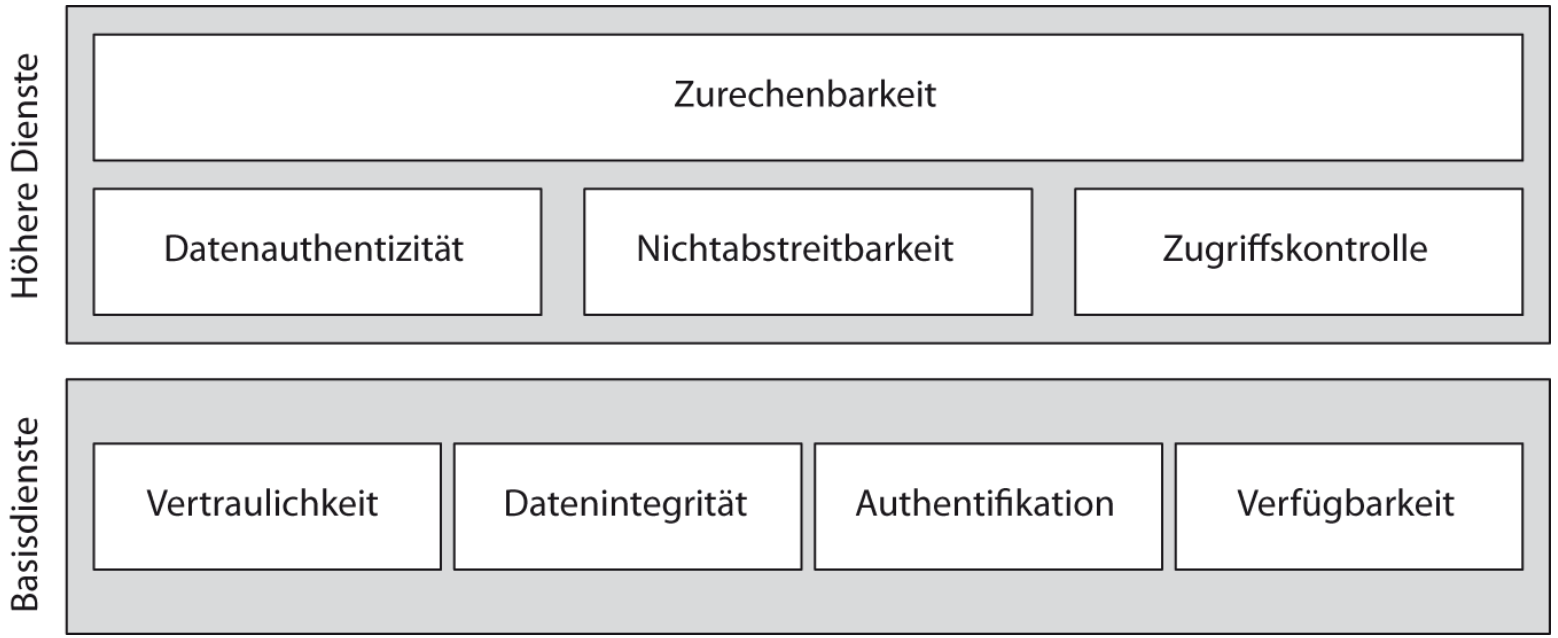


Informationssicherheit

- **Identitätssicherheit** (engl.: identity security) beinhaltet die Sicherung der Identität von Benutzern, das heißt die Gewährleistung, dass die Benutzer diejenigen sind, für die sie sich ausgeben. Für die Gewährleistung der Identitätssicherheit werden **Identitätsmanagementsysteme** (engl.: identity management system) eingesetzt.
- **Datensicherheit** (engl.: data security) beinhaltet die Verhinderung von Datenverlust, Datendiebstahl und Datenverfälschung. Durch vorbeugende Maßnahmen soll die jederzeitige Vollständigkeit und Korrektheit der Daten gewährleistet werden.
- **Kommunikationssicherheit** (engl.: communication security) oder **Netzwerksicherheit** (engl.: network security) beinhaltet alle Maßnahmen zur Gewährleistung der Sicherheit der Kommunikationsverbindungen und zur Sicherung der Informationssysteme gegenüber Angriffen aus Netzwerken.

9.2 Sicherheitstechnische Grundlagen

Schema für informationstechnische Sicherheitsziele



Informationstechnische Sicherheitsziele

- Unter dem Ziel der **Vertraulichkeit** (engl.: confidentiality) versteht man das Bestreben, geheime Information für unberechtigte Dritte unzugänglich zu halten.
- Eine Bedrohung des Sicherheitsziels der Vertraulichkeit ist die **nicht intendierte Informationsweitergabe** oder der **Datendiebstahl** (engl.: data breach). Oft wird mittels gezielter Angriffe auf an sich geschützte Information zugegriffen, die in weiterer Folge kopiert oder offen gelegt wird. Diese Informationsoffenlegung kann sowohl von unautorisierten Personen mittels Ausnutzung einer Sicherheitslücke des Rechners erfolgen, als auch durch an sich *berechtigte Personen innerhalb des Betriebs* (engl.: insider), die diese Daten beabsichtigt oder nicht beabsichtigt zugreifbar machen.
- Unter dem Ziel der **Datenintegrität** (Unveränderthеit, kurz: Integrität; engl.: data integrity) versteht man das Bestreben, die Unveränderthеit von Daten (im „Originalzustand“) nachzuweisen.

Verfahren zur Vertraulichkeit

- Durch **Verschlüsselung** (engl.: encryption) wird eine im Klartext vorliegende Information nach einer bestimmten Methode und unter der Einbeziehung eines *Schlüssels* in eine scheinbar sinnlose Zeichenfolge umgewandelt. Die resultierende Zeichenfolge kann durch Anwendung des richtigen Schlüssels wiederum in den Klartext zurückverwandelt werden.

Sicherheitsverfahren
Verschlüsselung

- **Symmetrische Verfahren**
  - Ver- und Entschlüsselung mit dem gleichen Schlüssel
    - DES (Data Encryption Standard): fixe Schlüssellänge 56 Bit
    - Triple-DES: Fixe Schlüssellänge 168 Bit
    - RC2, RC4 (ursprünglich „trade secrect"): keine fixe Schlüssellänge (diverse Lücken, in SSL nicht mehr erlaubt)
    - IDEA (ETH Zürich): fixe Schlüssellänge 128 Bit

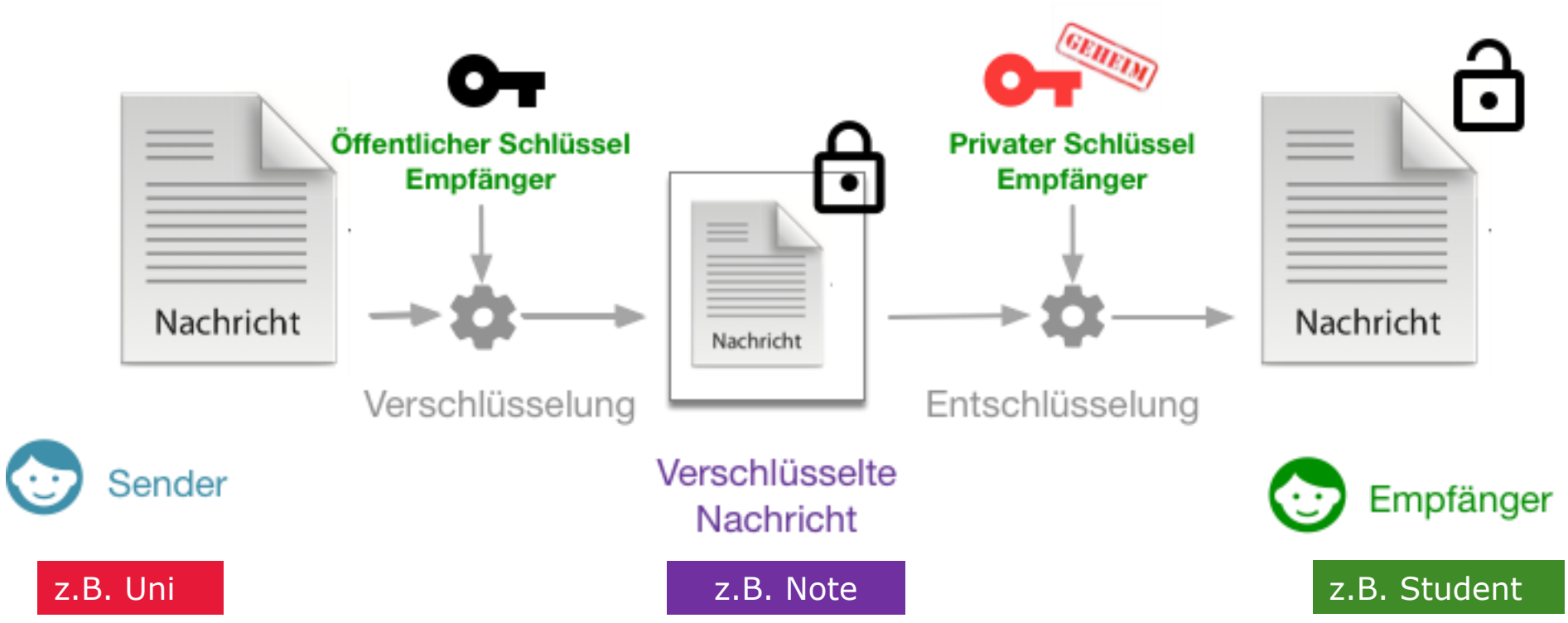
- **Asymmetrische Verfahren**

  Schlüsselpaare (privater und öffentlicher Schlüssel): unterschiedliche Schlüssel für Ver- und Entschlüsselung
  - **Privater Schlüssel** verlässt nicht den Rechner des Besitzers, **öffentlicher Schlüssel** ist allgemein bekannt, wird verteilt
    - Primfaktorenzerlegung: RSA (Schlüssellänge variabel, bspw. 2048 Bit sicher bis 2030, danach > 3072 Bit)
    - EC (Elliptische Kurven): bspw. bei Bitcoin im Einsatz

Asymmetrische Kryptografie

- Die **asymmetrische Kryptografie** (engl.: public key cryptography) verwendet Verschlüsselungsverfahren, die auf dem Einsatz von *Schlüsselpaaren* beruhen. Ein Schlüsselpaar besteht aus einem **geheimen Schlüssel** (privater Schlüssel, engl.: private key) und einem **öffentlichen Schlüssel** (engl.: public key). Eine Meldung, die mit einem der beiden Schlüssel verschlüsselt wurde, kann nur mit dem jeweils anderen Schlüssel wiederum entschlüsselt werden.

Anwendung von asymmetrischen Verschlüsselungsverfahren zur Erreichung von Vertraulichkeit

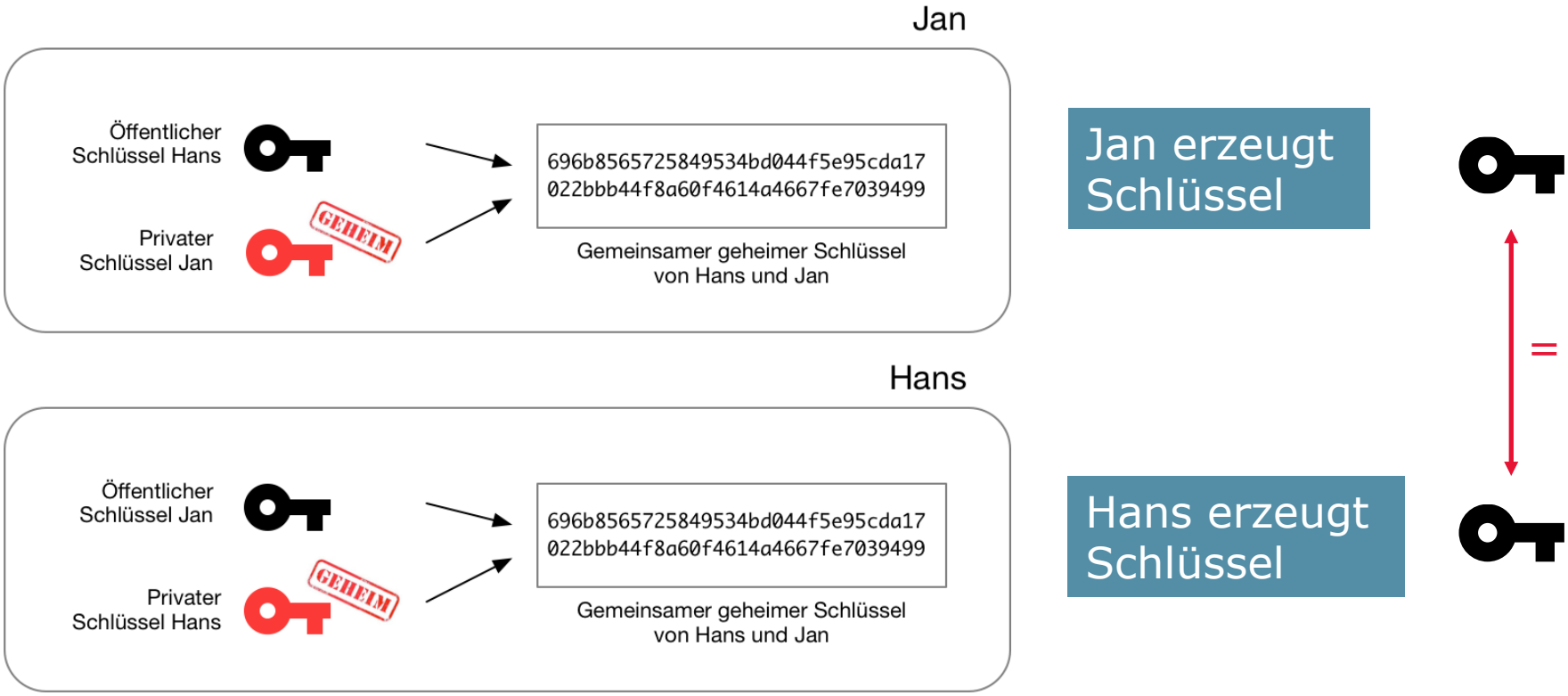


Eine mit einem **öffentlichen** Schüssel verschlüsselte Nachricht kann nur mit zugehörigem **privaten** Schlüssel entschlüsselt werden

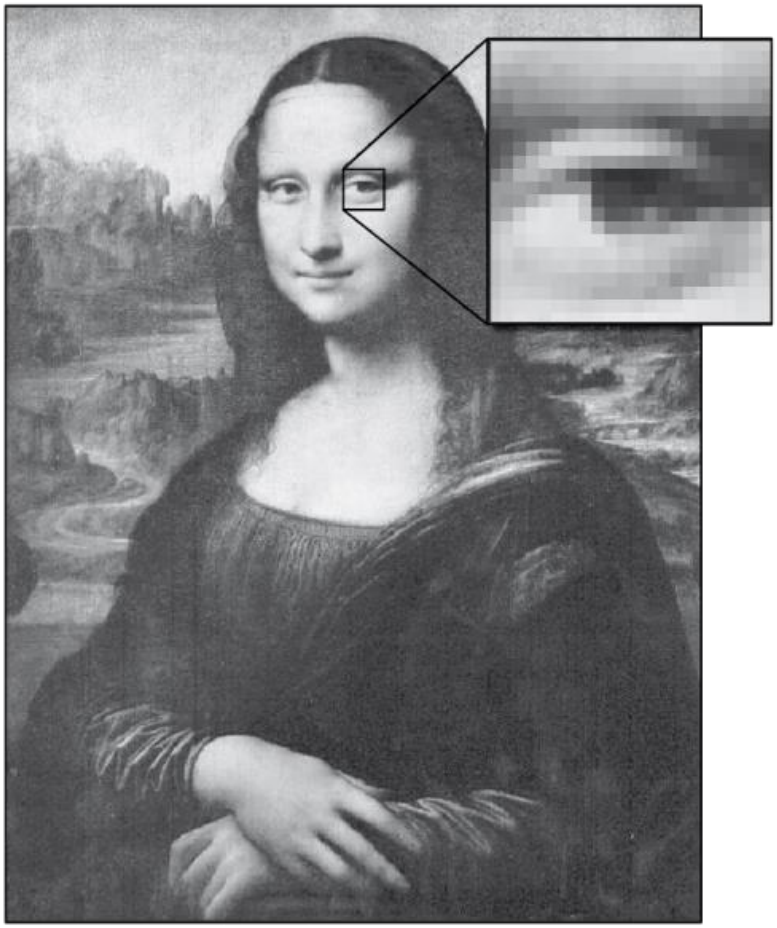
Nur der Besitzer des **privaten** Schlüssels kann die Nachricht dekodieren

Ableitung eines gemeinsamen geheimen Schlüssels nach Diffie, Hellman und Merkle

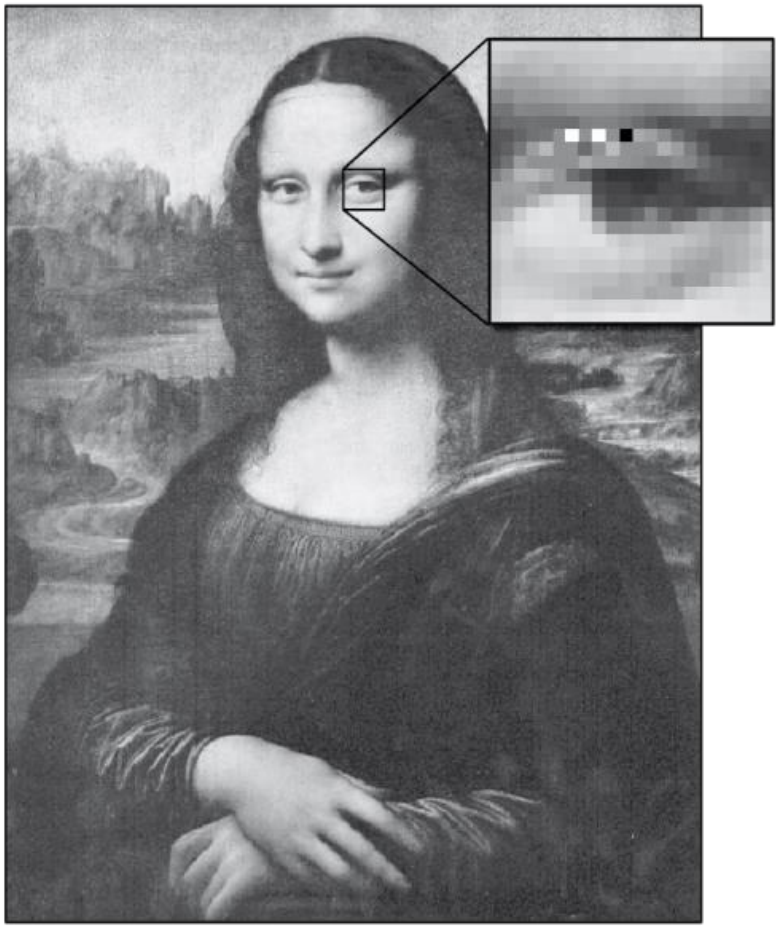
Nutzung von asymmetrischer Kryptografie zur Schaffung eines gemeinsamen Geheimnisses



Verfahren zur Übertragung vertraulicher Information: Steganografie



Ohne steganografische Information



Mit steganografischer Information

Sicherheitsdienste
Basisdienst: Datenintegrität

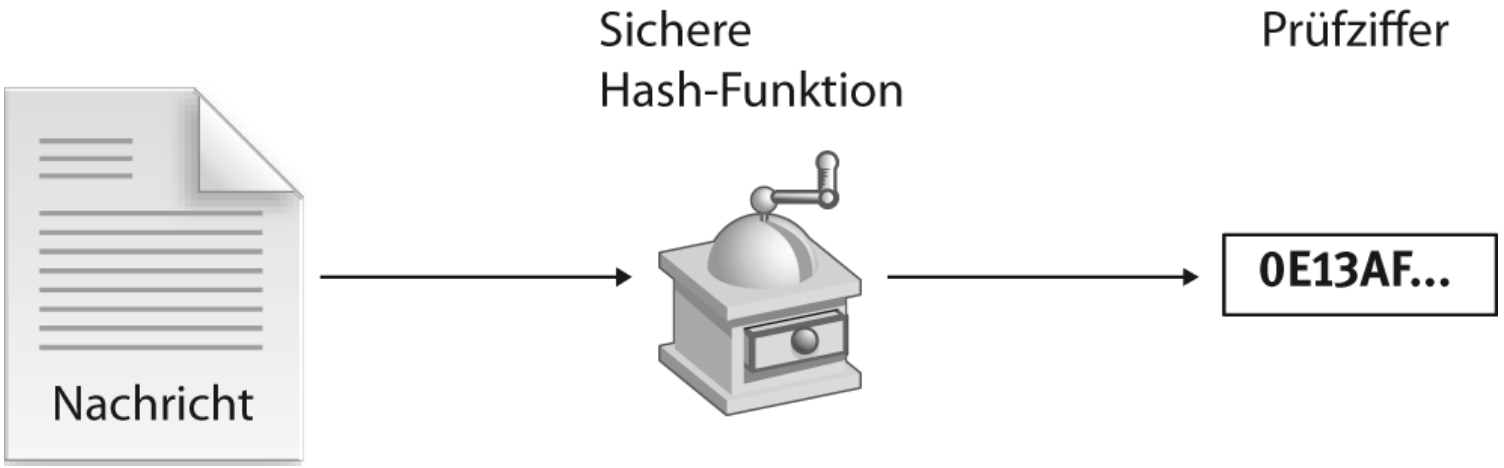
- Datenintegrität (Unveränderheit)
  - Ziel: garantieren, dass Daten in unveränderter Form (im „Originalzustand“) vorliegen
  - Verfahren: Hash-Funktionen

    Einweg-Funktion, die aus beliebigen Daten einen **Hash-Wert** in der Länge von meist 128 oder 160 Bit erzeugt, aus dem die Daten **nicht rekonstruiert** werden können. Bei jeder Veränderung der Daten verändert sich auch der Hash-Wert („Elektronischer Fingerabdruck“).

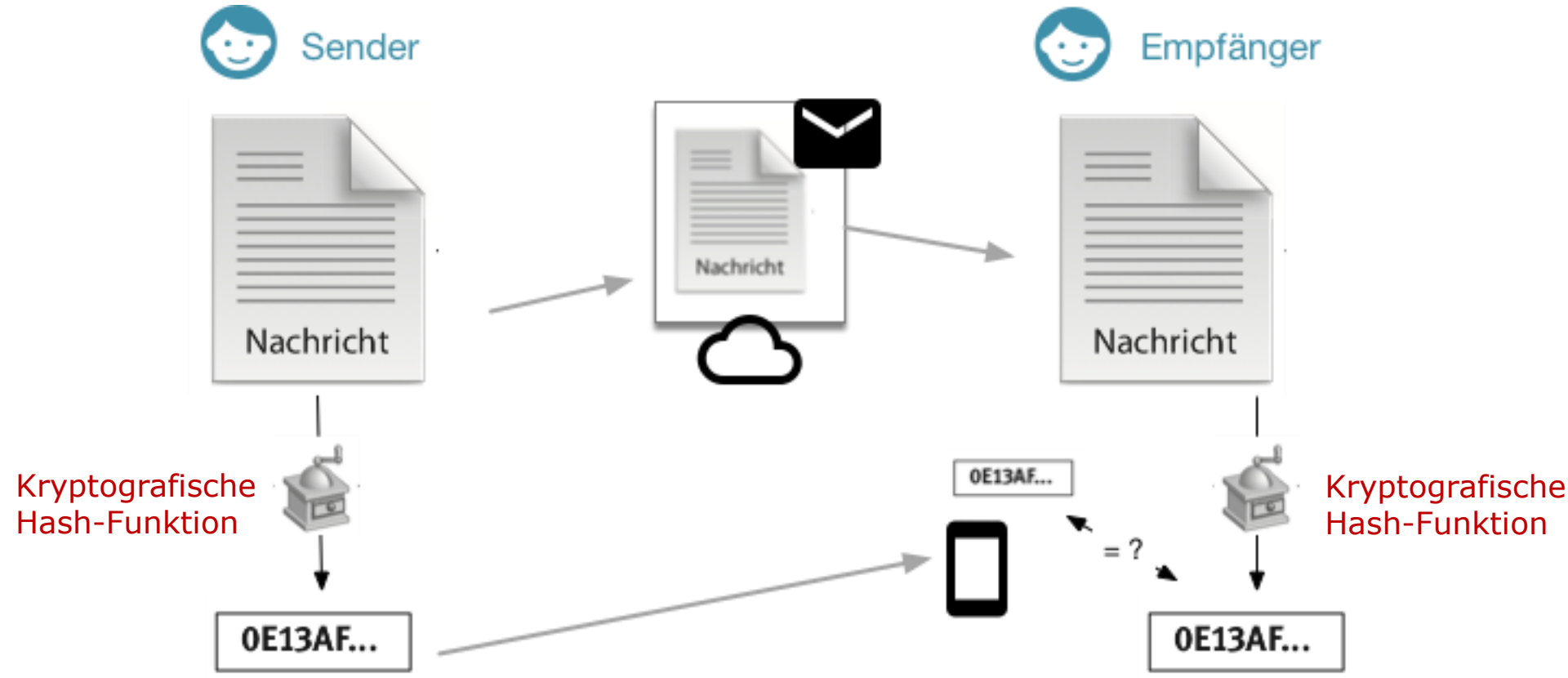
    Algorithmen: MD5 (128 Bit† 2010), SHA1 (160 Bit†), SHA2 (224-512 Bit), SHA3 (224-512 Bit, Aug 2015), RIPEMD160 (160 Bit)

Verfahren zur Integrität

- **Hash-Funktionen** (engl.: hash function) generieren aus beliebig vielen Daten einen wesentlich kürzeren (meist von 128 bis 512 Bit) und eindeutigen Wert (Hash-Wert, Prüfsumme). Hash-Funktionen sind nicht umkehrbar, das heißt, der erzeugte Hash-Wert lässt keine Rückschlüsse auf die ursprünglichen Daten zu. Falls es nicht oder nur sehr schwer möglich ist, zwei Nachrichten mit derselben Prüfsumme zu generieren, handelt es sich um eine **sichere Hash-Funktion** (engl.: secure hash function). Eine Prüfsumme, die durch eine sichere Hash-Funktion generiert wurde, wird auch als *digitaler Fingerabdruck* (engl.: message digest, message authentication code, Abkürzung: MAC) bezeichnet. Ein **HMAC** (Abkürzung von engl.: keyed-hash message authentication code) ist eine kryptografische Prüfsumme, die zusätzlich durch einen geheimen Schlüssel abgesichert wird.



Nutzung einer kryptografischen Prüfsumme zum Nachweis der Integrität



„Elektronischer Fingerabdruck"

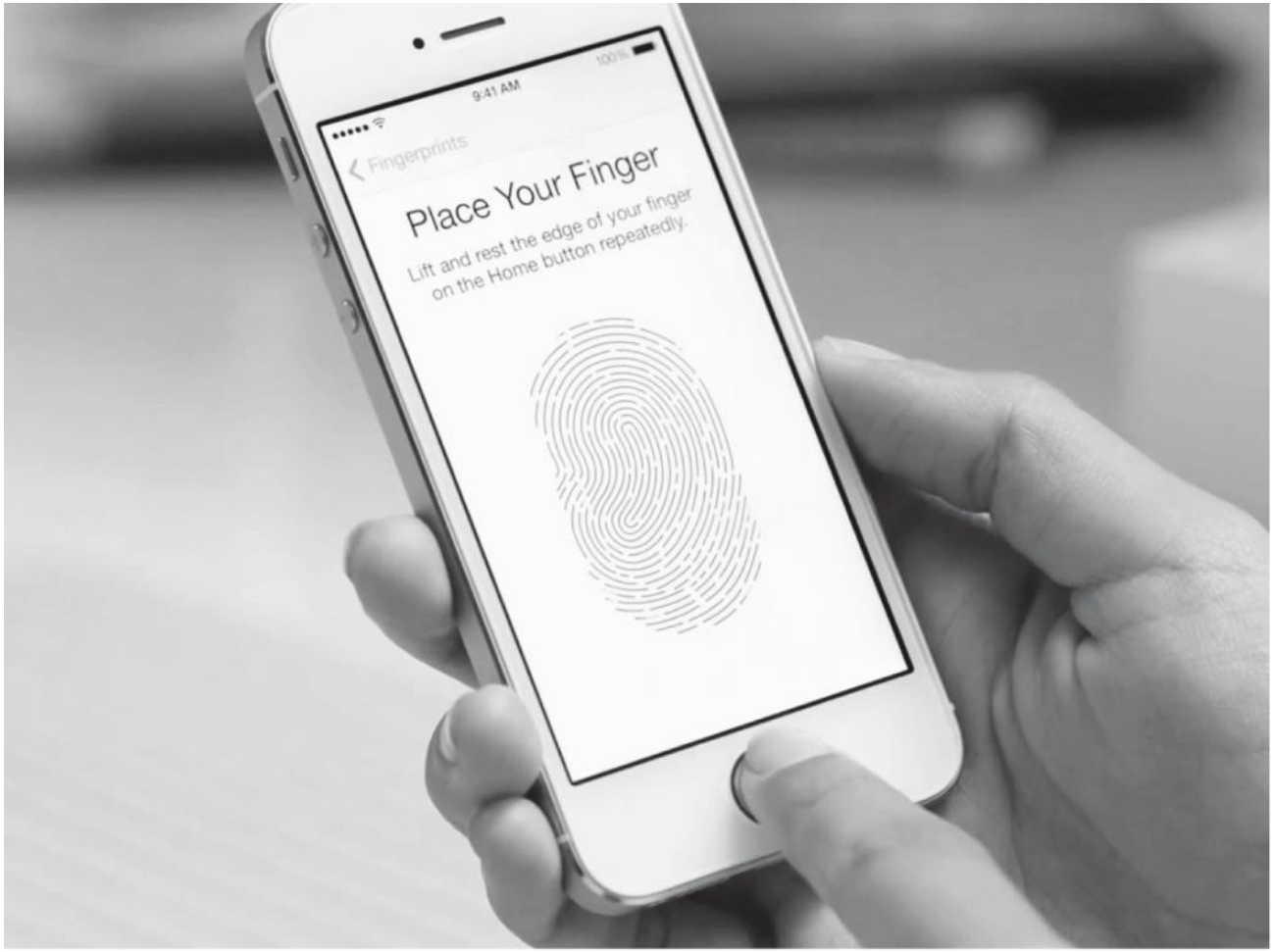
Informationstechnische Sicherheitsziele (2)

- Unter der **Authentifikation** (engl.: authentication) versteht man die nachweisliche Identifikation eines Benutzers oder eines Kommunikationspartners (beispielsweise eines softwarebasierten Diensts).
- Eine Bedrohung des Sicherheitsziels der Authentifikation ist der **Identitätsdiebstahl** (engl.: identity theft), bei dem sich ein Angreifer die **Anmeldeinformation** (engl.: credentials) der attackierten Person verschafft und sich als diese ausgibt.
- Unter dem Ziel der **Verfügbarkeit** (engl.: availability) eines Informationssystems versteht man das Bestreben, dass Dienste, die einem berechtigten Benutzer von einem Informationssystem angeboten werden, diesem auch stets zur Verfügung stehen. Es soll insbesondere verhindert werden, dass Dienste aller Art durch eine übermäßige Beanspruchung blockiert werden können.

Sicherheitsdienste
Basisdienst: Authentifikation

- Authentifikation
  - Ziel: Prüfung der Identität eines Benutzers
  - Verfahren:
    - Kenntnis eines **Geheimnisses**
      Beispiel: Kennwort (engl.: password)
    - Besitz eines **Gegenstandes**, der nicht weiter gegeben werden darf und schwer duplizierbar ist
      Beispiele: Autoschlüssel, Chipkarte, privater Schlüssel
    - **Körperliche Merkmale** (biometrische Verfahren)
      Beispiele: Fingerabdruck, Geometrie der Hand, Netzhaut, Iris, Gesichtsform, Stimme

Smartphone mit Fingerabdruckleser



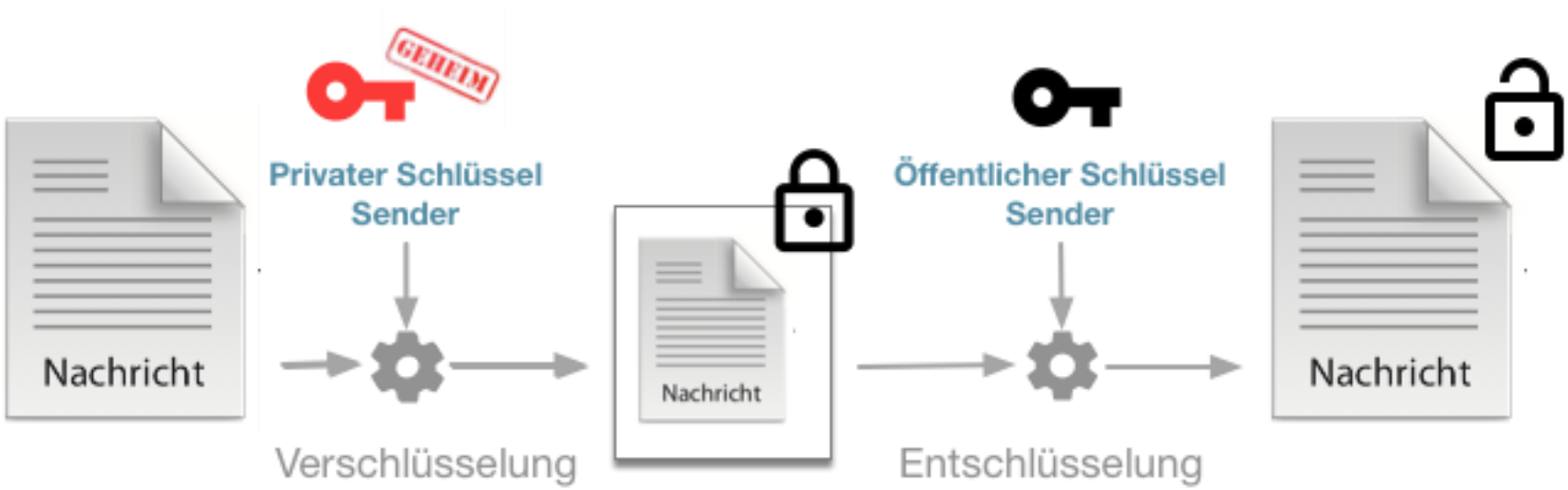
Spezielle Formen

- **Einmalkennwort:**
  - Kennwort, das für eine einmalige Verwendung bestimmt ist
  - meist eine sehr kurze Gültigkeitsdauer hat.
  - Dadurch werden manche Angriffe wie Mithören und Wiederholungen des Kommunikationsverkehrs verhindert.
  - Jeder Authentifizierungsversuch verlangt ein neues Einmalkennwort.

- **Multifaktorauthentifizierung:**
  - Identität einer Person wird auf Basis von mehreren getrennten Authentifizierungsverfahren geprüft wird.
  - Nutzung möglichst unterschiedlicher Kommunikationskanäle
  - **Zweifaktorauthentifizierung:**
    - Kombination von zwei Authentifizierungsverfahren
    - Bspw. Kennwort + Einmalkennwort via SMS

Sicherheitsverfahren

Authentifikation durch asymmetrische Verschlüsselungsverfahren



Sender

Verschlüsselte Nachricht

Empfänger

z.B. Student

z.B. Bestellung

z.B. Uni, Behörde, Bank usw.

Eine mit einem **privaten** Schüssel verschlüsselte Nachricht kann nur mit *zugehörigem* **öffentlichen** Schlüssel entschlüsselt werden

Nur der Besitzer des **privaten** Schlüssels kann die Nachricht geschickt haben

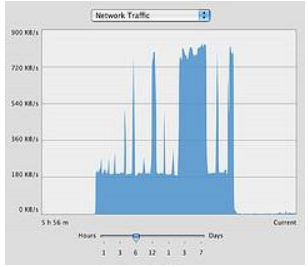
Lehrbuch **WIRTSCHAFTSINFORMATIK**

Sicherheitsdienste
Basisdienst: Verfügbarkeit

- Verfügbarkeit
  - Ziel: Gewährleistung, dass Dienste den berechtigten Benutzern stets zur Verfügung stehen
  - Angriffe:
    - **Denial-of-Service-Abgriff (DoS)**

      Ein Server wird mit „sinnlosen" Anfragen überflutet, sodass er seiner ursprünglichen Aufgabe nicht (oder nicht im vollen Umfang) nachkommen kann (Verweigerung des Dienstes)

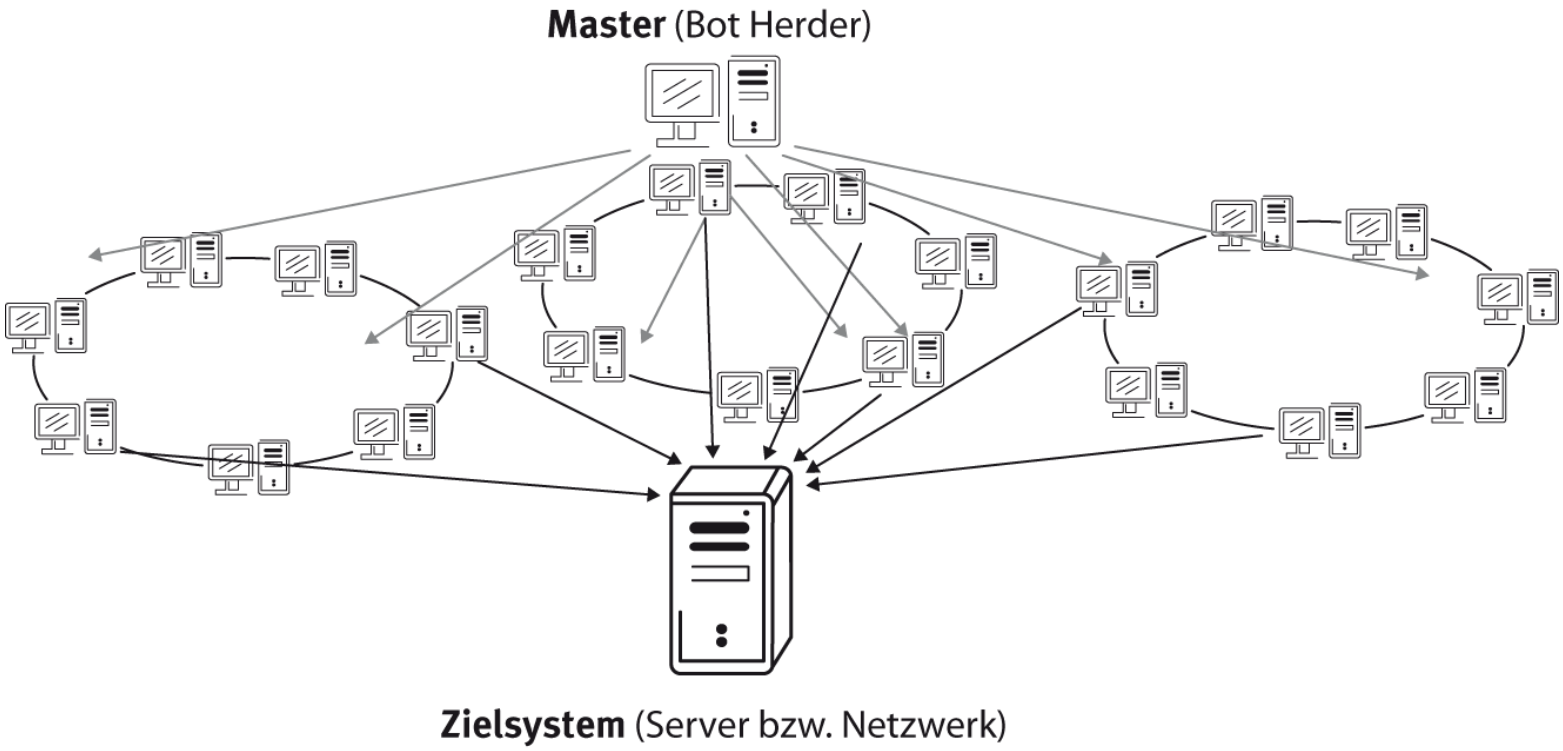
    - Spezialfall: Distributed-Denial-of-Service-Angriff (DDoS)
    - Besonders problematisch für E-Commerce-Anwendungen



  - Maßnahmen:
    - Erkennen von atypischen Nutzungsmustern
    - Beschränkung der Ressourcenzuweisungen an einzelne Benutzer

Verteilte Denial-of-Service-Angriff (DDoS)

- Unter einem **Botnetz** (engl.: botnet) versteht man eine Vielzahl von Rechnern, die mittels Schadprogrammen unter die Kontrolle eines Angreifers gelangen, der diese Rechner ohne Wissen der Besitzer für unterschiedliche Typen von Aufgaben missbrauchen kann.



Beispiele von DDoS-Angriffen:

Botnet Mariposa (2010)

- Im Jahr 2010 von spanischen Behörden aufgedeckt
- Das Botnetz umfasste mehr als 12 Millionen Rechner in mehr als 190 Ländern.
- Zu den befallenen Rechnern gehörten Rechner von etwa der Hälfte der 1.000 größten Unternehmen der USA (lt. US Fortune)

Botnet Mirai (2016)

- Besteht aus 800.000+ Mio gekaperten „Smart Devices“ Home-Router, IP-Kameras, TV-Boxes, ...
- **Okt 2016:** Angriff auf Dyn (DNS-Anbieter) hat zur Folge, dass Twitter, Netflix, Paypal, Spotify vorallem in USA einen Tag nicht mehr nutzbar waren
- **Nov 2016:** Gesamte Online-Anbindung des afrikanischen Landes Liberia massiv beeinträchtigt
- **Nov 2019:** zumindest 126 Varianten im Umlauf.
- Aktuell „Smominru“

Höhere Ziele

- Unter **Datenauthentizität** (engl.: data authenticity) versteht man die nachweisliche Identifikation von Information (zum Beispiel Meldungen oder Dateien). Hierzu zählt sowohl der Beweis der Integrität der Daten als auch der Beweis ihrer Herkunft.
- Unter dem Begriff **Nichtabstreitbarkeit** (engl.: non-repudiation) versteht man Maßnahmen, die gewährleisten, dass ein Absender das Versenden einer Meldung ebenso wenig abstreiten kann, wie ein Empfänger deren Erhalt.
- Die **Zugriffskontrolle** (engl.: access control) ist ein höherer Dienst zur Erreichung von Informationssicherheit, der auf der korrekten Authentifikation von Benutzern (und Programmen) aufbaut. Die Zugriffskontrolle befasst sich mit der Autorisierung von Zugriffen, um jedem Benutzer ausschließlich die Aktionen zu erlauben, zu denen er berechtigt ist.
- Die **Zurechenbarkeit** (engl.: accountability) ist ein höherer Dienst, der eine funktionsfähige Zugriffskontrolle sowie die Nichtabstreitbarkeit voraussetzt. Durch diesen Dienst wird protokolliert, welche Benutzer welche Systemressourcen in Anspruch genommen haben.
- Der **Schutz der Privatsphäre** (engl.: privacy) ist ein höheres Ziel, wobei angestrebt wird, dass jede Person bestimmen kann, was mit ihren personenbezogenen Daten geschehen darf.

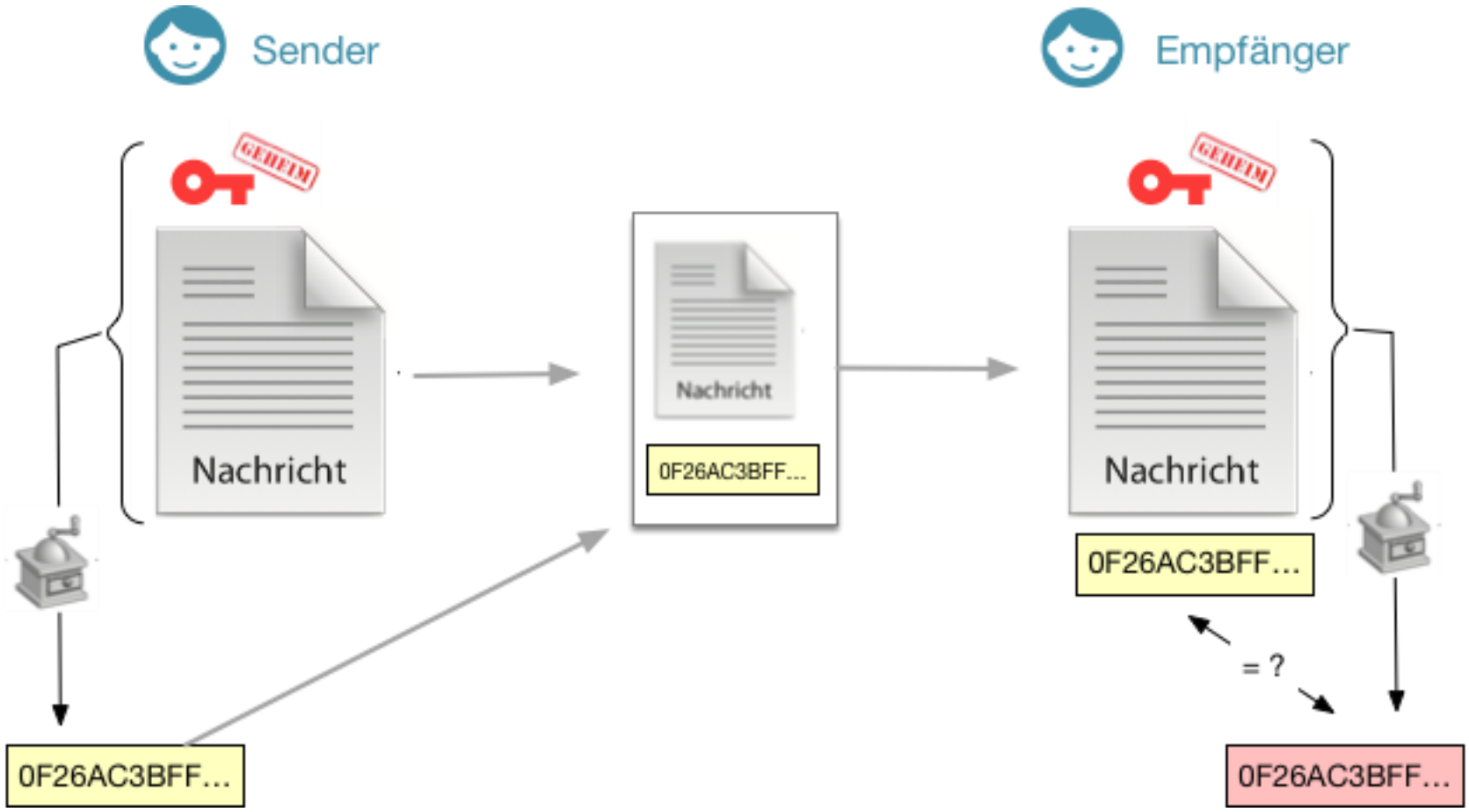
9.3 Sicherheitstechnische Anwendungen

Verfahren zur Wahrung von Datenintegrität + Authentizität

- **HMAC**
  - Abkürzung von engl.: hash message authentication code
  - Verfahren zur Erreichung von Integrität und zum Nachweis des Ursprungs der Daten
  - Kombination von kryptografischer Prüfsumme (elektronischer Fingerabdruck) und einem Schlüssel
  - Beliebige Verfahren für kryptografische Prüfsummen nutzbar

+

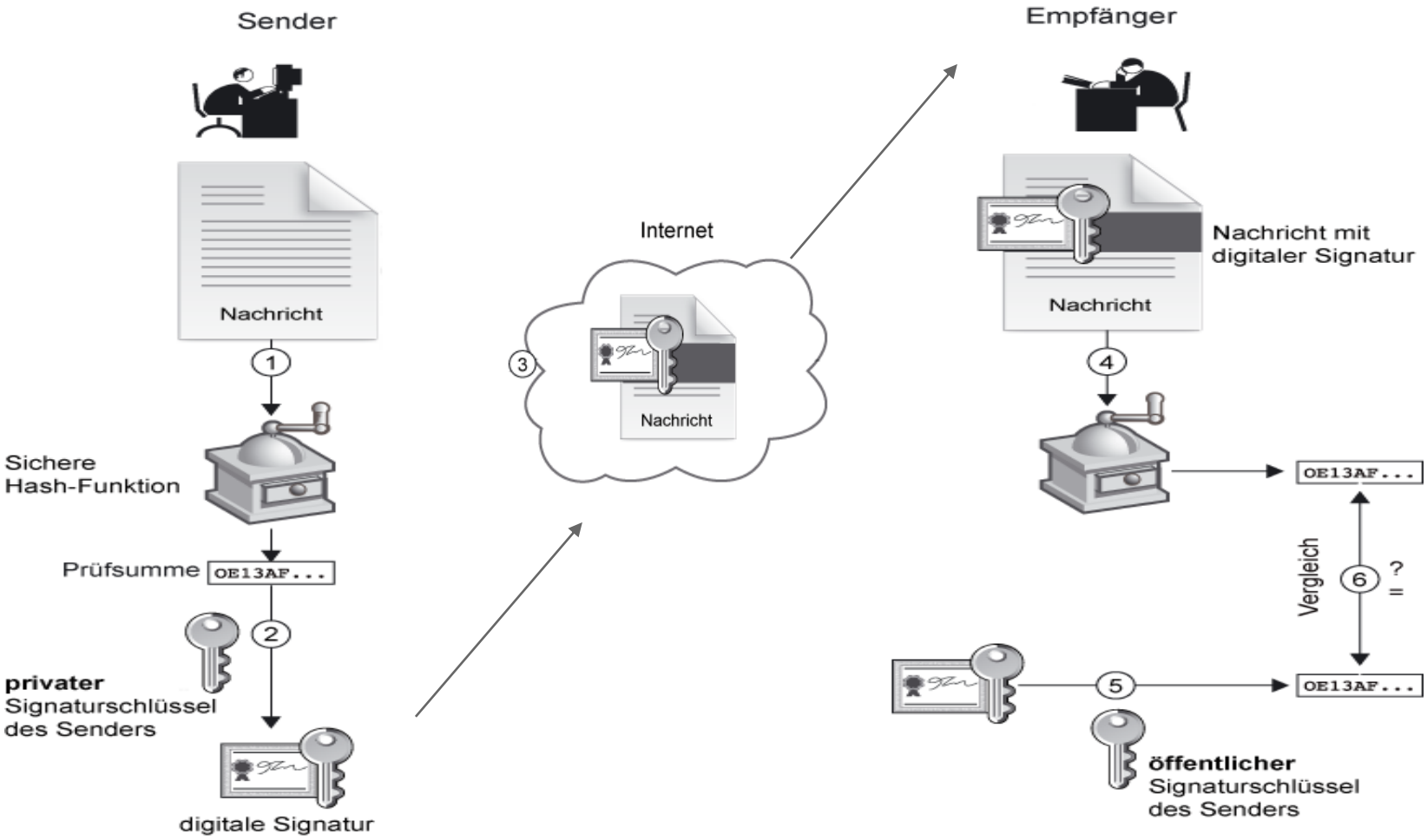
Nutzung eines HMAC zum Nachweis der Integrität und des Ursprungs



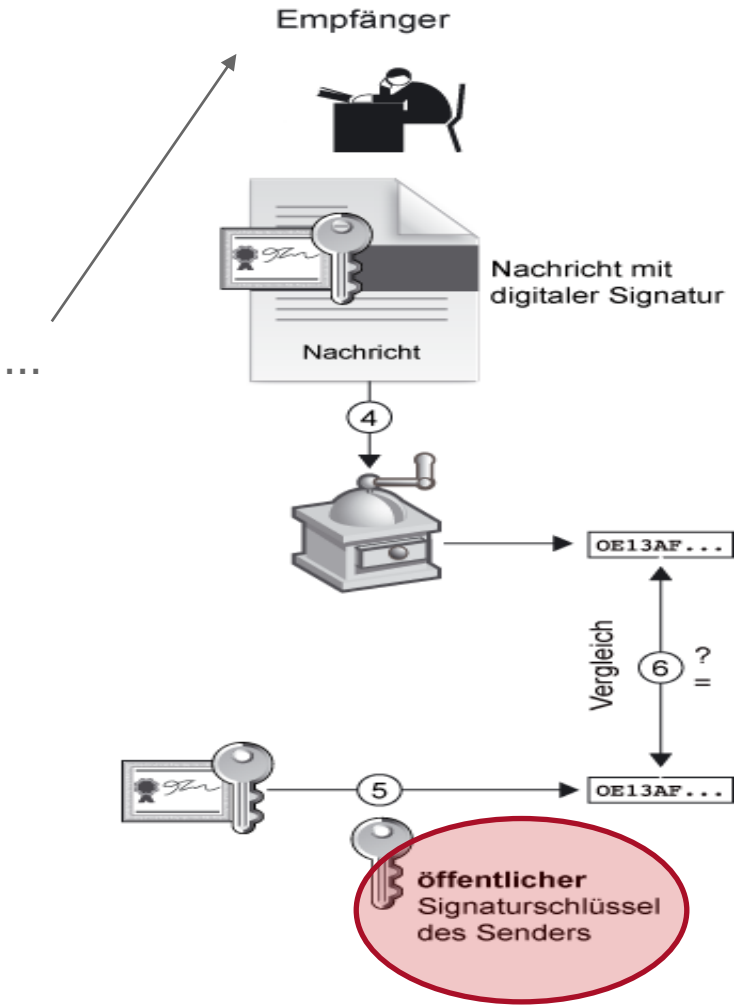
Elektronische Unterschrift

- Unter einer **elektronischen Unterschrift** (digitale Signatur, engl.: digital signature) versteht man einen kryptografisch geschützten Nachweis, dass ein eindeutig identifizierter Benutzer einen Datenbereich (ein digitales Dokument) unterzeichnet hat. Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel für einen Datenbereich, das mithilfe eines zugehörigen öffentlichen Schlüssels den Inhaber und die Unverfälschtheit der Daten erkennen lässt. Für digitale Signaturen, die dem Signaturgesetz genügen, muss der öffentliche Schlüssel aus einem Zertifikat einer anerkannten Zertifizierungsstelle stammen.

Ablauf: Elektronische Unterschrift



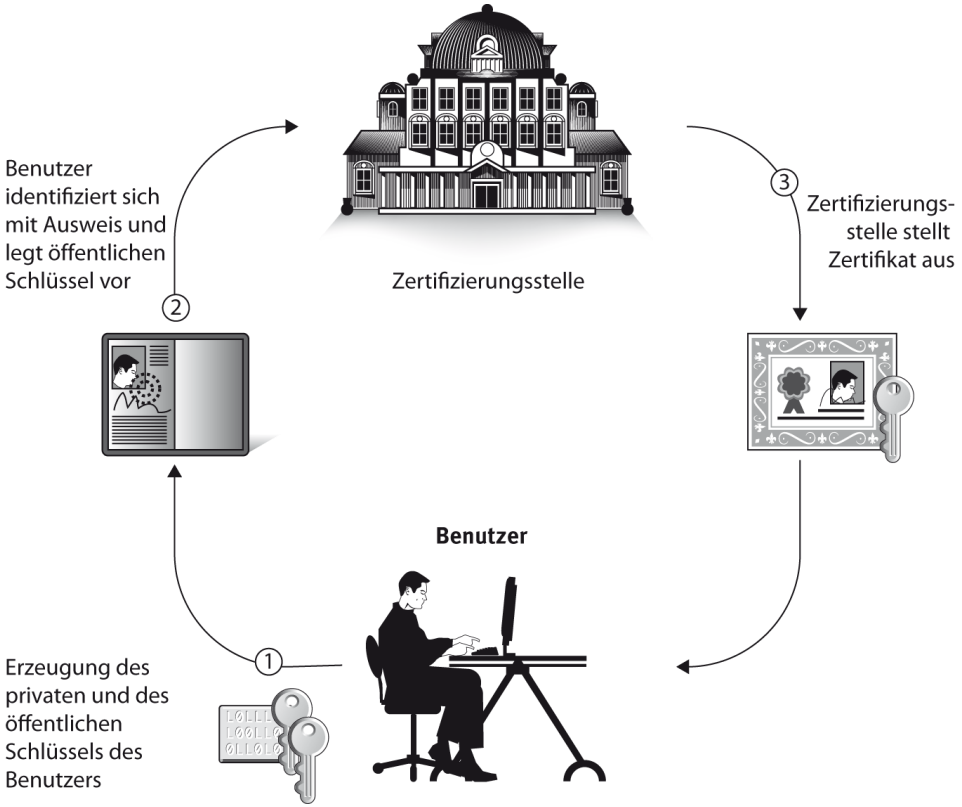
Personenbindung für Elektronische Unterschrift



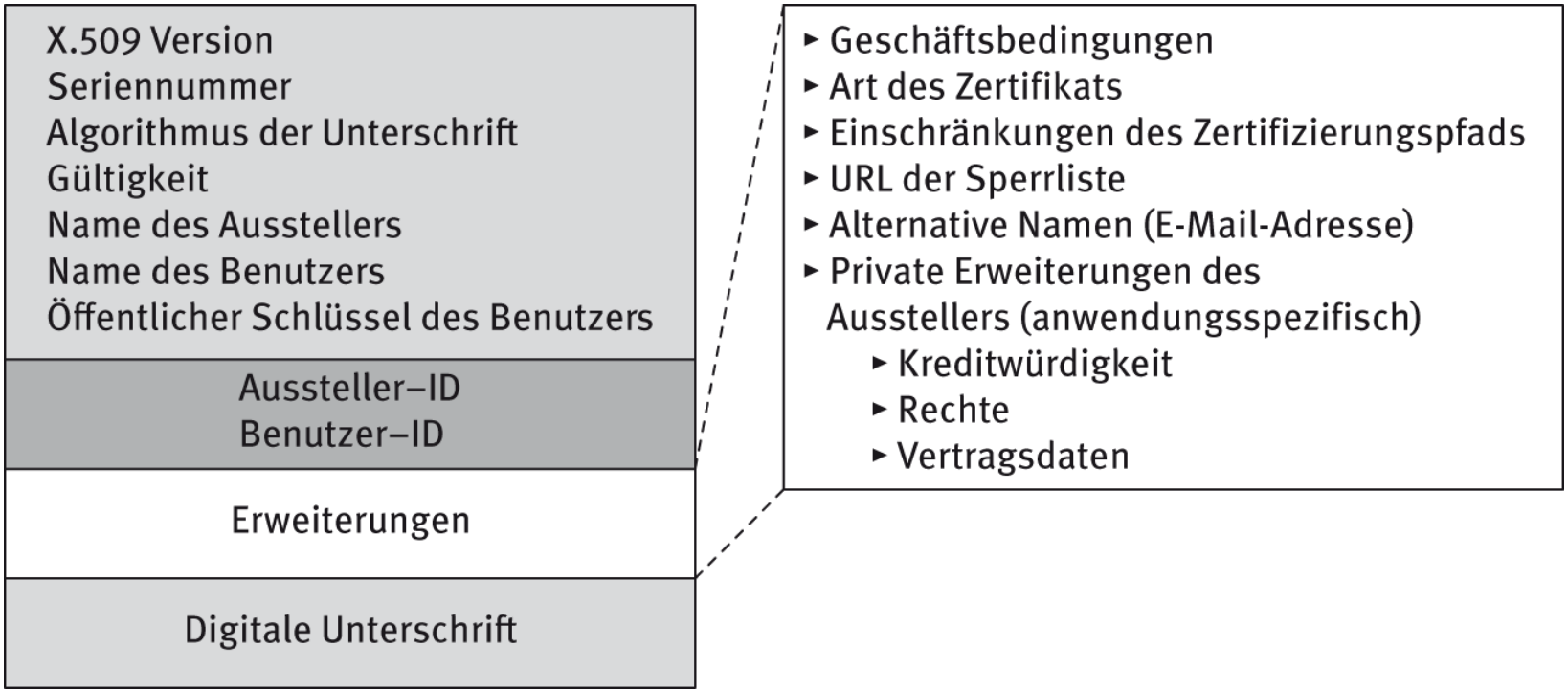
- Identität des Unterzeichners wird beim Empfänger durch dessen öffentlichen Schlüssel geprüft
- Wie kommt ein **Empfänger** in einem öffentlichen Netz auf zuverlässige Weise an den **öffentlichen Schlüssel** des **Absenders**?
- Wie kann ein **Empfänger** prüfen, ob ein **öffentlicher Schlüssel** wirklich zu der vermeintlichen **Person** gehört?

Elektronische Ausweise

- Ein **digitales Zertifikat** (engl.: digital certificate) ist ein digitales Dokument, das von einer Zertifizierungsstelle digital signiert wird und einen bestimmten öffentlichen Schlüssel (sowie weitere Information) nachweislich einer Person oder einer Organisation zuordnet.



Aufbau von X.509-Zertifikaten



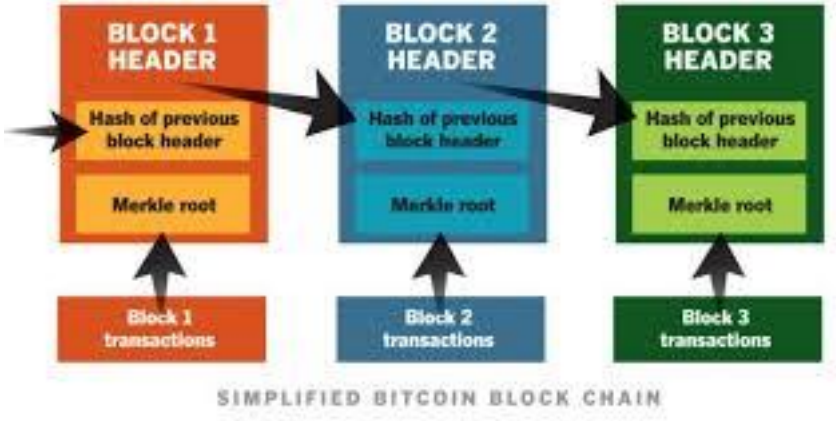
Verfahren zur Nachvollziehbarkeit von Geschäftstransaktionen
Gesicherte Transaktionsverzeichnisse

- **Transaktionsverzeichnis**:
  - Auflistung von zusammengehörigen (Geschäfts-)transaktionen.
  - Welche Information im Detail pro Transaktion gespeichert wird, ist anwendungsabhängig gestaltbar.
  - Typischerweise umfassen die Einträge im Transaktionsverzeichnis
    - einen Zeitstempel,
    - die Beschreibung einer Leistung,
    - den Erbringer und den
    - Empfänger der Leistung.

- **Gesichertes Transaktionsverzeichnis**:
  - durch kryptografische Verfahren wird verhindert, dass im Nachhinein Daten unbemerkt verändert werden können
  - gewährleistet die Nachvollziehbarkeit von Transaktionen

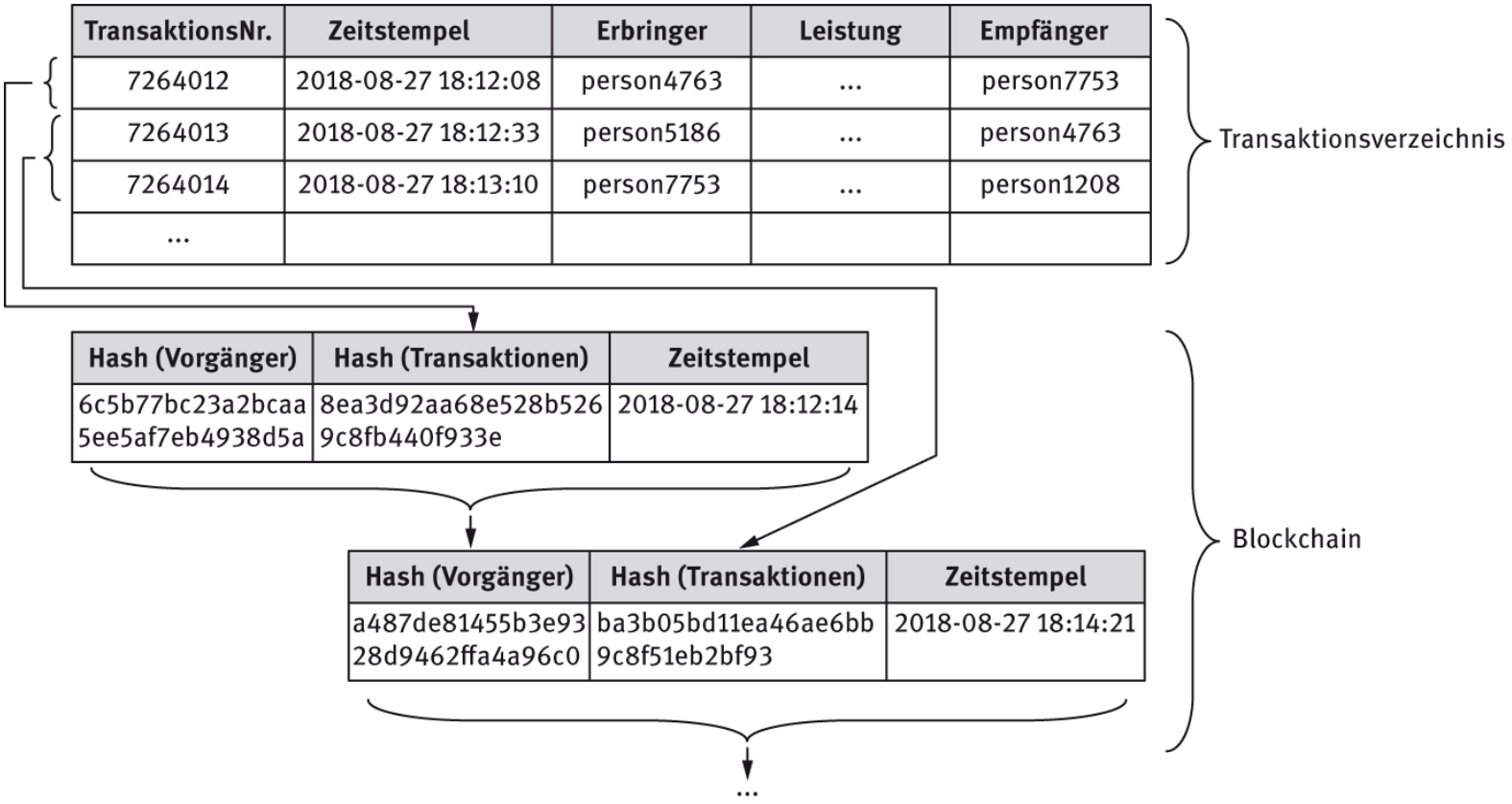
Blockchain

- Form eines kryptografisch gesicherten Transaktionsverzeichnisses
  - Mehrere Transaktionsdaten („Blöcke“) werden zu einer Liste hinzugefügt.
  - Jeder Block enthält den Hash-Wert des vorherigen Blocks.



  - Dadurch wird garantiert, dass
    - Transaktionen auf früheren Transaktionen aufbauen, und dass
    - im Nachhinein die Transaktionsgeschichte nicht verändert werden kann, ohne dass dies bemerkt wird.

Gesicherte Transaktionsverzeichnisse (Blockchain)



Private und öffentliche Transaktionsverzeichnisse

- Wer darf Transaktionen zu einer Blockchain hinzufügen?

- Private Transaktionsverzeichnisse:
  - Nur der Betreiber der Blockchain

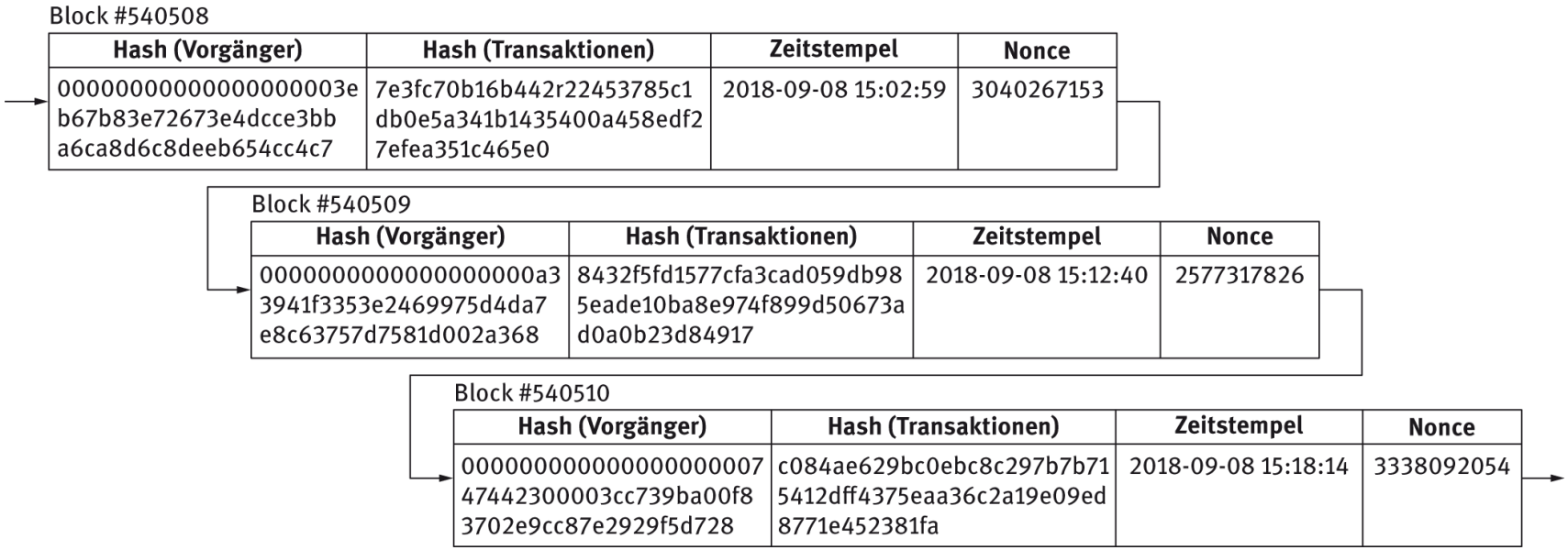
- Öffentliche Transaktionsverzeichnisse:
  - Im Prinzip jeder
  - Probleme:
    - Transaktionslegitimität und Transaktionskonsens: Wer prüft, ob die Transaktionen gültig und korrekt sind?
    - Verfügbarkeit: Schutz gegen DDoS-Angriffe

Öffentliche verteilte Transaktionsverzeichnisse (engl.. DLT Distributed Ledger Technology)

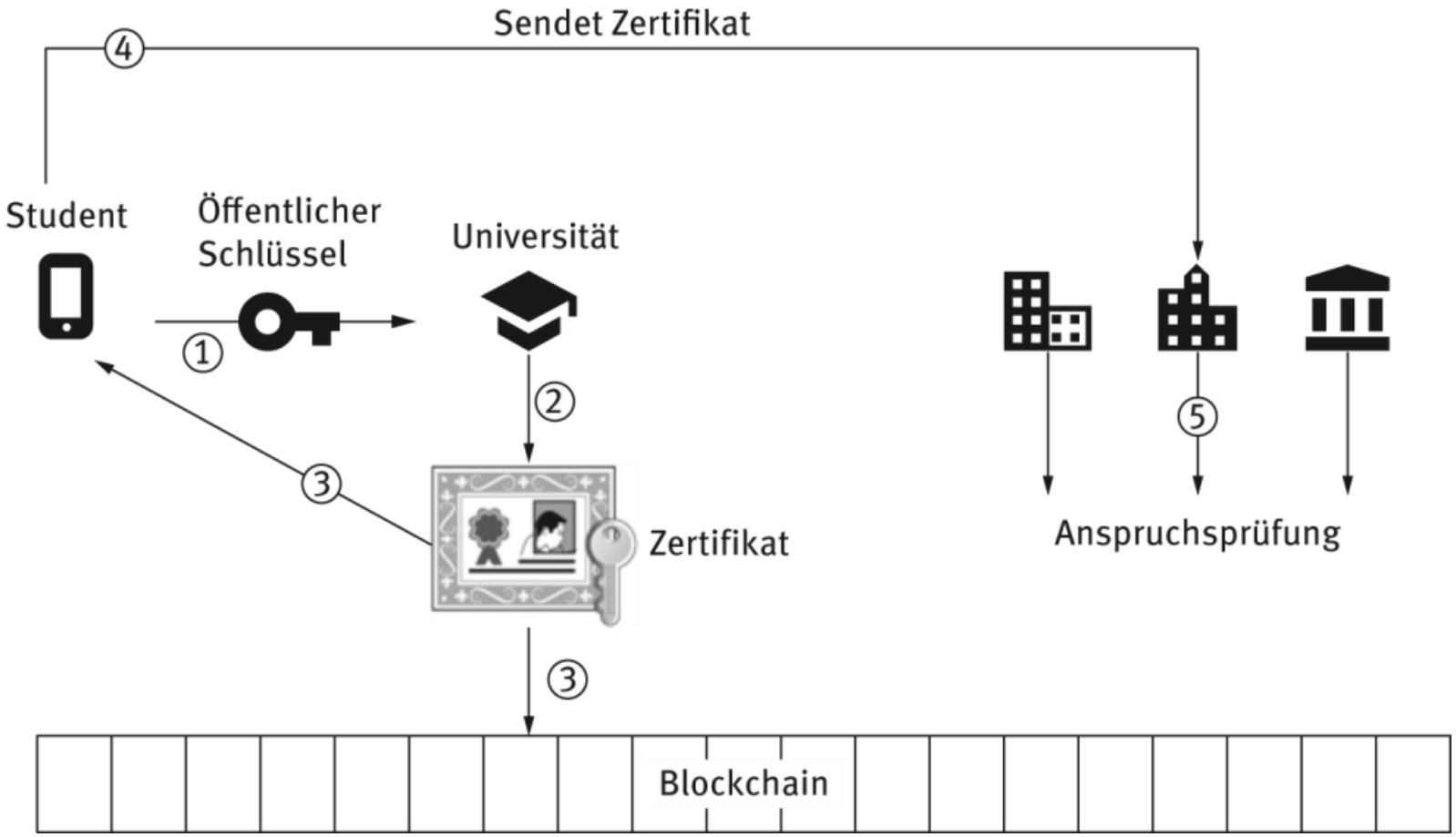
Verteiltes Transaktionsverzeichnis:

- Transaktionsverzeichnis wird redundant auf mehreren Rechnern gespeichert.
- Jedes Hinzufügen einer Transaktion wird mit allen beteiligten Rechnern synchronisiert.
- Korrektheit kann von jedem Teilnehmer verifiziert werden.
- Es gibt keine Abhängigkeit von einer zentrale Instanz.
- Systeme können auf einer gleichberechtigten Stufe (engl.: peer-to-peer) entwickelt werden.
- Konsensverfahren: wenn die Mehrzahl der Teilnehmer den Block akzeptiert, wird er dauerhaft in die Blockchain aufgenommen.
- Löst das Problem der doppelten Ausgaben von Beträgen (engl.: double spending).
- Zur Lösung des DDoS-Problems: bspw. Nachweis erfolgter Leistungen (engl.: proof of work).

Ausschnitt aus der Bitcoin-Blockchain



Blockcerts – Sicherung von Attestierungen in einer Blockchain



9.4 Sicherheitsmanagement

Sicherheitsmanagement

- Unter **Sicherheitsmanagement** (engl.: security management) versteht man sämtliche Aktivitäten zum Schutz von IT-Komponenten vor absichtlichem oder versehentlichem Missbrauch. Das Sicherheitsmanagement soll die Integrität und die Vertraulichkeit der Daten gewährleisten. Zu den Aufgaben gehören die Regelung von *Zugriffsberechtigungen* zu Programmen und Daten, sowie von *Zutrittsberechtigungen* zu Räumen, die sensible Daten oder IT-Komponenten beherbergen. Des Weiteren beinhaltet das Sicherheitsmanagement organisatorische Maßnahmen, welche nicht direkt die Sicherheit eines Systems erhöhen, aber die Grundlage für darauf aufbauende Dienste bilden (wie zum Beispiel das Schaffen und Verwalten einer Infrastruktur für die betriebsweite Anwendung asymmetrischer Verschlüsselungsverfahren).
- Ein **Risiko** (engl.: risk) ist ein Zustand oder ein Ereignis, das mit einer bestimmten Wahrscheinlichkeit eintritt und eine Gefährdung (beispielsweise eines Projekterfolgs) bedeuten könnte.
- Das **Risikomanagement** (engl.: risk management) umfasst eine große Menge von Tätigkeiten, die dazu beitragen sollen, Risiken zu erkennen, in ihrem Ausmaß abzuschätzen und deren Folgen zu vermindern.

Angriffsdefinitionen

- **Gezielter Angriff:** richtet sich gegen Personen, Unternehmen, Behörden oder Wirtschaftszweige.
  - Mittels **Spionagesoftware** wird gezielt Information „gestohlen" (Beispiel u.a. „Bundestrojaner")
  - Die Angreifer sind häufig keine Einzeltäter, sondern arbeiten im Auftrag von Organisationen (beispielsweise Geheimdiensten: Beispiel **informationstechnische Kriegsführung** (engl.: cyber warfare)).

- **Tag-Null-Angriff:** Angriff auf Rechnersysteme, der am Tag des Bekanntwerdens einer Sicherheitslücke erfolgt.
  - Oft keine Möglichkeit, Sicherheitsaktualisierungen zu installieren.

- **Seitenkanalangriff:**
  - Angriff, der auf der detaillierten Beobachtung eines Rechnersystems beruht, um Rückschlüsse auf die Rechnernutzung zu ziehen. Beispiele:
    - Stromverbrauchsschwankungen,
    - gesendete Datenpakete,
    - Zeitmessungen von Ressourcenzugriffen.

Menschliche Fehler

- Fülle von Möglichkeiten!

- Bei gezielten Angriffen: **Social Engineering**
  - Angriff, der versucht, durch gezielte Fragen die
    - Freundlichkeit,
    - Naivität oder
    - Unvorsichtigkeit von Mitarbeitern ausnutzen.
  - Ein Angreifer stellt einem Mitarbeiter gezielte Fragen, um diesem vertrauliche Information über die Sicherheitsmechanismen des Informationssystems zu entlocken.

Unbefugter Zugang oder Zugriff

- Diebstahl von Hardware
- Zerstörung von Hardware
- Unbefugter Zugriff

Schad- und Sabotageprogramme

- **Schadprogramme** (**Schadsoftware**, engl.: malicious software, malware) sind Programme, die mit der Intention geschrieben worden sind, unberechtigterweise Funktionen auf fremden Rechnern auszuführen. Die Auswirkungen dieser Programme reichen von harmlosen (aber lästigen) Bildschirmanzeigen, über das Ausspionieren von Dateninhalten und die unberechtigte Ressourcennutzung bis hin zu vollständigem Programm- und Datenverlust oder Unbenutzbarkeit eines Rechners. Schadprogramme werden entweder passiv über Wechseldatenträger und/oder Rechnernetze verbreitet oder können sich vielfach auch selbstständig vervielfältigen (replizieren).
- Drei Arten:
  - Virenprogramme
  - Wurmprogramme
  - Trojanische Pferde

Maßnahmen gegen Schadsoftware

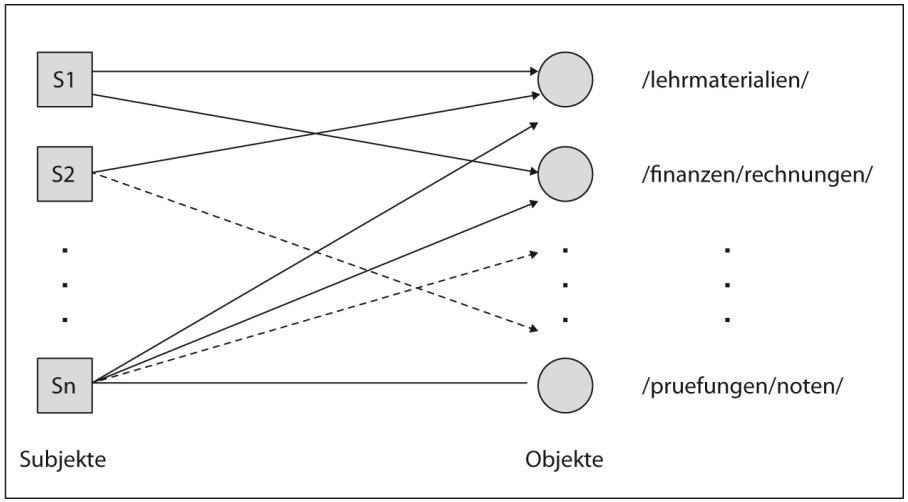
- Schutz eines Rechners oder Netzwerks gegen Angriffe
- Erkennen von Schadsoftware
- Schadensreduktion
- Beseitigen von Schadsoftware

Rechteverwaltung

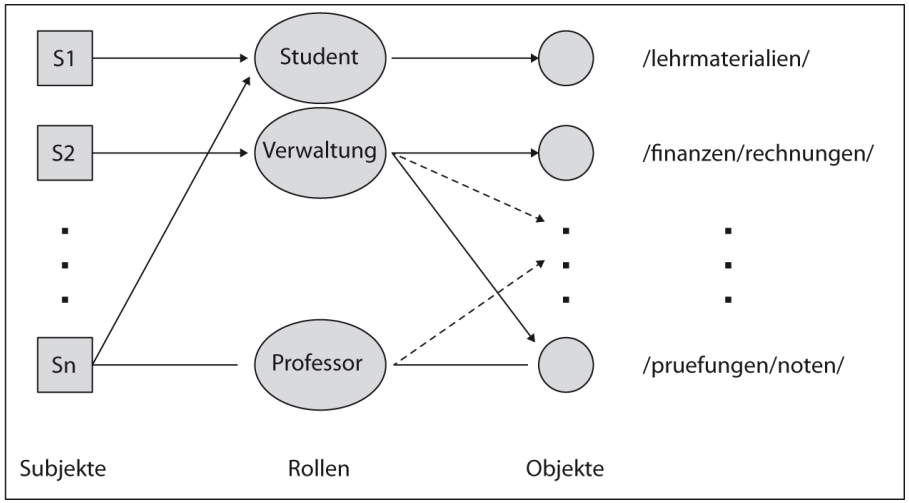
- Das Modell der **wahlfreien** oder **diskreten Zugriffskontrolle** (engl.: discretionary access control, Abkürzung: DAC) beruht auf der Annahme, dass der Eigentümer eines Objekts für dessen Schutz alleine verantwortlich ist. Der Eigentümer hat die „freie Wahl", wer (aktive Komponente, Subjekt) auf seine Objekte (passive Komponente) in welcher Weise (Operation) zugreifen darf.
- Die **zentralistisch verpflichtende Zugriffskontrolle** (engl.: mandatory access control, Abkürzung: MAC) ist auf die Steuerung des *Informationsflusses* ausgelegt. Das Verfahren basiert auf einer Klassifikation (Einstufung) der Subjekte und Objekte eines Systems. Hierzu erhalten die *Subjekte* (die Benutzer) und *Objekte* des Systems (Daten und Programme) jeweils eine **Sicherheitsmarkierung** (engl.: security label) zugewiesen, anhand derer entschieden wird, ob ein Informationsfluss zwischen einem Subjekt und einem Objekt (beziehungsweise zwischen zwei Subjekten) stattfinden darf.
- Bei der **rollenbasierten Zugriffskontrolle** (engl.: role-based access control, Abkürzung: RBAC) werden die Zugriffsrechte nicht an Subjekte (beispielsweise Benutzer), sondern an *Rollen* vergeben. In einem getrennten Schritt werden Benutzern diese Rollen gemäß ihren Aufgabenprofilen zugeordnet, wodurch diese implizit die Zugriffsrechte ihrer jeweiligen Rollen erhalten.

Wahlfreie Zugriffskontrolle (a) vs. rollenbasierte Zugriffskontrolle (b)

a)



b)



9.5 Umgang mit sensiblen Daten (Datenschutz)

Datenschutz

- Als **Datenschutz** (engl.: data privacy; protection of data privacy) bezeichnet man die Gesamtheit der gesetzlichen Regelungen und betrieblichen Maßnahmen zum Schutz der informationellen Selbstbestimmung von Personen und zur Sicherheit des Informationshaushalts.
- Das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** (Abkürzung: **IT-Grundrecht**) ist ein in Deutschland vom Bundesverfassungsgericht als Ausprägung des allgemeinen Persönlichkeitsrechts formuliertes Grundrecht zum Schutz personenbezogener Daten. Es ist bei Systemen anzuwenden, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.

Online-Durchsuchung

- Unter einer **Online-Durchsuchung** (engl.: online search with spyware) versteht man einen heimlichen Zugriff staatlicher Organe auf fremde Rechner über Netzwerke. Zwecke sind die Strafverfolgung, die polizeiliche Gefahrenabwehr und die nachrichtendienstliche Informationsbeschaffung. Bei der **Quellen-TKÜ** (Abkürzung von Quellentelekommunikationsüberwachung; engl.: source telecommunication surveillance) schneidet eingeschleuste Software zu überwachende (etwa WhatsApp- oder Skype-)Kommunikation vor deren Verschlüsselung mit und übermittelt sie an Ermittlungsbehörden. Anders als bei der Online-Durchsuchung werden bei der Quellen-TKÜ keine weiteren Daten erhoben. Beide Maßnahmen stehen in einem Spannungsverhältnis zur staatlichen Aufgabe der Gewährleistung von IT-Sicherheit und werden unter dem Gesichtspunkt der Verhältnismäßigkeit kontrovers diskutiert.

Rechtliche Grundlagen

- Seit dem 25. Mai 2018 bildet die **Datenschutzgrundverordnung** (DSGVO; engl.: General Data Protection Regulation, GDPR) gemeinsam mit der den Datenschutz im Bereich der Strafverfolgung harmonisierenden **JI-Richtlinie** (Datenschutzrichtlinie im Bereich von Justiz und Inneres) den rechtlichen Rahmen für den Schutz personenbezogener Daten natürlicher Personen in der Europäischen Union.
- Die in allen Mitgliedstaaten unmittelbar anwendbare DSGVO enthält allerdings Öffnungsklauseln, die es den nationalen Gesetzgebern gestatten, bestimmte Aspekte des Datenschutzes selbstständig zu regeln. Davon abgesehen dürfen die Bestimmungen der DSGVO, die im Übrigen auch für außereuropäische Unternehmen relevant sind, wenn sie Waren oder Dienstleistungen auf dem europäischen Binnenmarkt anbieten oder EU-Bürger überwachen, auf nationaler Ebene weder abgeschwächt noch verstärkt werden.
- Durch die Rechtsvereinheitlichung soll der europäische Datenschutz nicht zuletzt im Hinblick auf die Herausforderungen durch Globalisierung und Plattformwirtschaft gestärkt werden. Insbesondere zur Nutzung des durch die Öffnungsklauseln der DSGVO gebotenen Spielraums und zur Umsetzung der JI-Richtlinie gibt es allerdings weiterhin **nationale Datenschutzgesetze,** etwa das neu gefasste Bundesdatenschutzgesetz (BDSG) in Deutschland und das neu erlassene Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) in Österreich.

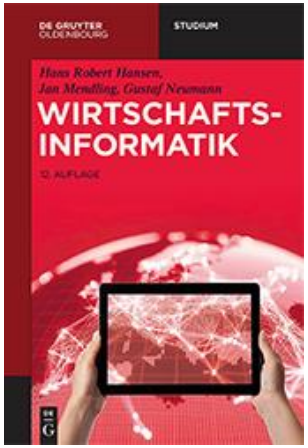
Grundsätze gem. Art. 5 DSGVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Die wichtigsten Punkte

1. Durch die *zunehmende Vernetzung von betrieblichen Informationssystemen* eröffnen sich neben den positiven Effekten auch vermehrt Angriffsziele und Risiken sowohl für den Betreiber als auch den Nutzer der Informationssysteme.
2. Um den *möglichen Bedrohungen zu begegnen*, müssen sowohl die *Sicherheitsziele* (und damit verbunden die Bedrohungen), als auch die möglichen *Maßnahmen* zu Erreichung dieser Ziele bekannt sein.
3. Die *Maßnahmen zur Erreichung der Sicherheitsziele* umfassen technische Verfahren, organisatorische Strukturen und juristische Regelungen (Gesetze). Viele der technischen Verfahren zur Erreichung der Sicherheitsziele haben eine lange, teils militärische Vergangenheit.
4. Zu den *potenziellen Angreifern* gehören neben Individuen (Hacker) vermehrt hochspezialisierte Organisationen (Betreiber von Botnetzen oder professionelle Industriespionage) und Geheimdienste (informationstechnische Kriegsführung).
5. Mithilfe von kryptografischen Verfahren eröffnen sich zunehmend mehr Möglichkeiten zur Absicherung der digitalen Kommunikation, wodurch beispielsweise die Automatisierung komplexer Geschäftstransaktionen oder digitale Währungssysteme möglich werden.
6. Den Interessen der Betreiber von Informationssystemen stehen häufig die Interessen und Rechte der Benutzer gegenüber. Der Schutz der Privatsphäre manifestiert sich unter anderem in den gesetzlichen Regelungen bezüglich des Umgangs mit personenbezogenen Daten. Gleichzeitig stehen die Rechte auf Privatsphäre den Aufgaben der Exekutive gegenüber, wodurch mancherorts die staatliche Datensammelwut gerechtfertigt wird.

Online-Materialien



Übungs- und Lehrmaterialien zu diesem Kapitel finden Sie im Web über den abgebildeten QR-Code. Richten Sie Ihre Smartphone- oder Tablet-Kamera auf das nebenstehende Bild, um zu den Inhalten zu gelangen.