DHBW Stuttgart

Technik der digitalen Netze
Teil 3 – Sicherheit

Stephan Rupp

Nachrichtentechnik

www.dhbw-stuttgart.de

Inhalt

DHBW Stuttgart

Sicherheit

- Begriffe: Vertraulichkeit, Integrität, Verfügbarkeit
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit
- Hochverfügbare Systeme

Sichere Systeme – ganz abstrakt

DHBW Stuttgart

Vertraulichkeit (Confidentiality):

- Information sollte nicht unerwünscht an Dritte gelangen (z.B. Fernmeldegeheimnis, Schutz personenbezogener Daten, firmenvertrauliche Daten)
- Angriffe: Mithören, „Datendiebstahl“
- Lösungen: Zugangskontrolle, Authentisierung, Autorisierung, Verschlüsselung

Integrität (Integrity):

- Unversehrtheit
- Information sollte nicht verfälscht sein
- Angriffe: Identitätsdiebstahl; manipulierte Daten
- Lösungen: Prüfsummen, Signatur

DHBW Stuttgart

Verfügbarkeit (Availability):

- Anwendungen bzw. Dienste sollten für autorisierte Nutzer jederzeit verfügbar sein
- Angriffe auf die Systemverfügbarkeit müssen verhindert oder abgewehrt können (Lastabwehr, Denial of Service, schädliche Software)
- Nicht jede Software ist vertrauenswürdig!
- Lösungen: Redundanz, Kapselung und Sicherheitsmodell (Rollen, Rechte und Pflichten definieren, umsetzen und einfordern)

CIA

(für die Fans von Eselsbrücken)

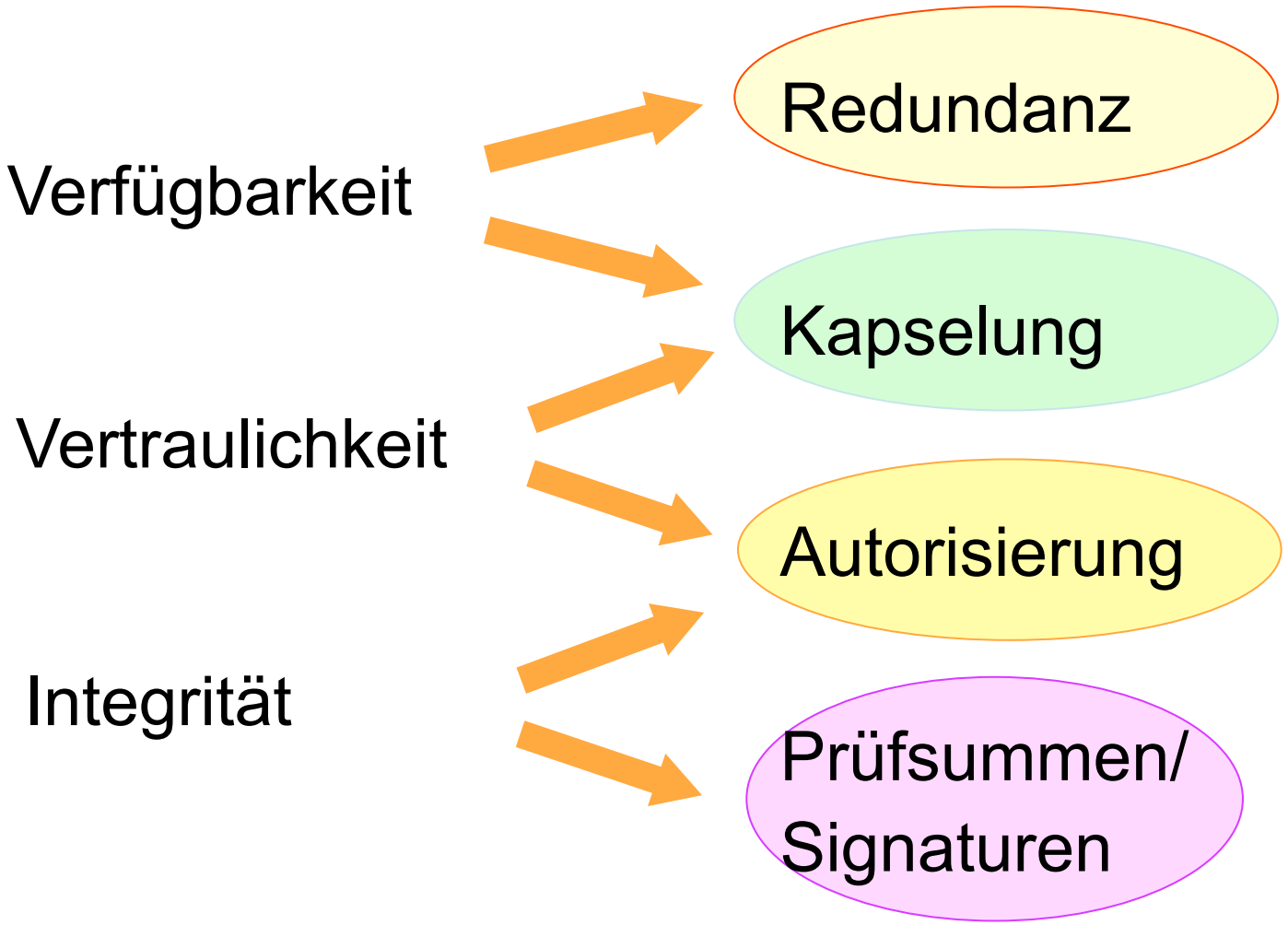
Englisch - Deutsch

Security = Sicherheit

Safety = funktionale Sicherheit

Sicherheitskonzepte

DHBW Stuttgart



Was ist Kapselung (Encapsulation)?

DHBW Stuttgart

Bob in einer unsicheren Umgebung

Alice in einer sicheren Umgebung

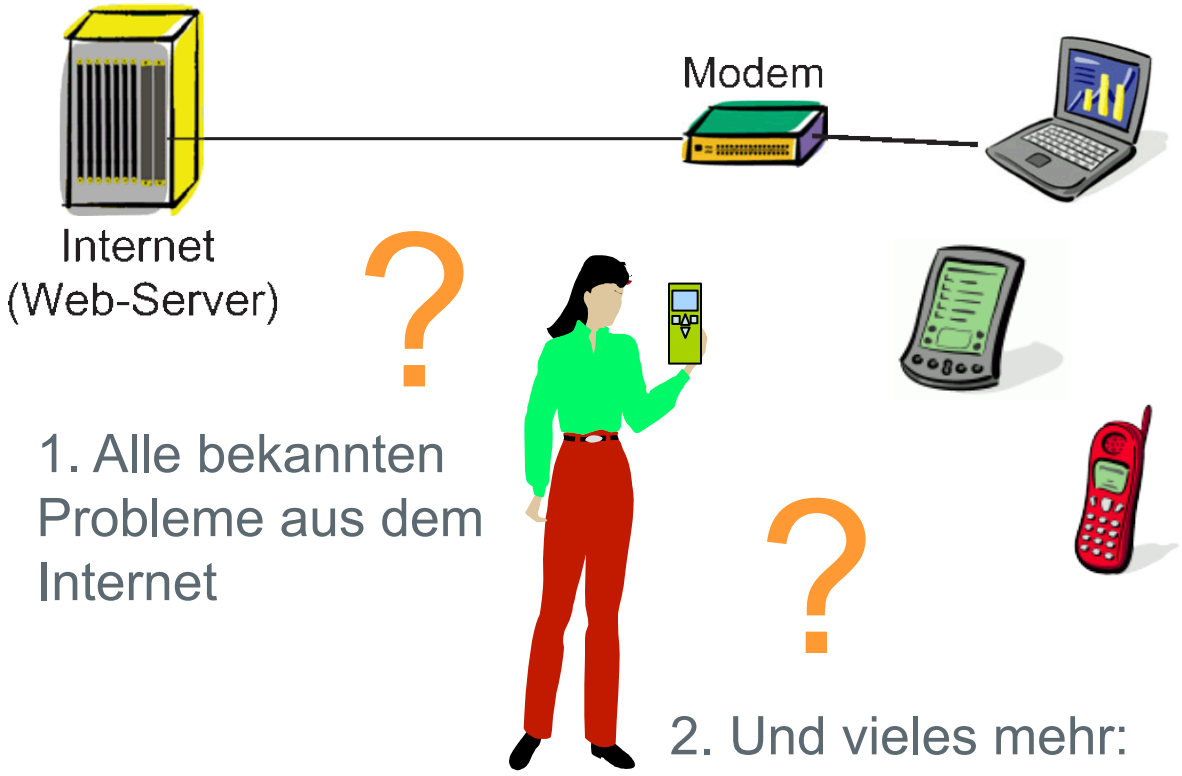
Inhalt

DHBW Stuttgart

Sicherheit

- Begriffe: Vertraulichkeit, Integrität, Verfügbarkeit
- Bedrohungen: Risiken und Nebenwirkungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit
- Hochverfügbare Systeme

Die Probleme wandern mit.



1. Alle bekannten Probleme aus dem Internet

2. Und vieles mehr:
- Bewegungsprofile
- persönliche Daten
- neue Verbreitungsmöglichkeiten für Schädlinge

Schreibtisch

(zuhause oder im Geschäft)

Mobile Dienste: unterwegs und überall dabei

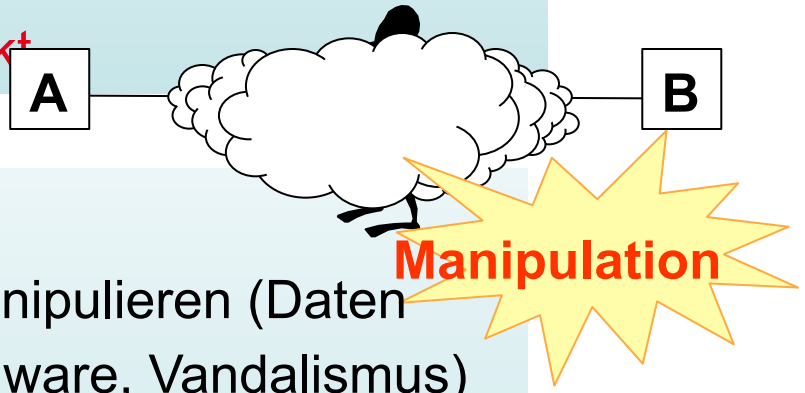
Was kann mir passieren?

DHBW Stuttgart

Passive Angriffe

- Mithören
- Passwörter ausspionieren
- Datenklau
- Identitätsdiebstahl
- Verhaltenmuster und Nutzerprofile erstellen
- bleiben völlig unbemerkt

Funktechnologien sind leicht zu belauschen!



Aktive Angriffe

- Eingriff in die Kommunikation
- Manipulation von Daten
- Verbindung entführen
- Boykott (Denial of Service)
- Geräte manipulieren (Daten stehlen, Malware, Vandalismus)
- mit falscher Identität agieren
- Übertölpeln von Nutzern (z.B. Passwörter stehlen)

Inhalt

DHBW Stuttgart

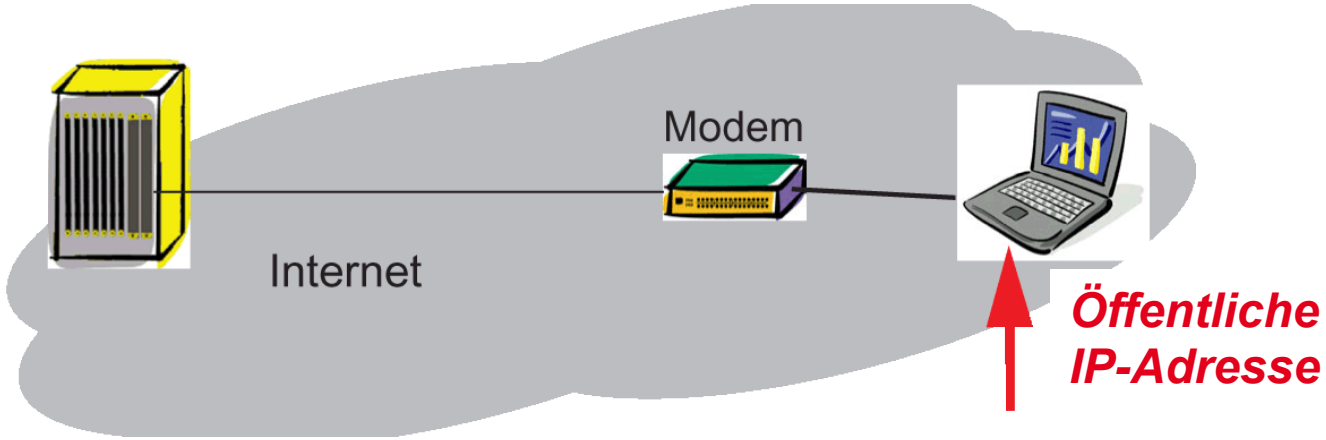
Sicherheit

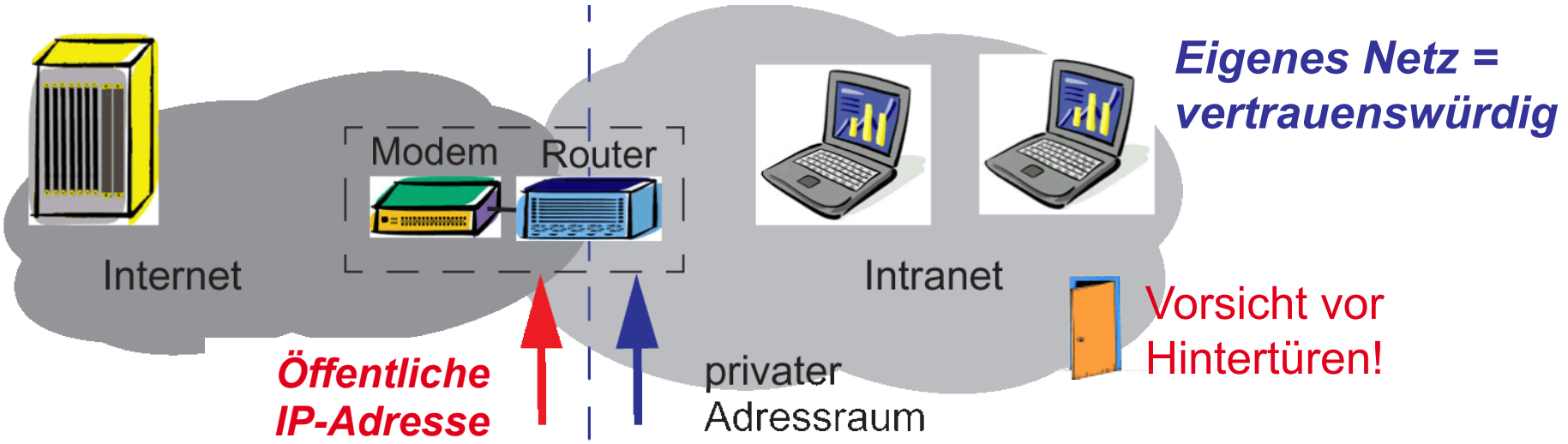
- Begriffe
- Bedrohungen
- Schutzmaßnahmen: Verhaltensregeln, die eigenen 4 Wände, der Vorraum
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit, Hochverfügbare Systeme

Verhaltensregeln

DHBW Stuttgart

Öffentliches oder fremdes Netz = nicht vertrauens-würdig





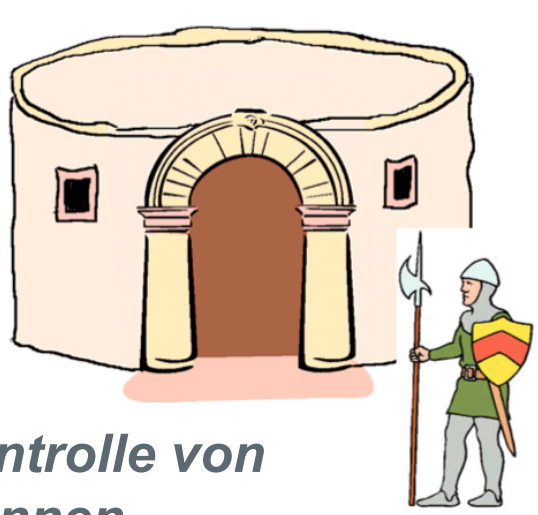
Eigenes Netz = vertrauenswürdig

Vorsicht vor Hintertüren!

Die eigenen 4 Wände

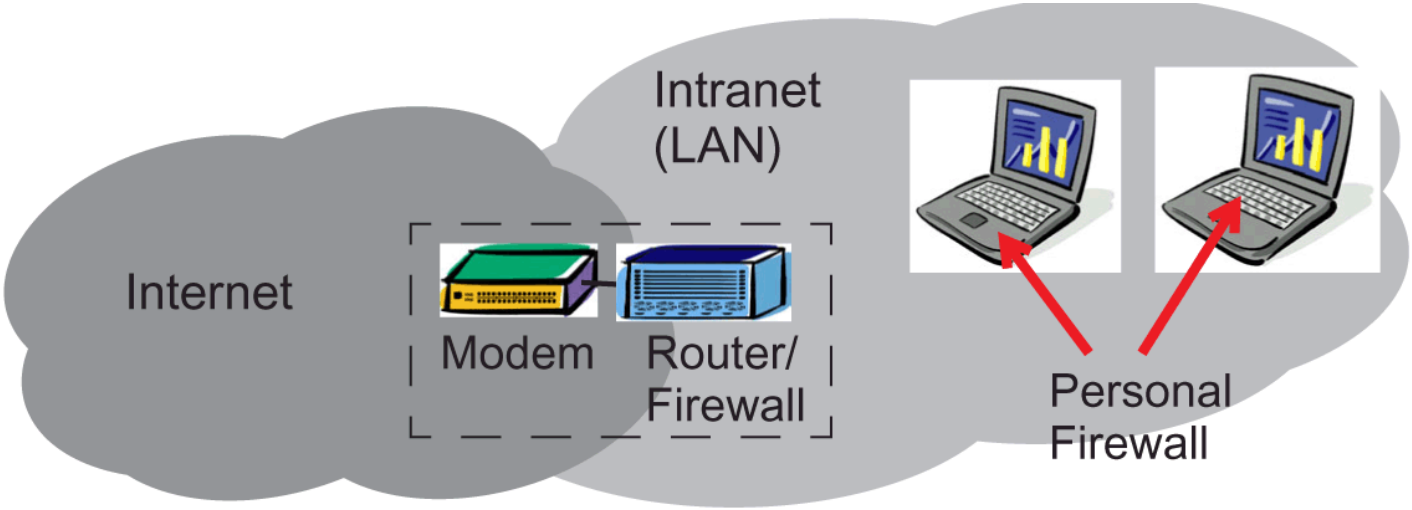
DHBW Stuttgart

Stadttor



= Zugangskontrolle von Aussen und Innen

Firewall

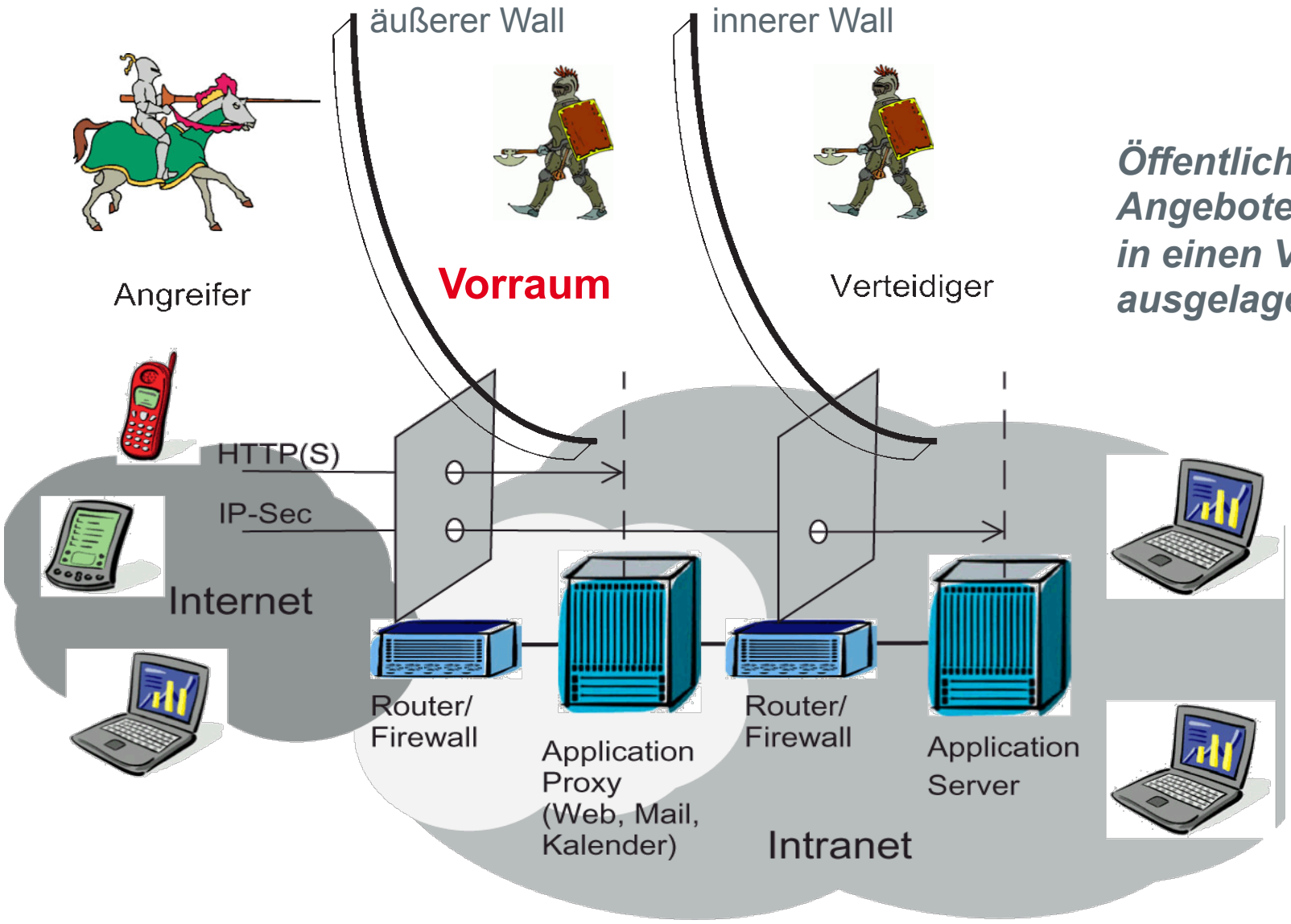


Mehrstufige Kapselung

Vorraum: Marktplatz und Lobby

Burg Falkenstein, Luftbild von Westen

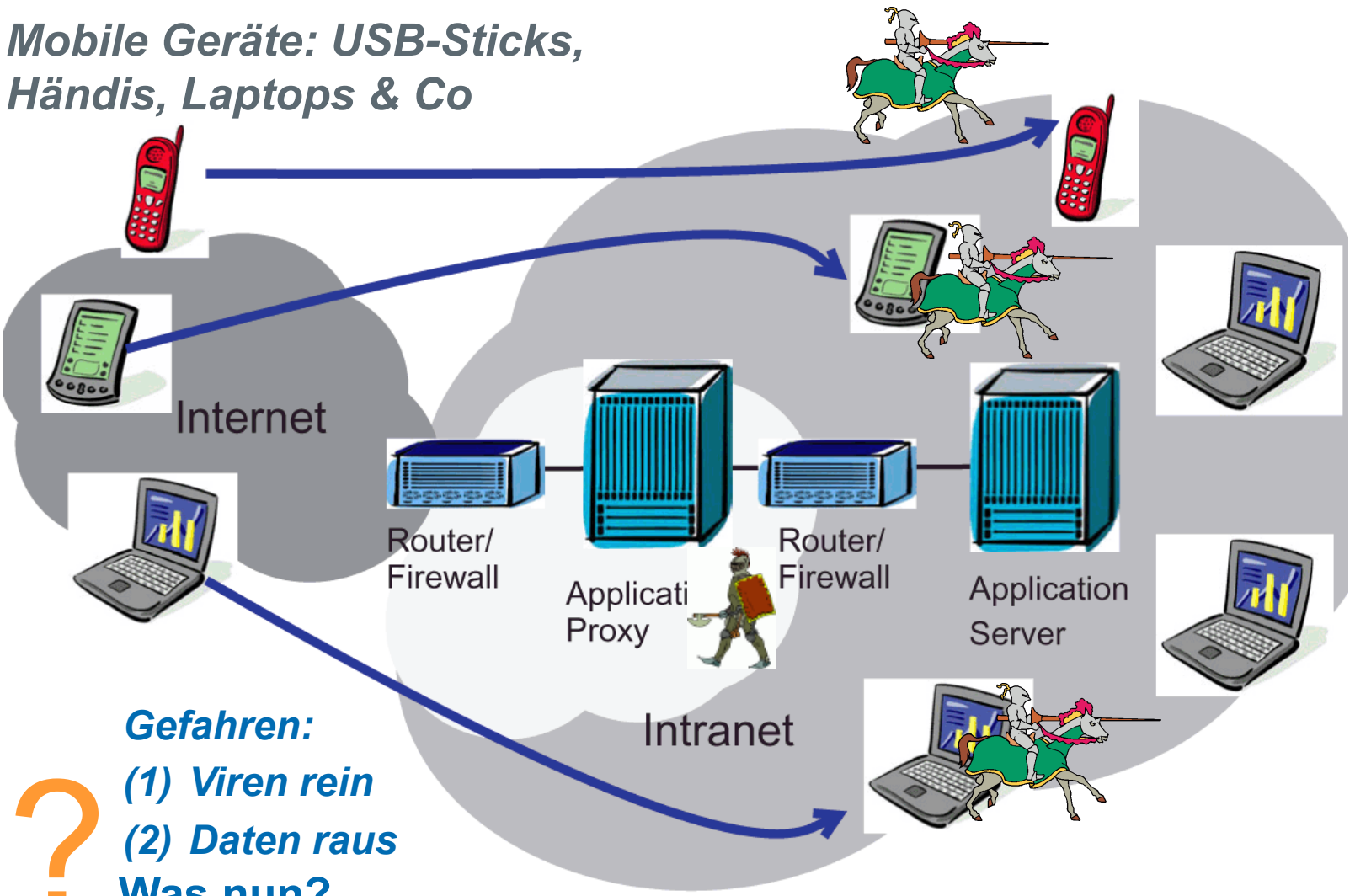
Vorraum



Öffentliche Angebote werden in einen Vorraum ausgelagert

An der Firewall vorbei ins Intranet

DHBW Stuttgart



Inhalt

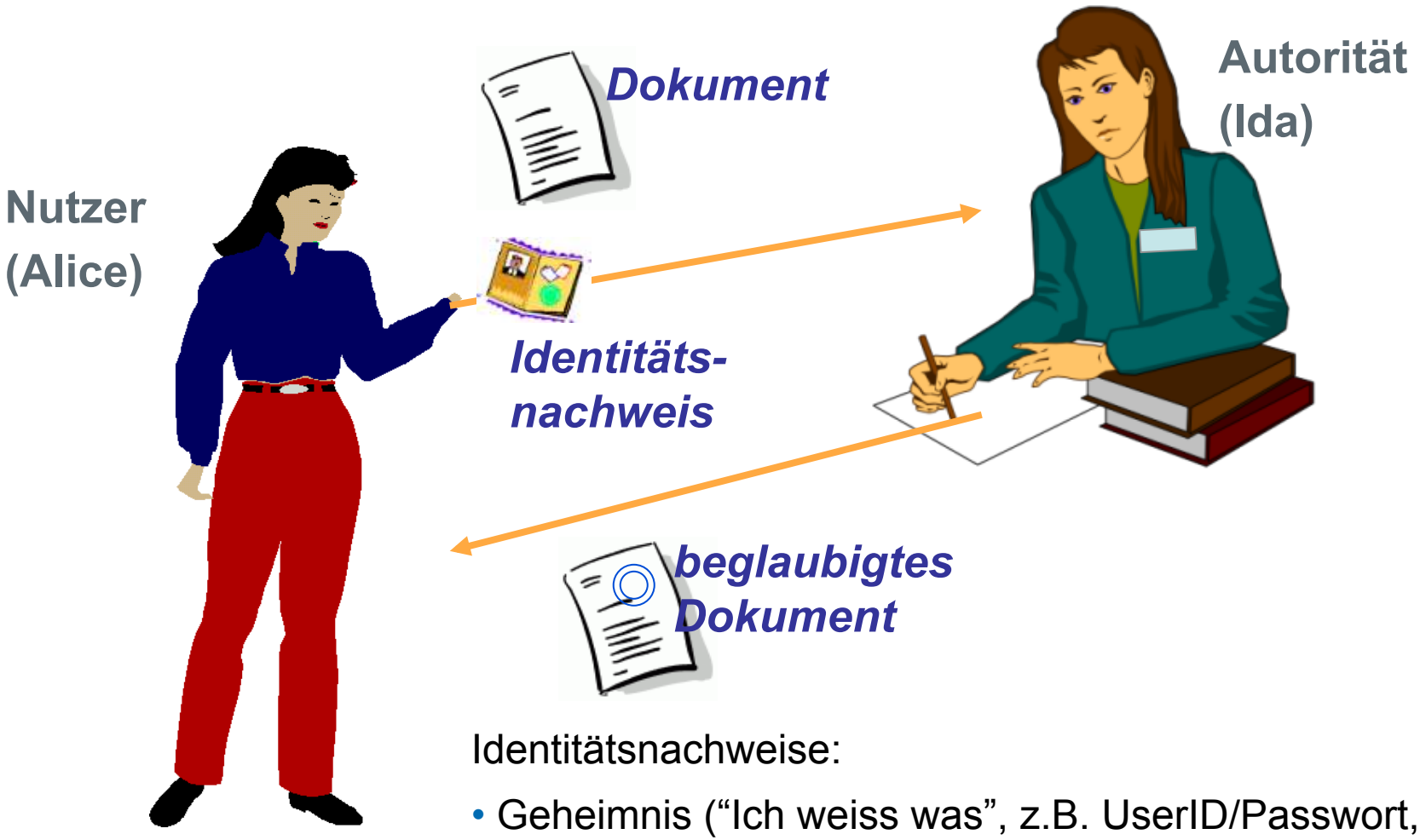
DHBW Stuttgart

Sicherheit

- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise: Authentisierung, Zertifikate, Signaturen
- Geheimniskrämerei
- Verfügbarkeit, Hochverfügbare Systeme

Identitätsnachweis, Ursprungsnachweis

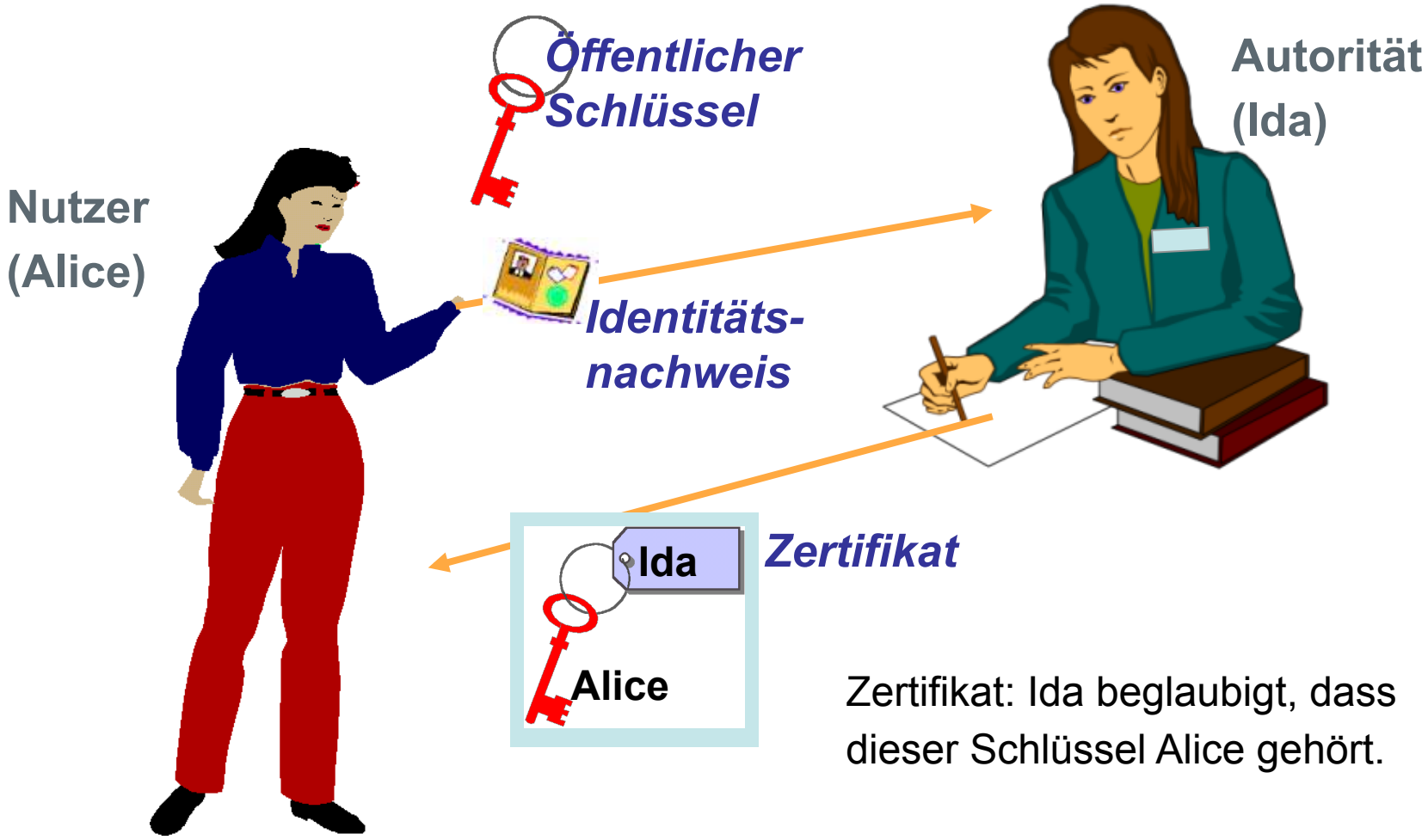
DHBW Stuttgart



Identitätsnachweise:

- Geheimnis (“Ich weiss was”, z.B. UserID/Passwort, ...)
- Token (“Ich hab was”, z.B. Ausweis, Chipkarte, ...)
- Biometrische Merkmale (“ich bins”)

Zertifikate



Zertifikat: Ida beglaubigt, dass dieser Schlüssel Alice gehört.

Nutzung von Zertifikaten

DHBW Stuttgart

Ursprungsnachweise für

- Dokumente (digitale Signatur, verschlüsselte Dokumente)
- Software aus vertrauenswürdigen Quellen
- signierte E-Mail (Vermeidung von Spam und Manipulation)

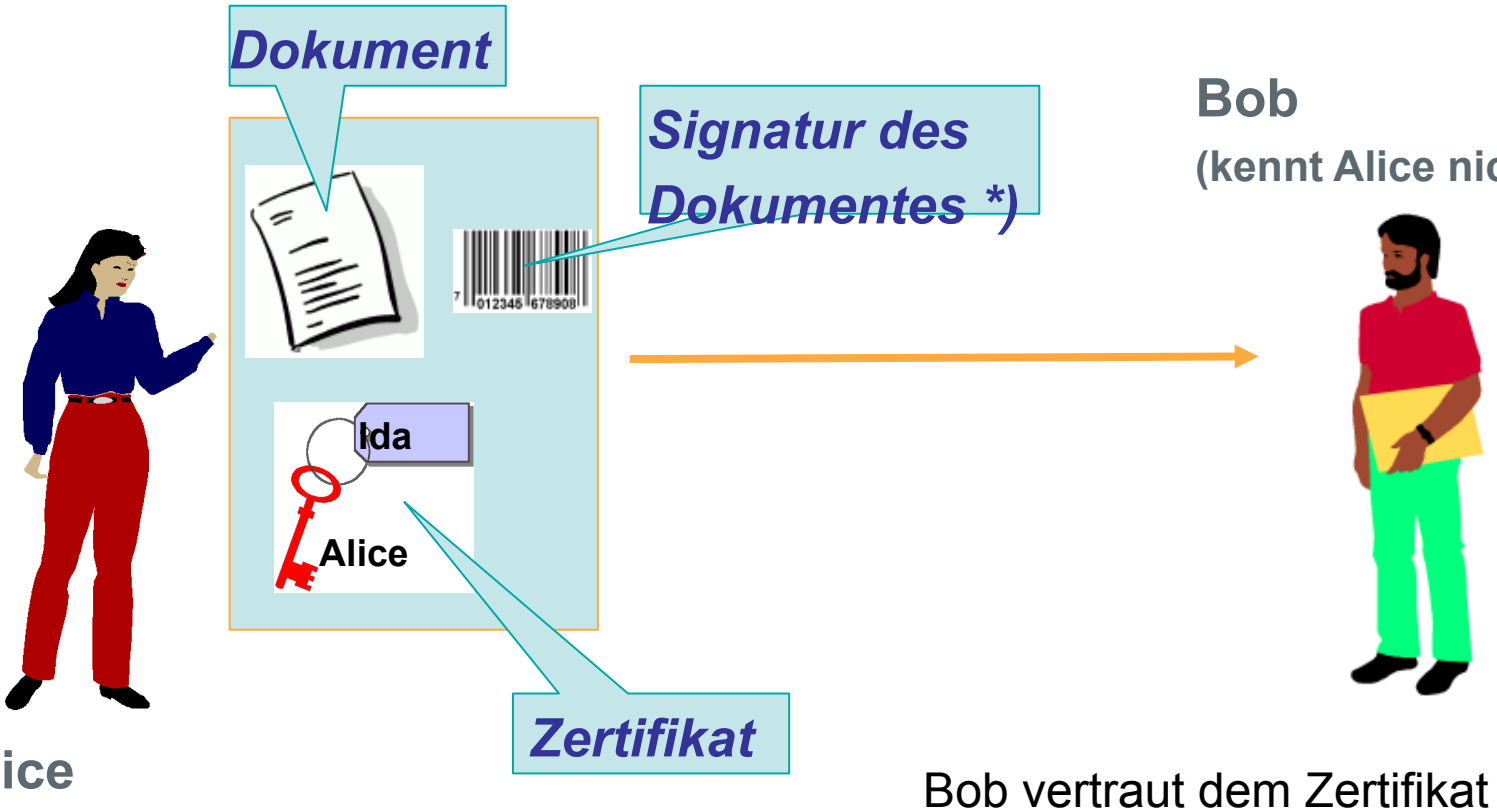
Aufbau verschlüsselter Verbindungen

- z.B. für Secure Socket Verbindungen (https, SSL)

Identitätsnachweise für

- Server bzw. Clients für verschlüsselte Verbindungen
- RAS Token (Shared Key im Token)
- SIM-Karten, Kabelmodems (personalisierte Auslieferung)

Ursprungsnachweis für Dokumente

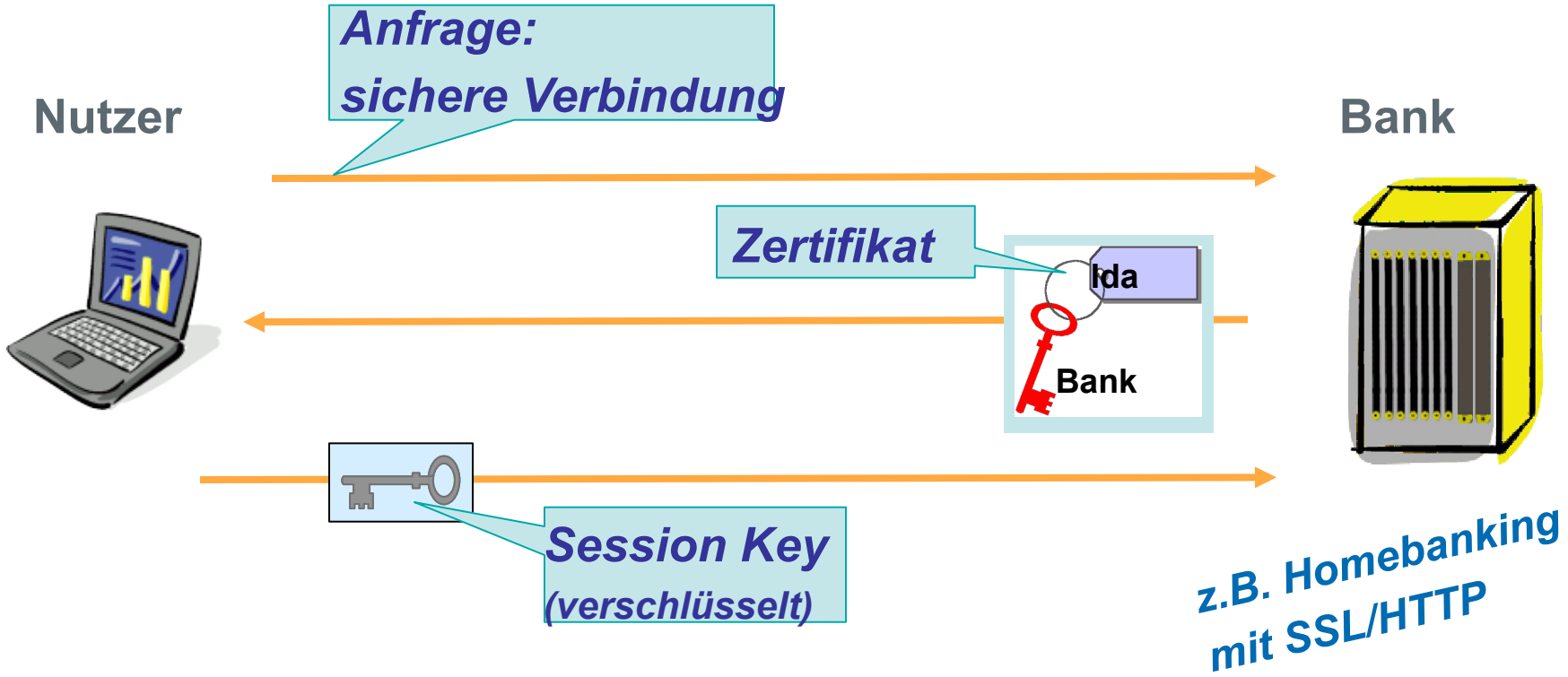


*) Signatur: mit dem privaten Schlüssel von Alice verschlüsselte Prüfsumme des Dokumentes

Bob vertraut dem Zertifikat von Ida und kann prüfen, dass:

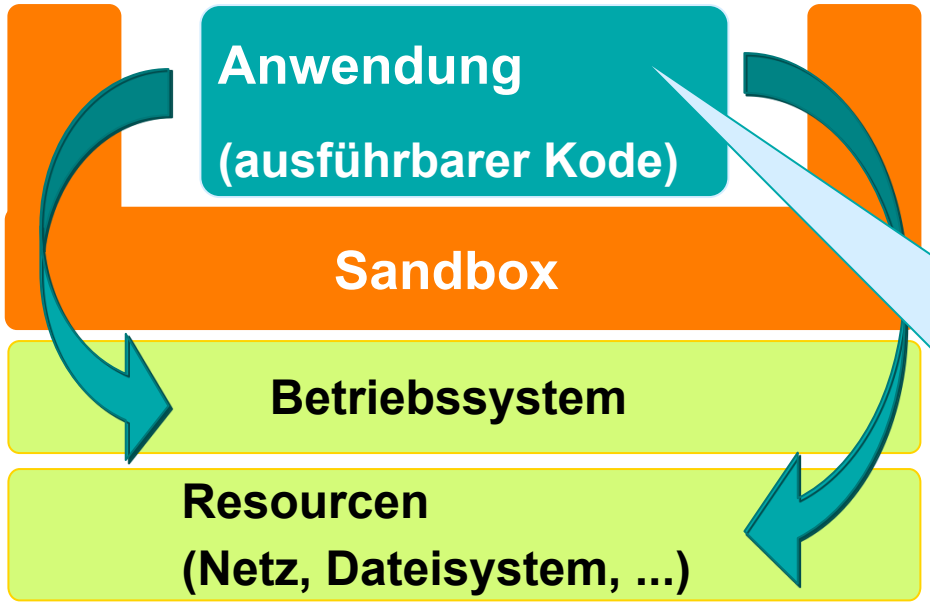
- das Dokument von Alice stammt
- das Dokument nicht manipuliert wurde

Aufbau verschlüsselter Verbindungen



Der Nutzer entnimmt dem Zertifikat den öffentlichen Schlüssel der Bank. Mit dem öffentlichen Schlüssel verschlüsselt er einen symetrischen Session Key, den er der Bank übermittelt. Der Session Key wird nun für den Austausch verschlüsselter Dokumente verwendet.

Kapselung von Software



Nur vertrauenswürdige Anwendungen erhalten Zugriff auf das System und seine Resourcen.

Vertrauensbeweis durch ein Zertifikat:

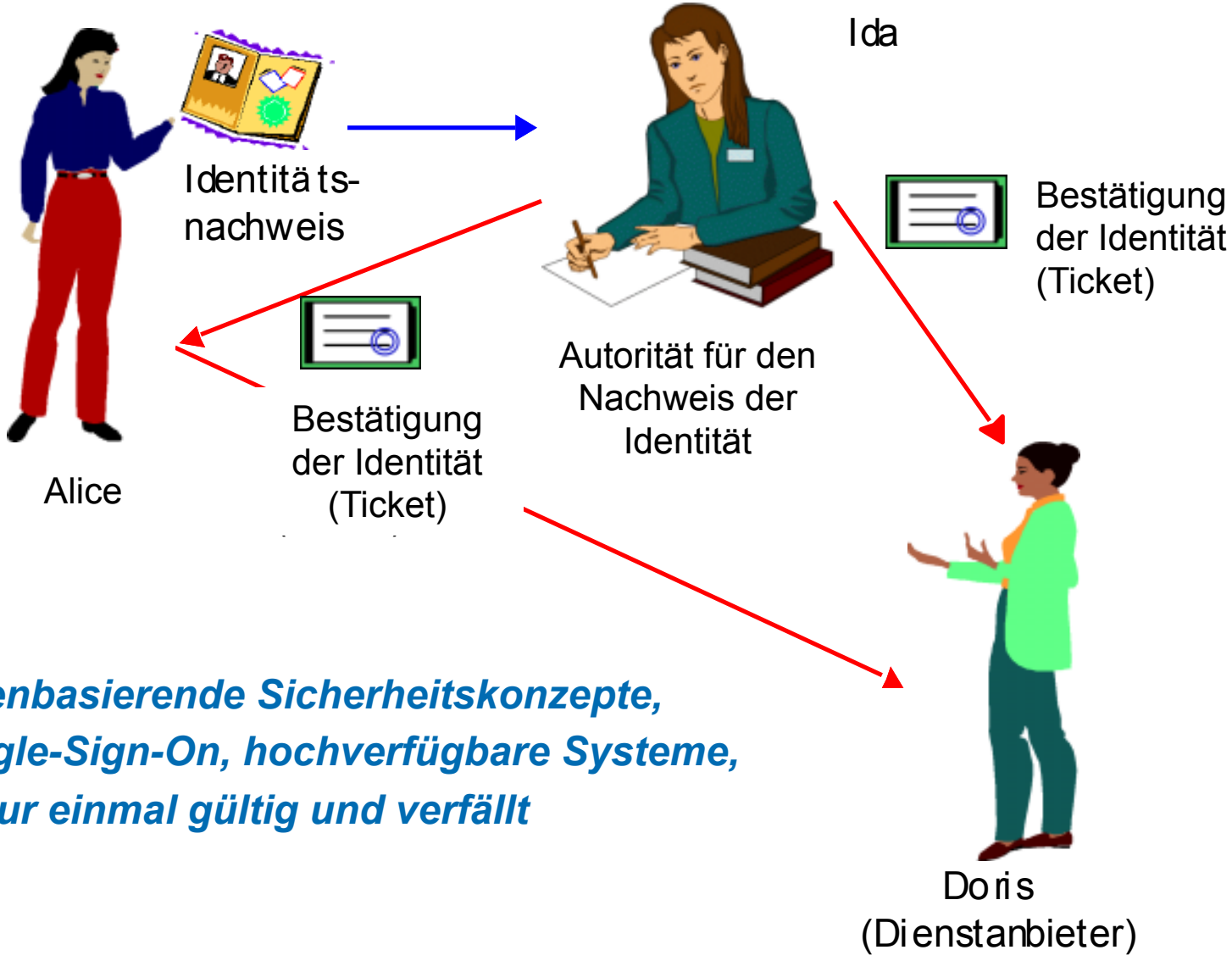
- Software stammt aus einer vertrauenswürdigen Quelle
- Software wurde nicht manipuliert.

?

Signierte Trojaner?

Tickets bzw. Token als Eintrittskarte

DHBW Stuttgart



Für rollenbasierende Sicherheitskonzepte,
z.B. Single-Sign-On, hochverfügbare Systeme,
Ticket nur einmal gültig und verfällt

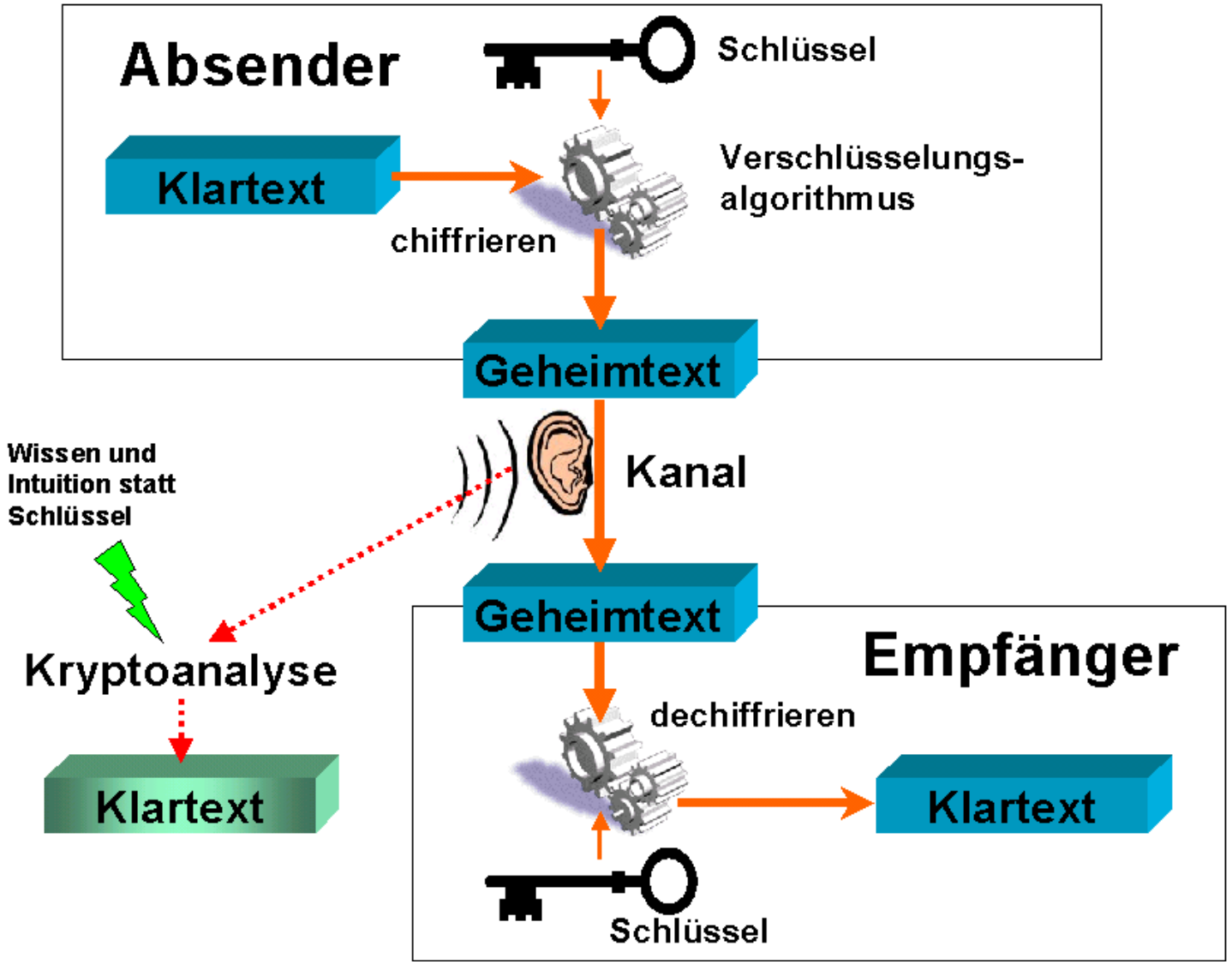
Inhalt

DHBW Stuttgart

Sicherheit

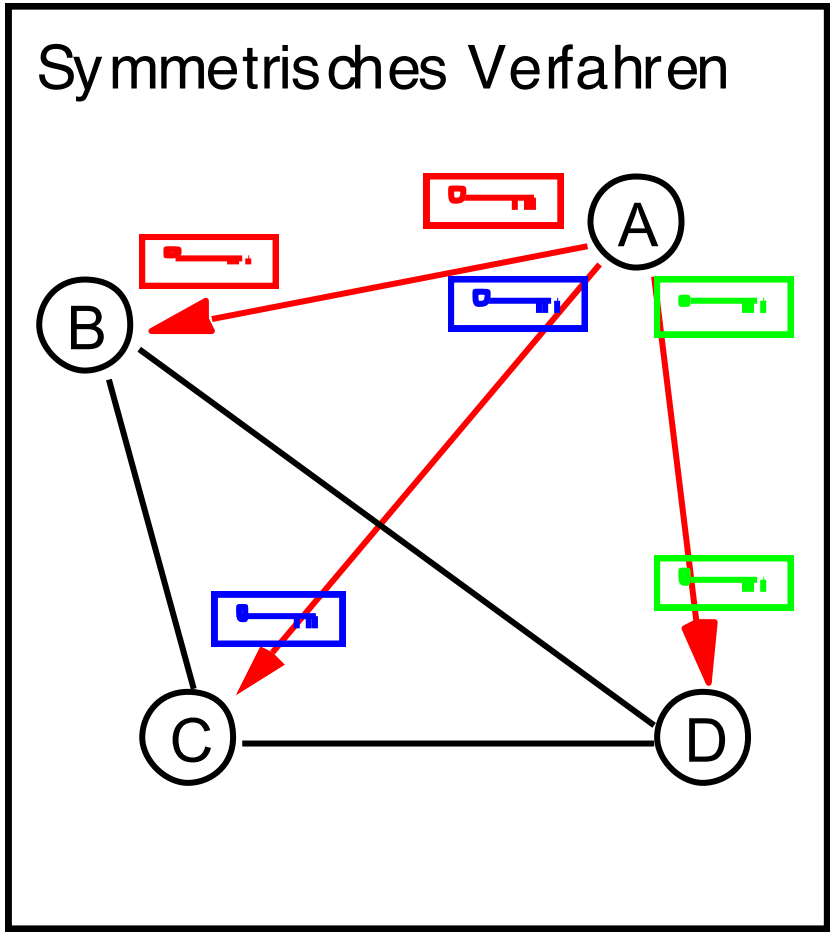
- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei: Verschlüsselung symmetrisch und asymmetrisch, Hashfunktionen
- Verfügbarkeit, Hochverfügbare Systeme

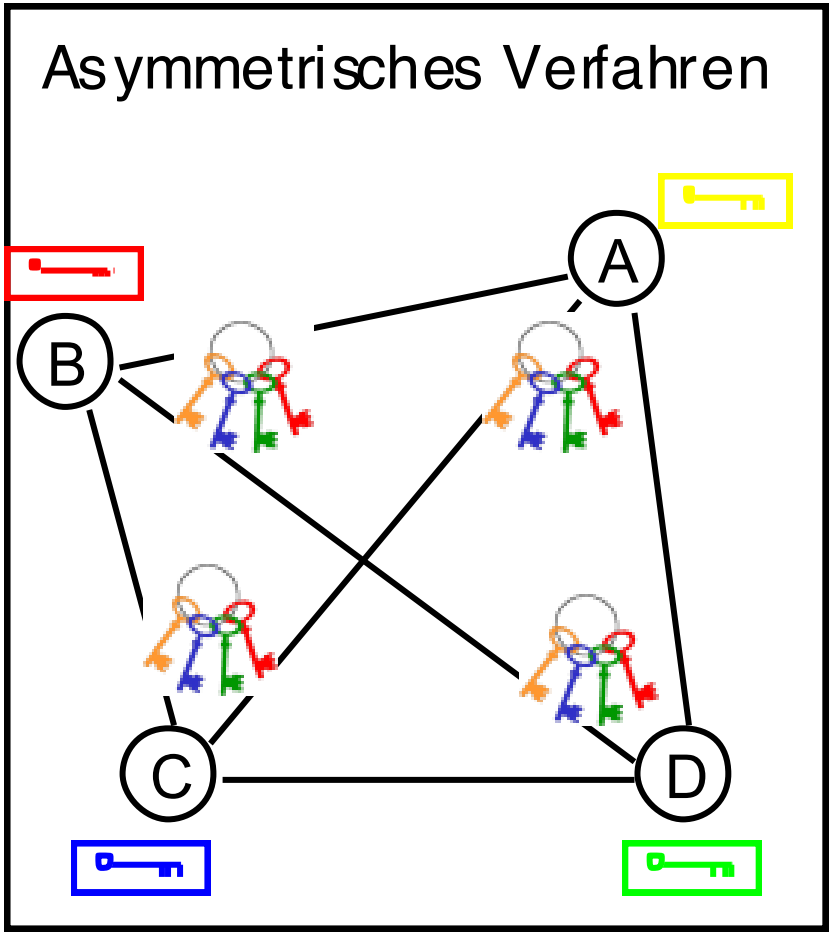
Verschlüsselung und Entschlüsselung



Schlüssel und Schlüsselpaare

DHBW Stuttgart

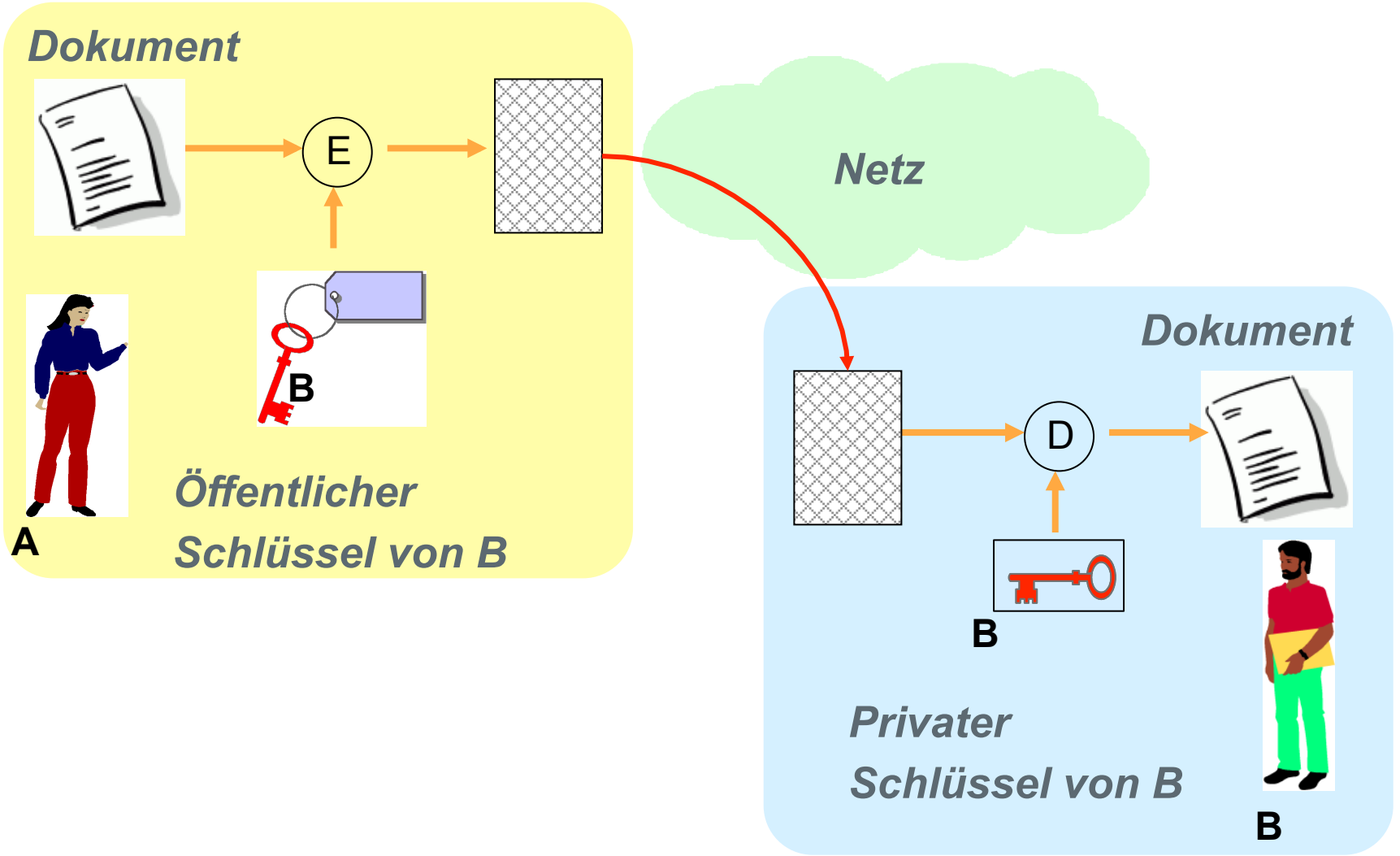




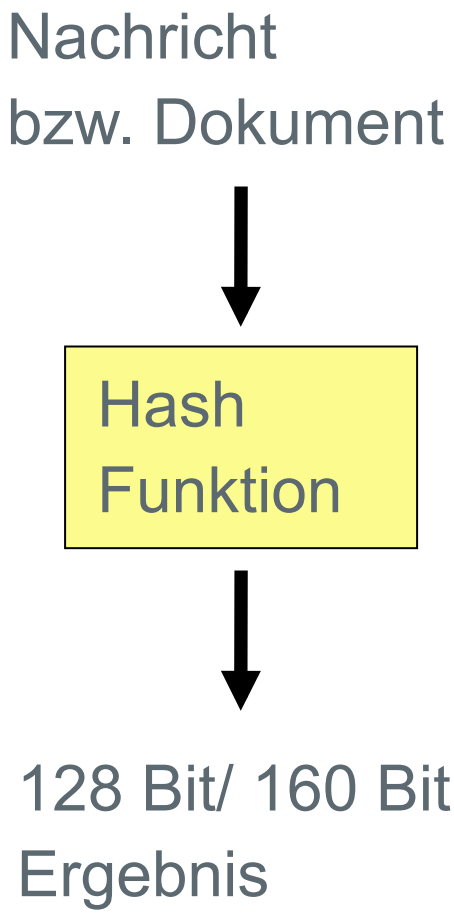
Schnelle Verfahren, aber Verteilung der Schlüssel problematisch

Langsam, aber Schlüsselverteilung gelöst

Asymetrische Verschlüsselung



Hash-Funktion als Prüfsumme



Hashfunktion (auch *message digest*):

- generiert eine Prüfsumme fixer Länge,
- aus der das Eingangsdokument nicht rekonstruierbar ist und
- die sich bei kleinsten Änderungen im Eingangsdokument ändert.

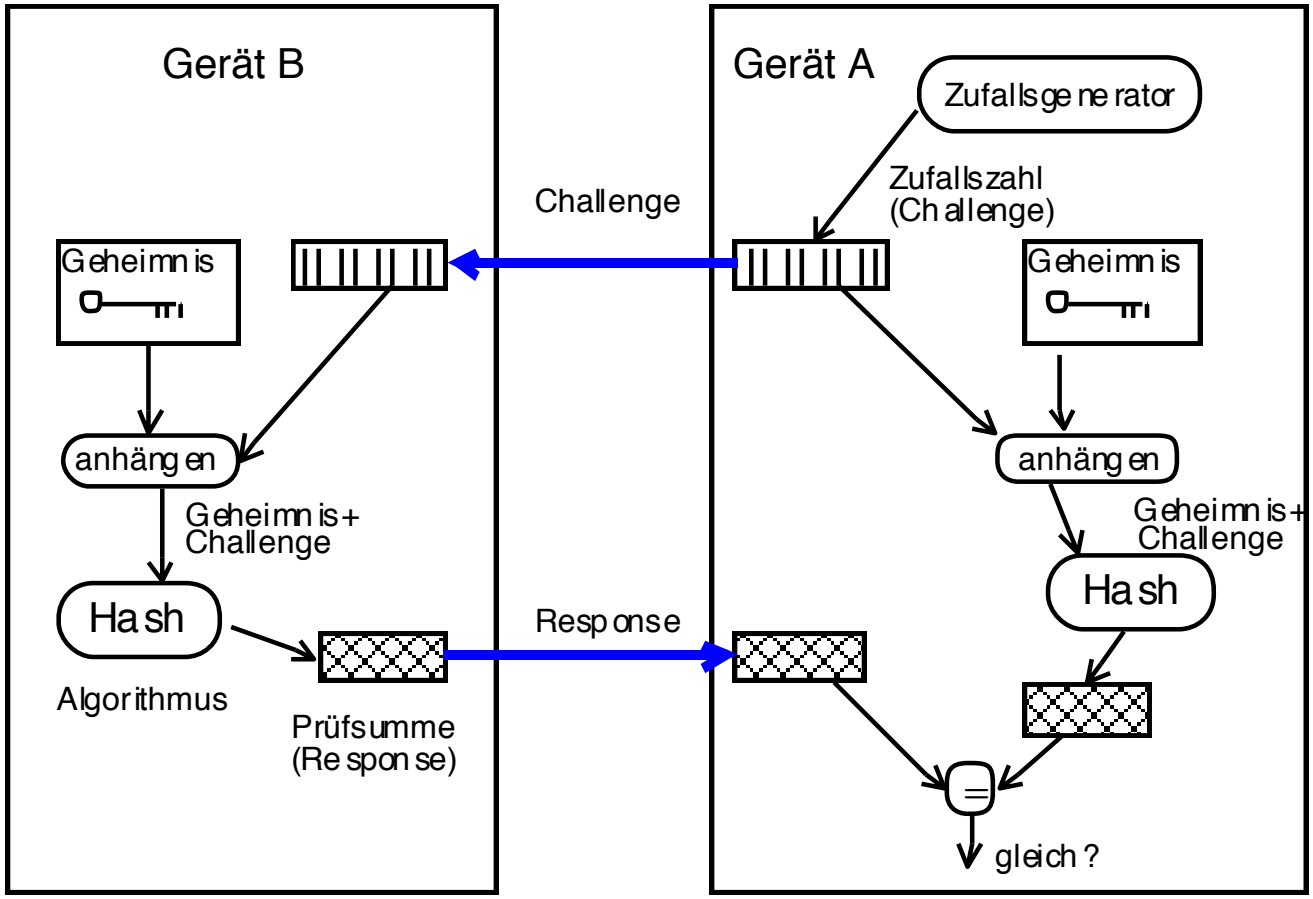
Prüfsumme (*hash*) lässt sich als Integritätsnachweis für Nachrichten und Dokumente verwenden, sowie in Kombination mit einem privaten Schlüssel als Ursprungsnachweis (z.B. Signatur bzw. message authentication codes).

DHBW Stuttgart

Gymnastik

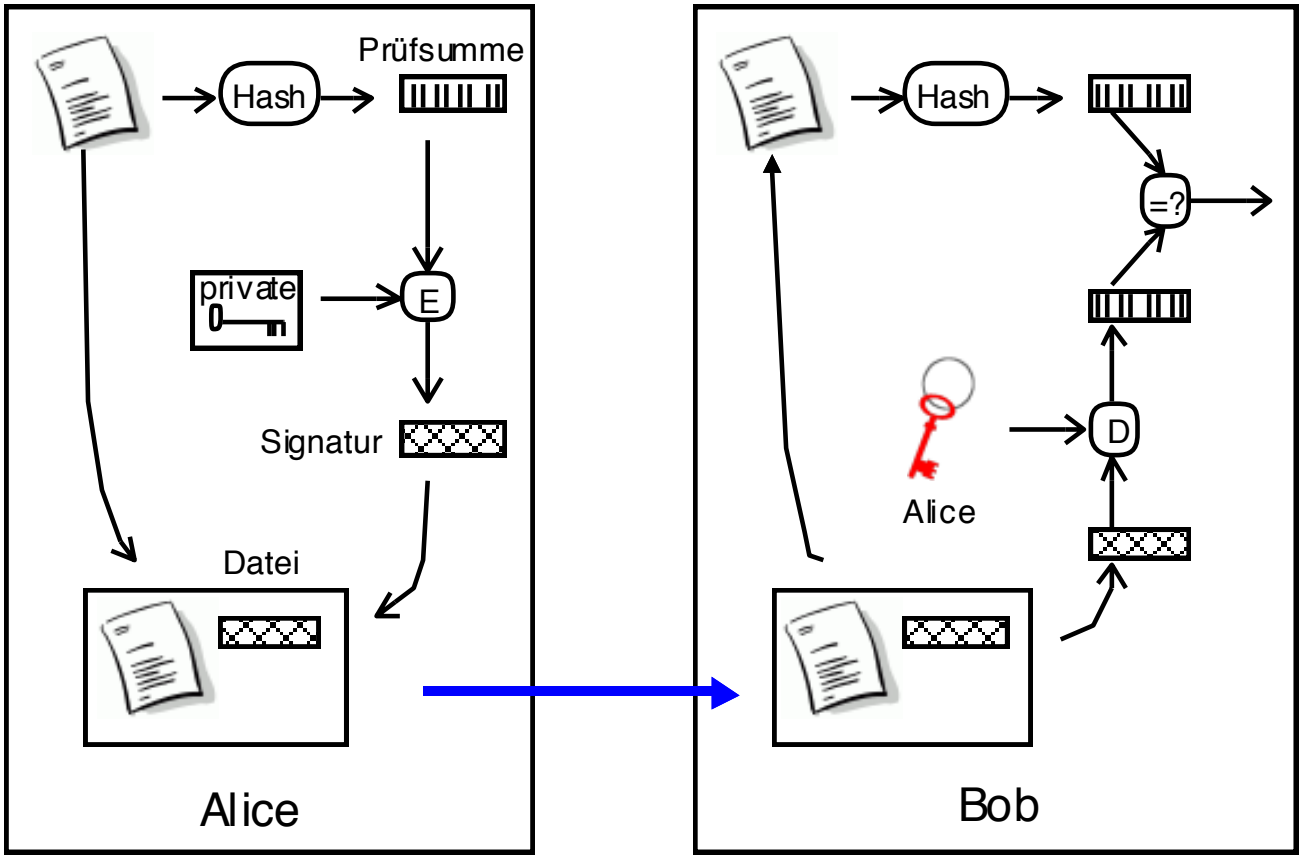
authentisieren, verschlüsseln und signieren

Authentisieren mit Challenge-Response



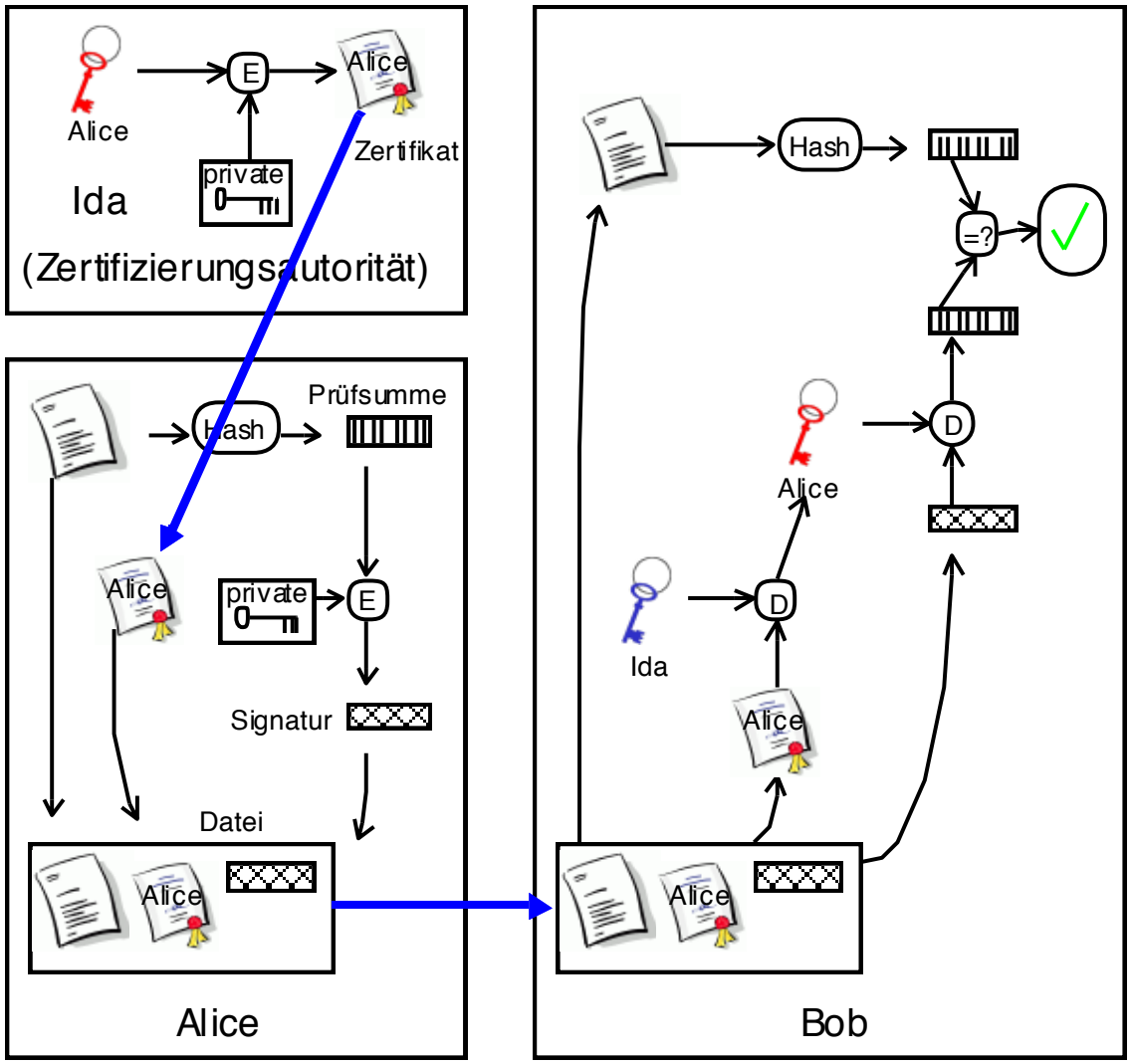
- Worin liegt der Vorteil gegenüber einfachem Authentisieren mit User-ID und Passwort? (Hinweis: was wird im Klartext übermittelt? Was wird beim nächsten Mal im Klartext übermittelt?)

Ein Dokument signieren - einfacher Fall



- Wie funktioniert das? (Hinweis: E=Encryption/Verschlüsselung, D= Decryption/Entschlüsselung)
- Woher bekommt Bob den öffentlichen Schlüssel von Alice und woher weiß er, das es der korrekte Schlüssel ist?

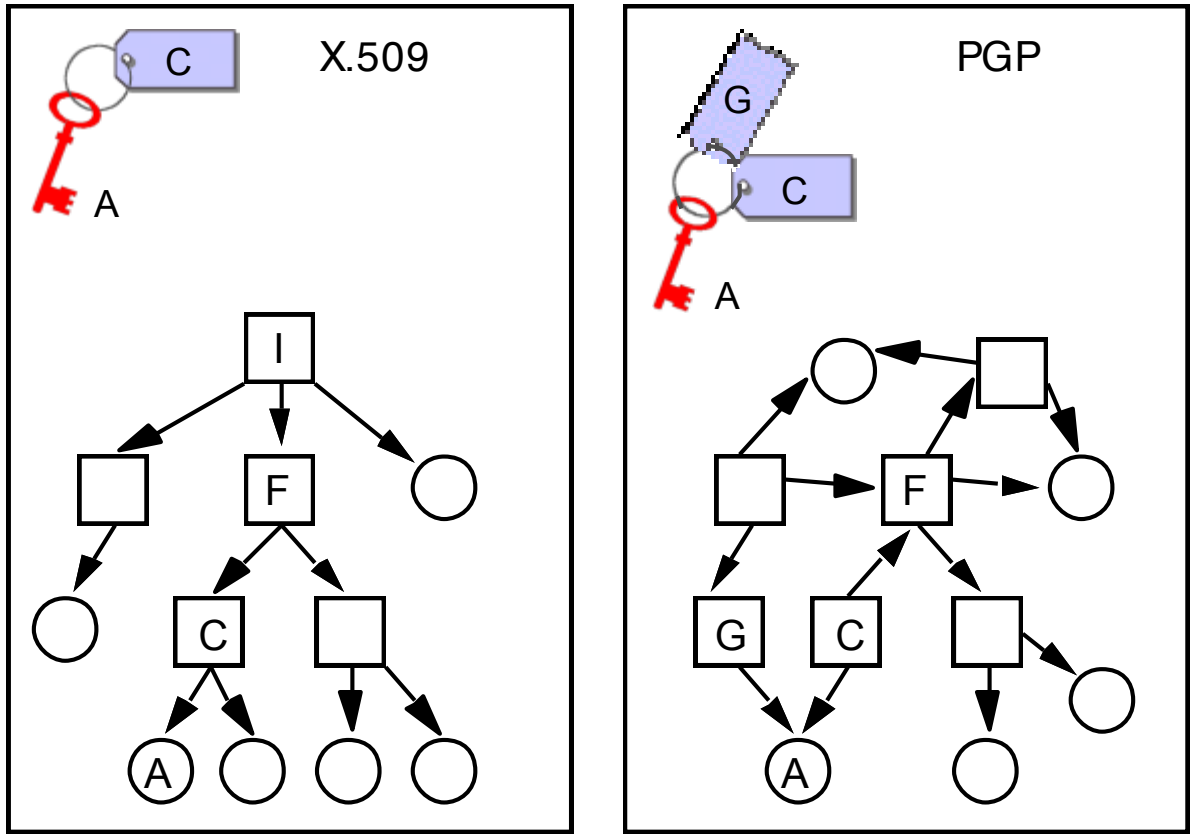
Ein Dokument signieren - Root Zertifikat



- Was ist der Unterschied zum Verfahren auf der letzten Seite? Vorteile?

Vertrauensbeziehungen bei Zertifikaten

DHBW Stuttgart



- Zertifikate nach dem X.509 Standard benötigen streng hierarchische Vertrauensbeziehungen.
- Zertifikate nach PGP (bzw. GnuPG) sind da flexibler.
- Was wären die Vorteile bzw. Nachteile im Vergleich der Verfahren?

Inhalt

DHBW Stuttgart

Sicherheit

- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit: Redundanz + Kapselung
- Hochverfügbare Systeme

Department of Redundancy Department

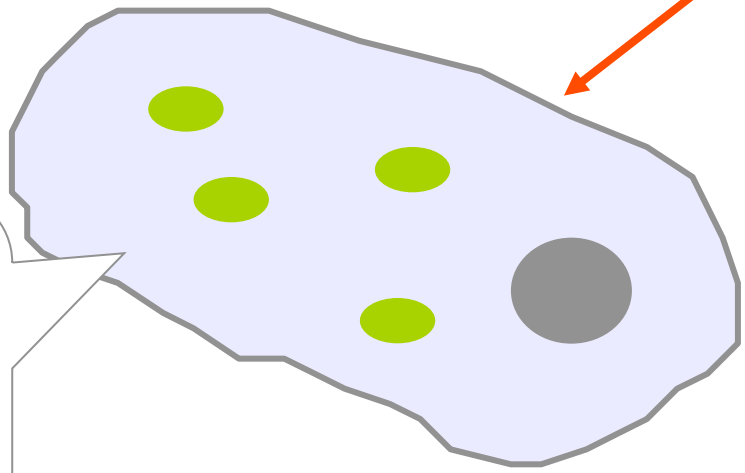
Office hours

Mo – Fr: 8am – 5pm, 9am – 6pm

Tu – Mo: 9am – 4pm

Was ist Kapselung?

DHBW Stuttgart



Schutzwand
(Perimeter, mit Zugangskontrolle)

Drinnen = vertrauenswürdig

Draussen = nicht vertrauenswürdig

Immunsystem:
- Viruserkennung
- Anti-Virus
- Anti-Worm
- Antibiotika (Reset)

Mikrobe

Kapselung = Perimeter-basierender Schutz

(ein fundamentales Konzept und ganz alter Hut)

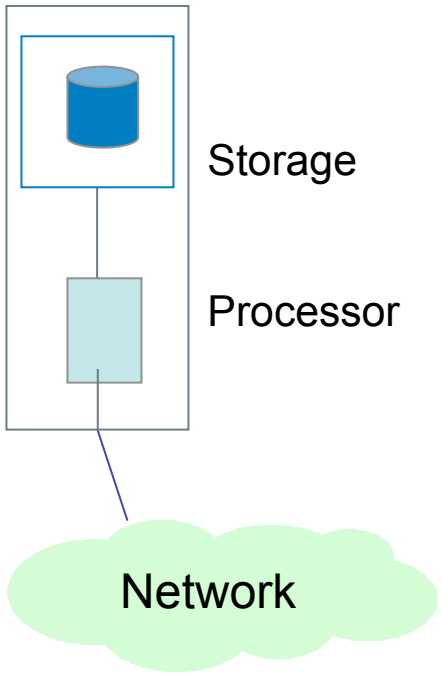
Inhalt

DHBW Stuttgart

Sicherheit

- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit
- Hochverfügbare System: Lösungsansätze

Redundanz: Grundlagen



Zu schützen:

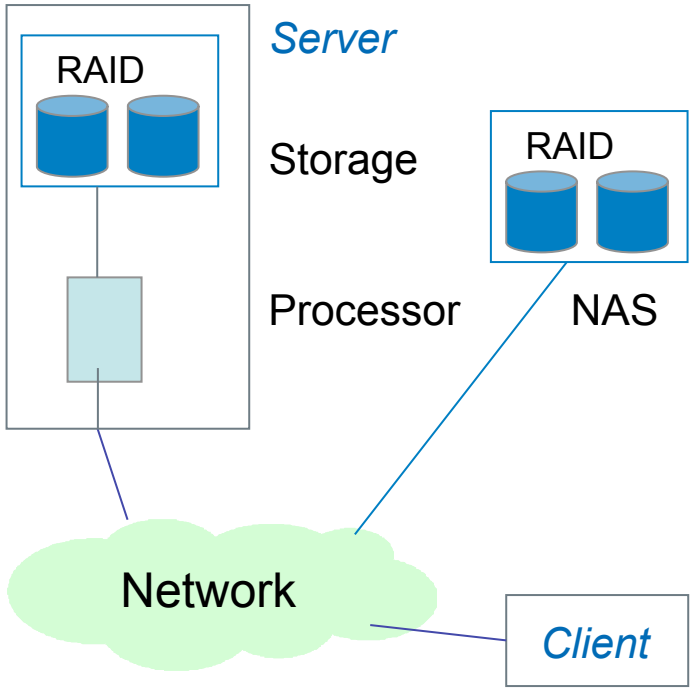
- Zustände (States) im Prozessor
- Daten im Speicher

Lösungen:

- Zustände: Der Anwendungssoftware überlassen (z.B.Kapselung von Transaktionen, Jounal-Files) bzw. dem Anwender überlassen (zwischendurch Speichern)
- Daten im Speicher: Back-ups

- Reicht für Desktop-PCs (nicht wirklich hochverfügbar)

Redundante Speicher



Zu schützen:

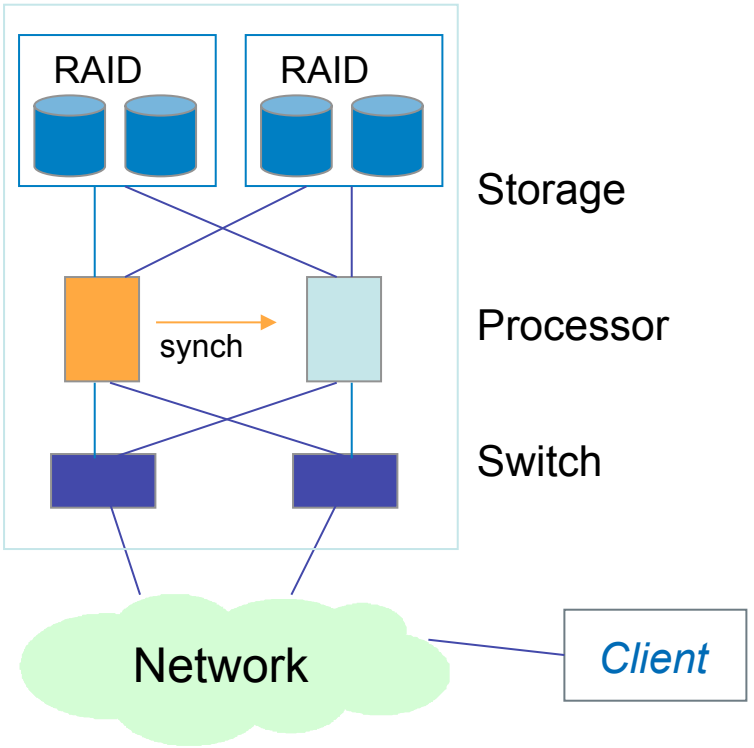
- Daten im Speicher

Lösung:

- Redundante Speichermedien (lokales RAID bzw. Network Attached Storage mit RAID)
- Back-ups

- Reicht für kleine Netze (nicht wirklich hochverfügbar)

Doppelt genäht hält besser

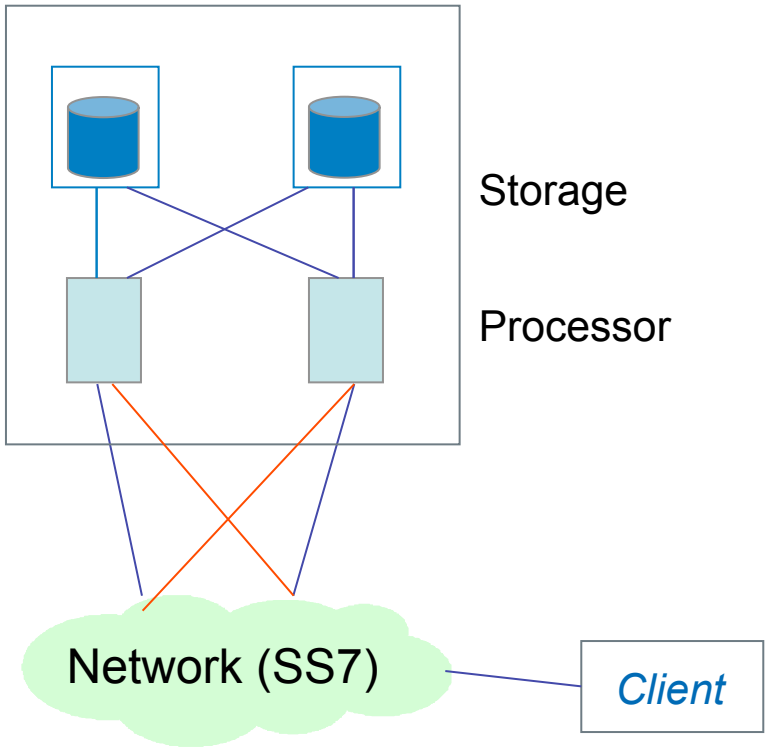


Systemarchitektur

- Redundante Switches (Ethernet)
- Redundante Prozessoren mit synchronisiertem Arbeitsspeicher
- Redundanter Speicher
- Gleicher Standort
- Erweiterbar mit mehr Prozessoren und Speicher

- Reicht für Systeme mittlerer Grösse ohne Disaster-Recovery
- Fail-Over bzw. Switch-Over für Wartung/Updates
- Schutz vor instabiler bzw. bösartiger Software (Anwendung, OS, Middleware)?

„Mated-Pairs“ in TK-Netzen

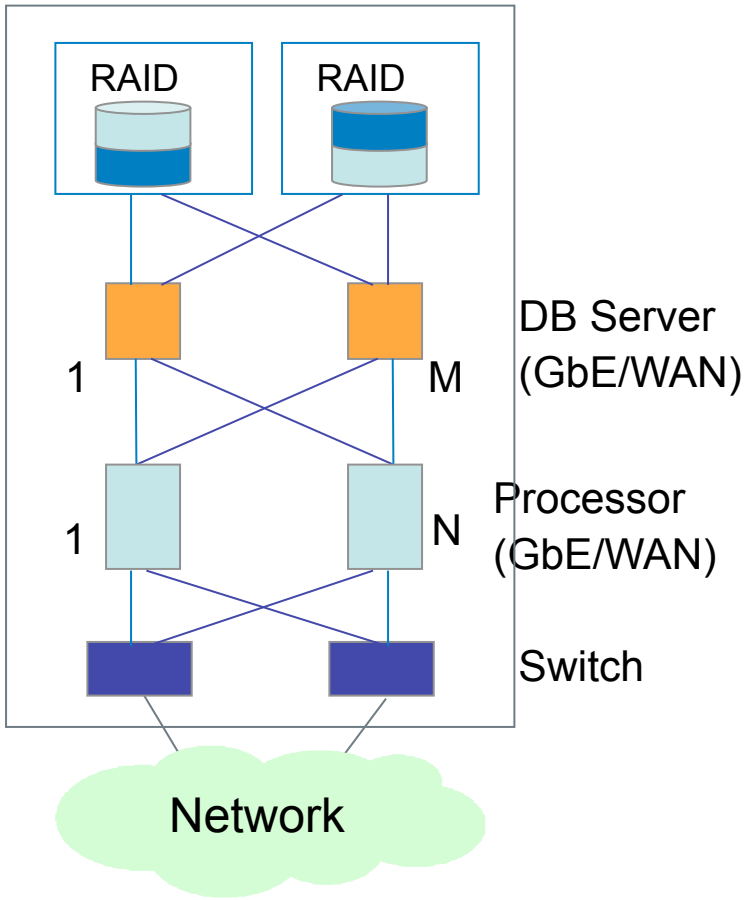


Systemarchitektur

- Redundante Prozessoren mit redundantem Speicher
- Netz unterstützt Fail-Over (Felhlerpfad wird vorkonfiguriert)
- Spezialfall der 2N Redundanz
- Wird teuer für viele Systeme (2N)

- Reicht für Systeme mittlerer Grösse ohne Disaster-Recovery
- Netz muss Fehlerpfade unterstützen
- Schutz vor instabiler bzw. bösartiger Software?

Einer Extra: N+1 Redundanz

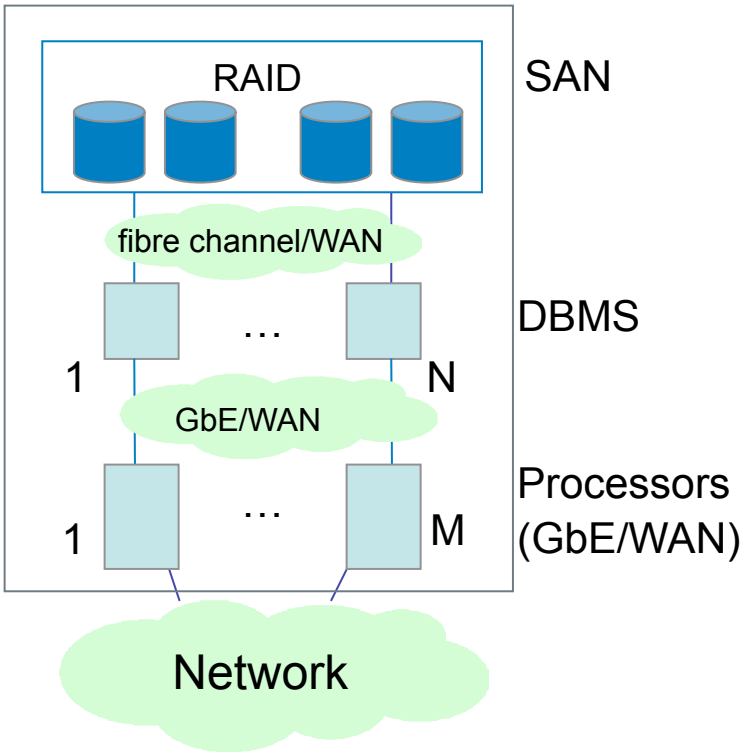


Systemarchitektur

- Redundanter Speicher (RAID, persistente Daten)
- M+1 redundante Datenbank-Server mit synchronisiertem Arbeitsspeicher
- N+1 redundante Prozessoren
- SW-Architektur auswärts skalierbar für grosse, verteilte Systeme

- Konzept: Trennung der Daten von der Anwendung (Data Base Servers), Ausfall eines Prozessors/DB Servers ohne Datenverlust
- Systeme mittlerer Grösse

N+k Redundanz mit Speichernetzen



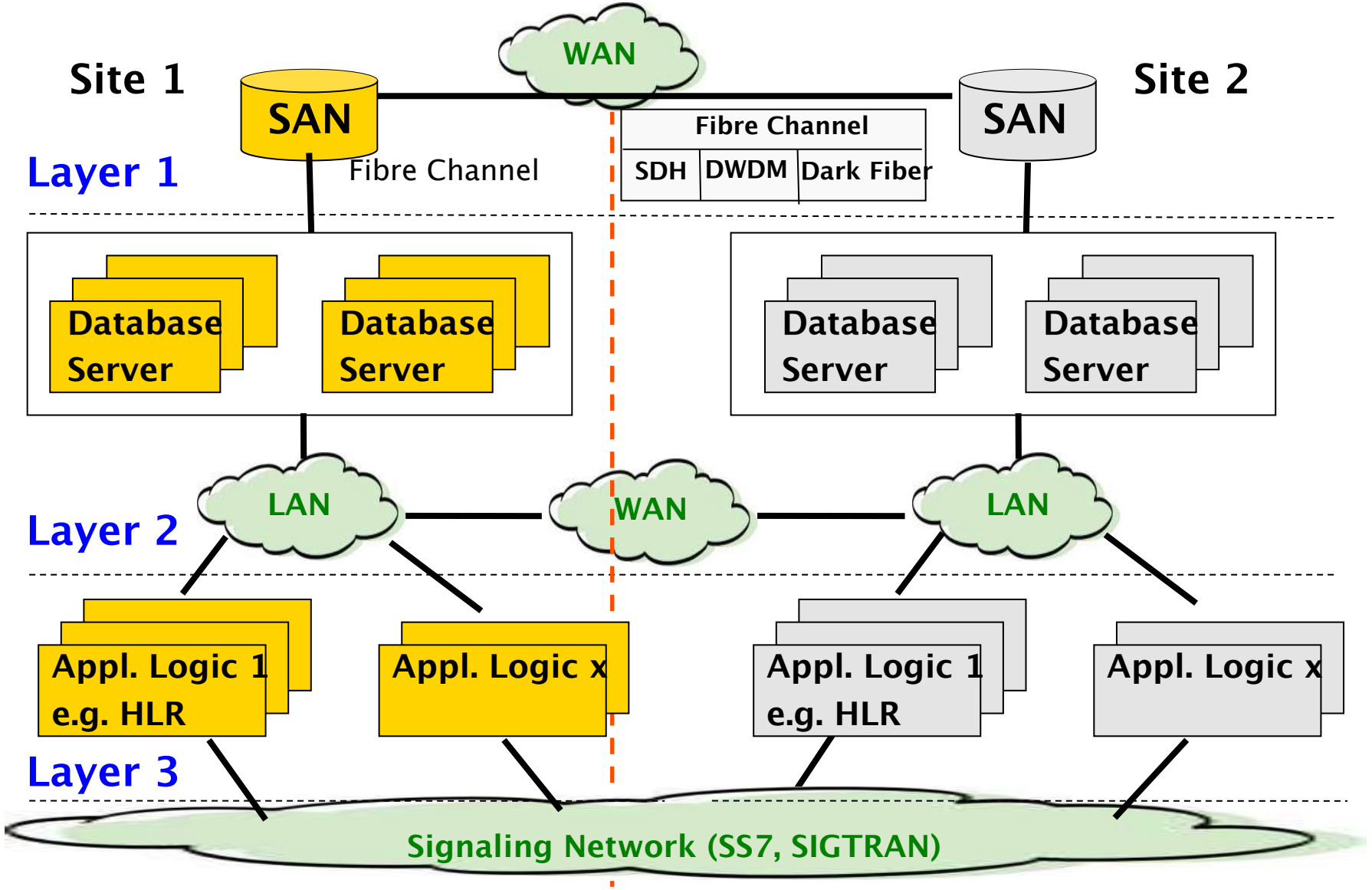
Systemarchitektur

- Redundante Speicher
- Redundantes Datenbank Management System (DBMS)
- Redundante Prozessoren
- Geographische Redundanz über Hochgeschwindigkeitsnetze
- Virtualisierung der Resourcen of (Speicher und Prozessor)
- Unterstützt N+k für Prozessor, DBMS und Speicher

- Reicht für grosse, verteilte Systeme mit höchster Verfügbarkeit
- Anwendung/Watchdog benötigt für Recovery
- Schutz vor instabiler bzw. bösartiger Software?

Beispiel: N+k Redundanz im Kernnetz

DHBW Stuttgart



Vergleich Redundanzkonzepte für TK

DHBW Stuttgart

Characteristic	Typical High Availability Systems	Redundancy by Distributed Storage Networks
Unit Cost	High (Proprietary HW and standby redundant policy)	Low (Commercial off-the-shelf HW and optimised redundancy policy)
Typical Architecture	Mated-pair	Load-sharing peers
Local Fault Tolerance	2 x N	N + k
Geographical Redundancy	4 x N	N + k
Disaster Recovery Time	Minutes -> Hours	Instant

Bedrohungen für verteilte Systeme

DHBW Stuttgart

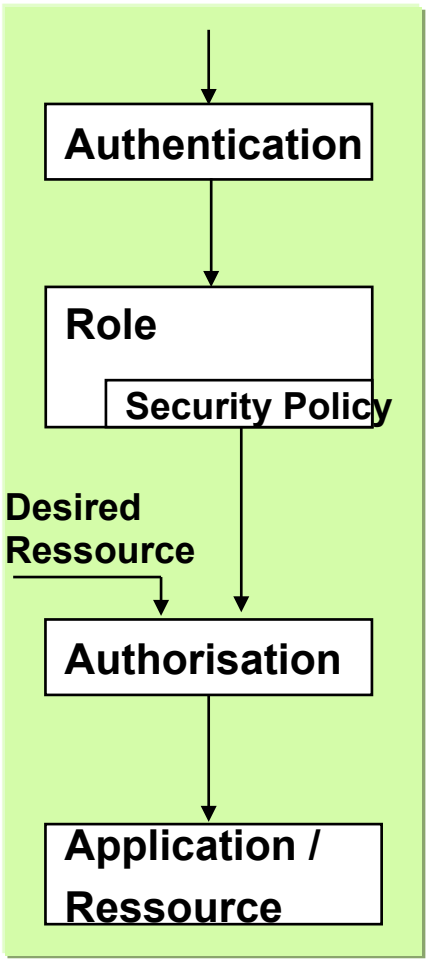
- Gleiche Gefahren wie für isolierte Systeme.
- Das Potential für Schaden ist wesentlich höher.

Jedoch:

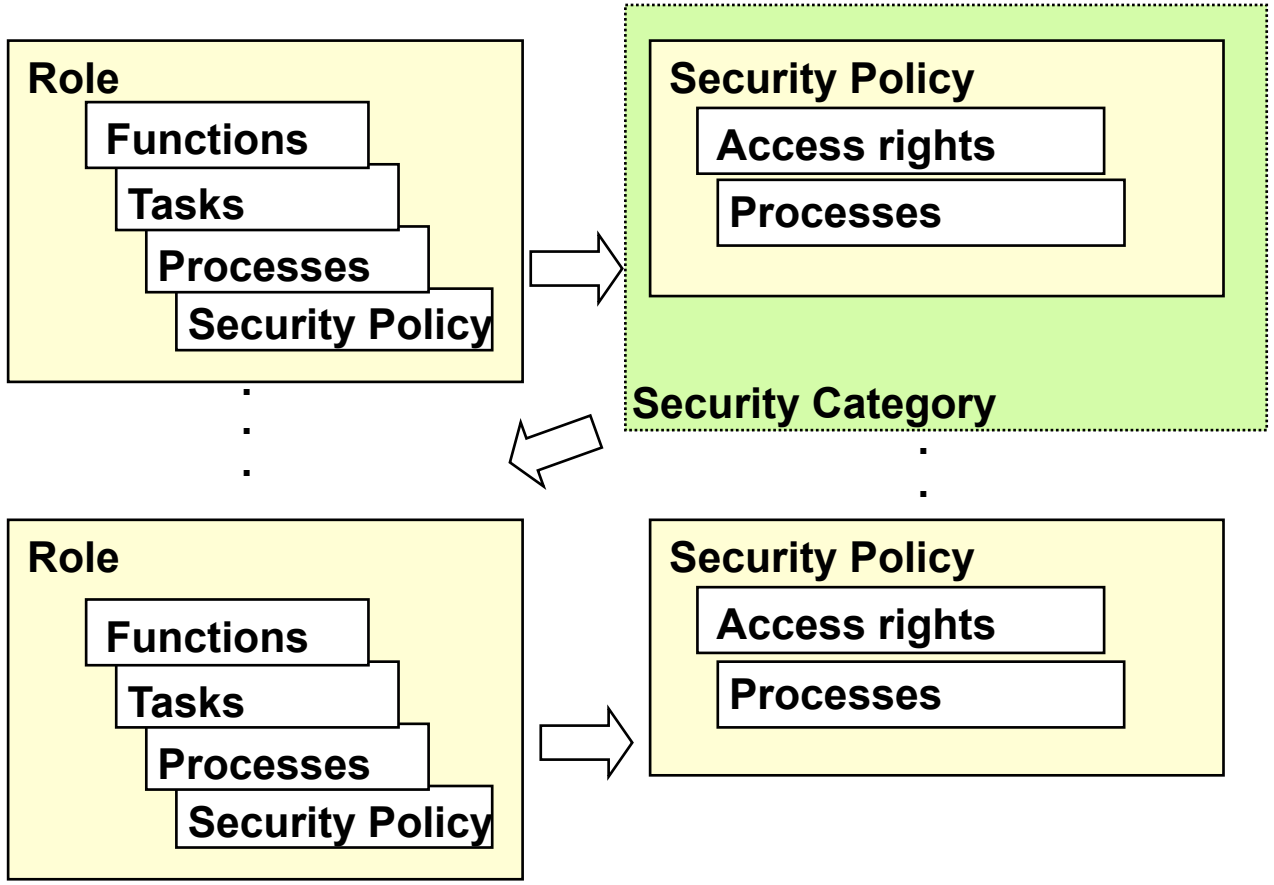
- Kann für den Schutz viel mehr investiert werden als in isolierte Systeme.

Sicherheitskonzept: Zugangskontrolle

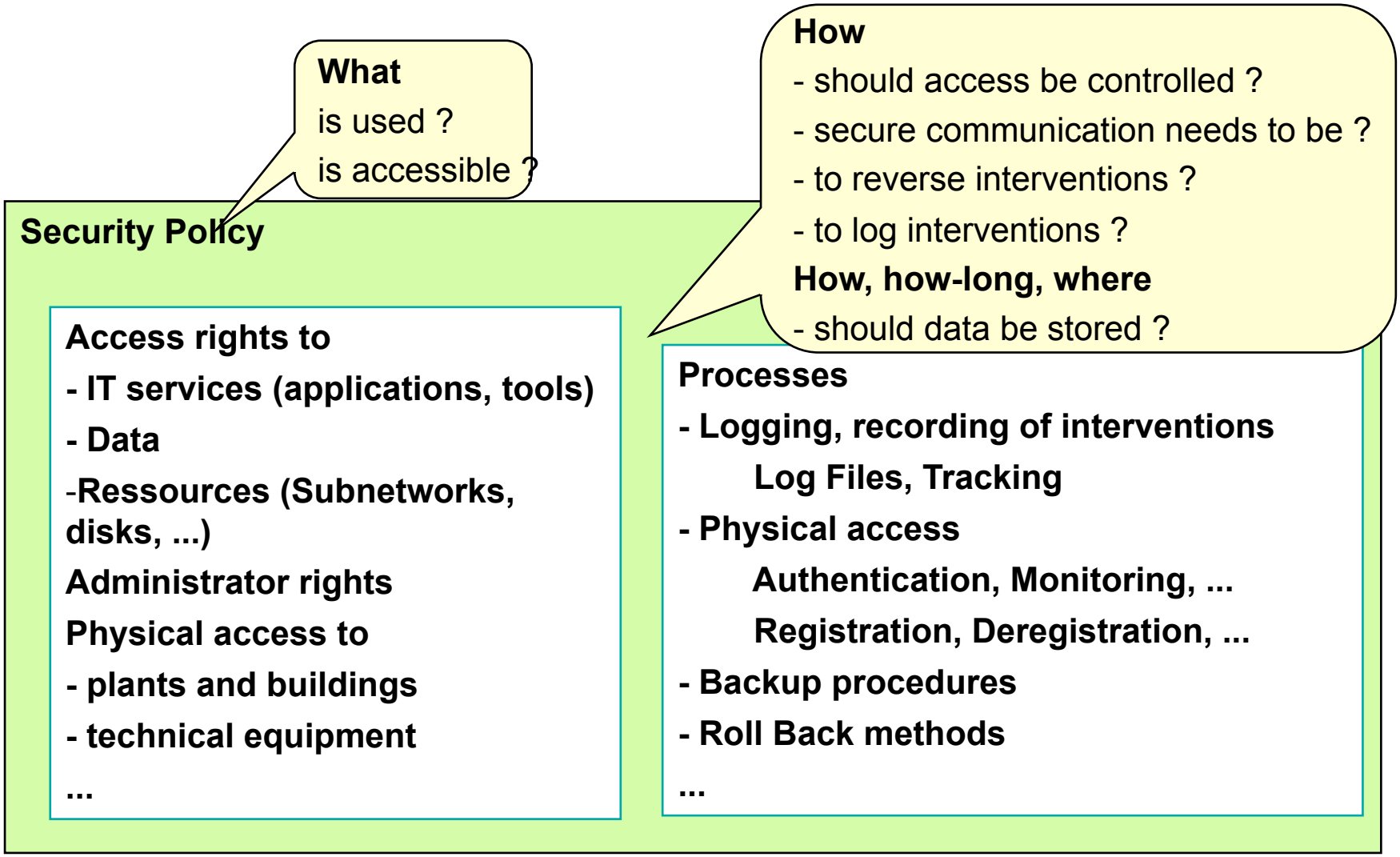
DHBW Stuttgart



Departments/ Organisations define:



Richtlinien (Policies)



DHBW Stuttgart

ENDE Teil 3 – Sicherheit

Literaturempfehlung: Bruce Schneyer, Secrets & Lies: IT-Sicherheit in einer vernetzten Welt, dpunkt.verlag/Wiley; Auflage: 1. Aufl. (2001), ISBN-13: 978-3898641135

Sicher ist nur, dass nichts wirklich sicher ist.
Nicht einmal das ist sicher.
Joachim Ringelnatz