

Sicher ist, dass nichts sicher ist.
Selbst das ist nicht sicher.
(J. Ringelnatz)

Kapitel 1 Authentifikation (Fort)

1.1 Mobilfunk der dritten Generation (3G): UMTS

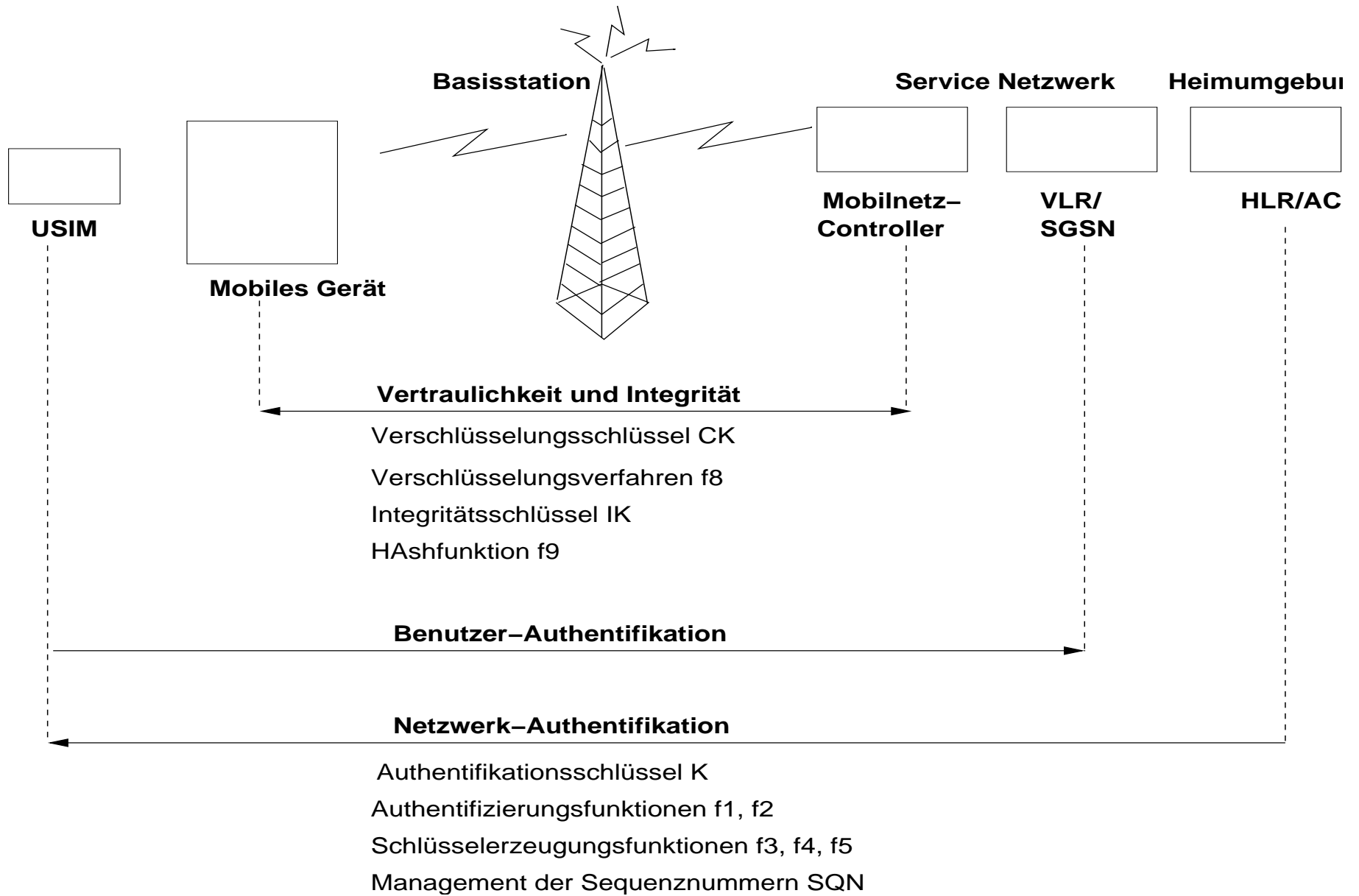
- **UMTS** = Universal Mobile Telecommunication System
weltweiter Standard basierend auf dem GSM-Standard
- Standardisierungsgremium: **3GPP** (*3rd* Generation Partnership Projekt),
Mitglieder: Standardisierungsgremien aus verschiedenen Ländern und Kontinenten, wie Europa, Nord-Amerika, Japan oder auch Korea

UMTS-Sicherheitsarchitektur

- Adaption von **GSM-Basisdiensten**:
 - Vertraulichkeit der Teilnehmeridentität,
 - die Authentifizierung des Teilnehmers gegenüber dem Netz,
 - die verschlüsselte Kommunikation auf der Luftschnittstelle,
 - die SIM-Karte als persönliches Sicherheitsmodul mit der Authentifikation des Teilnehmers gegenüber der SIM-Karte.

USIM (UMTS Subscriber Identity Module) als Analogon zur SIM-Karte

- UMTS-**Erweiterungen**:
 - Erweiterte **UMTS Authentifikation** und Schlüsselvereinbarung:
Heimatnetz authentifiziert sich gegenüber dem Benutzer,
Sequenznummern: Wiedereinspielung von Authentifizierungsdaten verhindern,
Vereinbarung von Integritätsschlüssel IK für MAC-Berechnungen
 - **Integrität der Kontrollsignale**:
Sichern der Kontrollsignale beim Verbindungsaufbau mit MAC
 - USIM **kontrollierte Nutzung** von Schlüsseln:
Das USIM erneute Authentifikation, falls das verschlüsselte Datenaufkommen einen bestimmten Betrag übersteigt
 - Service Netzwerk kontrollierte Nutzung der **Schlüssellebenszeit**:
Schlüsselerneuerung
 - **Integrität** und Vertraulichkeit der Kommunikationsdaten:
128-Bit Kommunikationsschlüssel, MACs für Integrität
 - Anzeige von fehlerhaften Authentifikationen: **Fehlermeldungen**



Authentifikation

Basis: vereinbarter geheimer Schlüssel **K**: USIM und HE

HE erzeugt n-Authentifizierungs-Vektoren (AV)

1. Für jede Verbindung: HE erzeugt neue Sequenznummer SQN und ,
128 Bit Zufallszahl RAND
Berechnung des 64 Bit MAC = $f_1(\mathbf{K}, (\text{SQN} \mid \text{RAND} \mid \text{AMF}))$
2. Berechnung der erwarteten Antwort XRES = $f_2(\mathbf{K}, \text{RAND})$
3. Erzeugung des 128 Bit Schlüssels CK = $f_3(\mathbf{K}, \text{RAND})$
4. Erzeugung des 128 Bit Schlüssels IK = $f_4(\mathbf{K}, \text{RAND})$
5. Erzeugung des 48-Bit langen Anonymitätsschlüssels AK = $f_5(\mathbf{K}, \text{RAND})$
6. Erstellen des Authentifikationstokens AUTN = SQN XOR AK | AMF | MAC
7. **Authentifizierungs-Vektor** AV = RAND | XRES | CK | IK | AUTN
8. AVs werden an Service Netzwerk weitergereicht

Verbindungsaufbau: bei Anfrage wird RAND und AUTN gesendet

1. USIM berechnet $AK = f_5(\mathbf{K}, RAND)$ und extrahiert damit die Sequenznummer SQN aus dem Token AUTN.
2. USIM berechnet $MAC' = f_1(\mathbf{K}, (SQN \mid RAND \mid AMF))$, Vergleich mit dem in AUTN enthaltenen MAC,
Bei Nichtübereinstimmung: senden einer Reject-Nachricht an das VLR bzw. den SGSN
3. USIM überprüft die Gültigkeit der Sequenznummer SQN,
Falls ungültig: melden eines Synchronisationsfehlers an das VLR bzw. SGSN und Service Netzwerk fordert von HE ein Feld von frischen Authentifikations-Vektoren an
4. USIM berechnet $RES = f_2(\mathbf{K}, RAND)$, Antwort an das Service-Netzwerk
5. Service-Netzwerk vergleicht RES mit dem Wert XRES aus dem Token AUTN,
Bei Gleichheit: Netzwerk extrahiert die beiden Schlüssel CK und IK aus AUTN
6. Abschließend berechnet die USIM die Schlüssel CK und IK:
 $CK = f_3(\mathbf{K}, RAND)$ und $IK = f_4(\mathbf{K}, RAND)$

Sicherheit von UMTS?

1.2 Biometrische Merkmale

- unverwechselbare und unveräußerliche Merkmale \Rightarrow eindeutige Charakterisierung

Beispiele und Anwendungsgebiete?

- Allgemeines Vorgehen:
 1. zu analysierende biometrische Eigenschaften erfassen
 2. digitalisierte Speicherung der Referenzwerte, "lernen"
 3. Referenzdatensätze z. B. im biometrischen Gerät oder Chipkarte
 4. Erfassung aktueller Probemuster bei jeder Authentifikation
z.B. Fingerabdrucksensoren, Videokamera
 5. aktuell erhobene Daten digitalisieren und
 6. mit gespeichertem Referenzwert vergleichen
- Unterscheidung: statische und dynamische Verfahren
Beispiele für statische: Fingerabdruck, Handgeometrie, Iris, Retina
Beispiele für dynamische: typische Verhaltensmuster beim Unterschreiben, Tipprhythmus, Lippenbewegungen

1.2.1 Problembereiche u.a.

- **Abgleich:** Referenzwerte mit aktuellen Werte, Unterschied zu Passwortverfahren?
- **Abweichungen** zwischen Referenz- und Probemuster sind unvermeidlich
Korrelationstests notwendig, Festlegen von Toleranzwerten
- **2 Fehlertypen:**
Berechtigter Benutzer wird abgewiesen, Kontrollen u.U zu streng
⇒ Akzeptanzproblem
Unberechtigter wird authentifiziert, Kontrollen zu locker
⇒ Sicherheitsproblem
- **Leistungsmaße** zur Bewertung der Güte eines Erkennungssystems:
False Rejection Rate (FRT): Abweisung autorisierter Benutzer
False Acceptance Rate (FAR): Akzeptanz unautorisierter
Equal Error Rate (EER) (Gleichfehlerrate)
Ziel: niedrige Gleichfehlerrate

- **Beispiele:** Fingerabdruck: FAR 1 zu 10^4 bis 1 zu 10^6
FRT: 1 zu 10^2 bis $1 : 3 \times 10^2$
EER bei IrisIdent: 1 zu $1,2 \times 10^6$
- **Vorsicht:** Fehlerrate meist ungeprüfte Angaben von Herstellern
- noch keine Standardisierung: Probleme bei Interoperation
Herstellerspezifische Erfassungsgeräte und Vergleichsalgorithmen
aktuelles Ergebnis einer 3-jährigen Studie BioTrust: www.biotrust.de
aktuelle Produkte weisen noch erhebliche Fehlerraten auf;
Zukunft liegt bei multimodalen Systemen
- Biometrie: rasante Entwicklung, Steigerungsraten über 20 % bei Biometrie-Produkten

1.2.2 Sicherheit biometrischer Techniken:

- **Vorteile:** keine absichtliche/unabsichtliche Weitergabe
Fälschen ist i.d.R. schwierig
Besitz eines Referenzwertes zur Authentifikation reicht nicht (wirklich?)

- Probleme aus enger Kopplung zwischen Merkmal und Person:
 - (1) Bedrohung der informationellen Selbstbestimmung
 - (2) Gefahren durch gewaltsame Angriffe gegen Personen
 - (3) Gefahren durch Unveränderbarkeit biometrischer Eigenschaften
- ad (1) informationelle Selbstbestimmung
 - Problem:** Biometrische Merkmale: eindeutige Identifikation, kein 'Ablegen' der Eigenschaften möglich, flächendeckende, ggf. auch unbemerkte Merkmalerhebung? Erstellung von Aufenthalts- und Bewegungsprofilen, Überwachung am Arbeitsplatz?! etc.
- ad (2) gewaltsamer Angriffe
 - Problem:** Gewaltkriminalität: menschliche Schlüssel
 - Lösungen?** spezielle Kontrollen: Lebend-Checks
Notfallvorsorge, z.B. Notfinger
- ad (3) Unveränderbarkeit der Merkmale

Problem: statisch festgelegte Daten

kompromittierte Daten? keine Erneuerung der Merkmale möglich!

Fälschungssichere Verarbeitung der Referenzwerte erforderlich!

datenschutzkonforme Speicherung erforderlich!

vertrauenswürdige Produkte?

Fazit biometrischer Techniken?

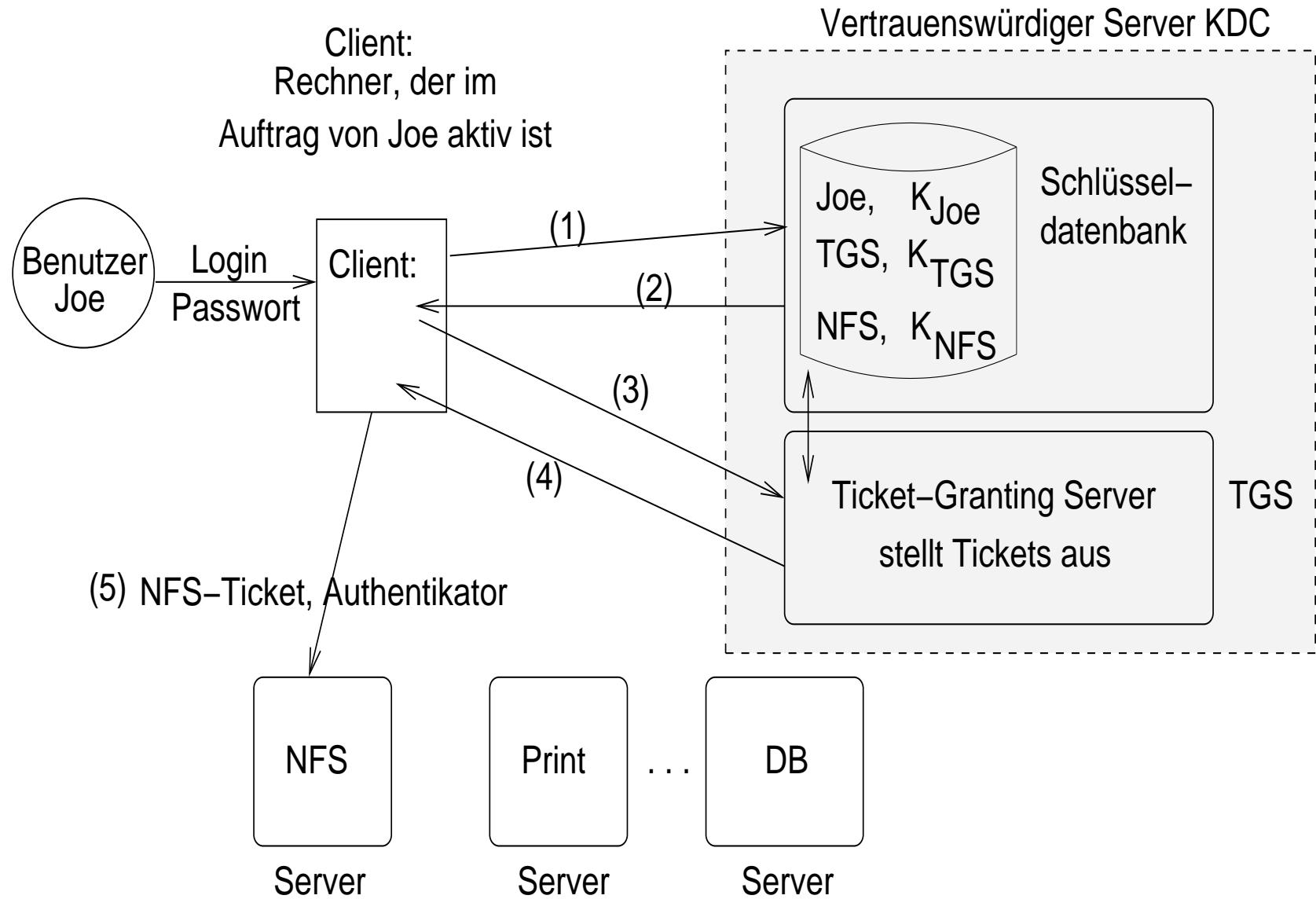
1.3 Kerberos-Authentifikationsprotokoll

- im Rahmen des Athena Projektes (Start 1983) am MIT
in Kooperation mit IBM und DEC entwickelt
- seit Version 5: wählbare Verschlüsselungsverfahren (nicht mehr nur DES vorgeschrieben)
- Hierarchie von Authentifikationsservern, KDC = Key Distribution Center:
autonome Verwaltung eines Bereichs (engl. *realm*),
Kommunikation mit den anderen Servern: Realisierung eines Single-Sign-On
- Implementierung: als frei verfügbare Referenzimplementierungen und
in kommerziellen Produkten, z.B. in Sun Solaris, Windows 2000

Kerberos-Dienste

1. **Authentifikation** von Subjekten (Principals): u.a. Benutzer, PC, Server
2. **Austausch von Sitzungs-Schlüsseln** zur Kommunikation zwischen Principals

Kerberos-Grobarchitektur:



Basis:

- jeder Principal A hat geheimen Master-Key K_A mit KDC vereinbart
- bei menschlichen Principals: Schlüssel wird aus dessen Passwort abgeleitet
- Nutzung eines Dienstes im verteilten System (z.B. NFS): erfordert gültiges Ticket
- KDC stellt auf Anfrage eines Principals ein Ticket aus

Ticket mit Authentifikations- und Verschlüsselungsinformationen

- ein Ticket $T_{c,s}$ ist nur für den Principal C (z.B. Joe) und den Server S (z.B. NFS) gültig
- $T_{c,s} = S, C, addr, timestamp, lifetime, K_{c,s}$, es gilt:
 - S Name des Servers, der in Anspruch genommen werden soll,
 - C Name des anfordernden Clients, $addr$ ist dessen IP-Adresse, Lebenszeit des Tickets, Sitzungs-Schlüssel $K_{c,s}$ für die Kommunikation zwischen S und C
- das Ticket wird mit dem Master Key K_s des Servers S verschlüsselt, $\{T_{c,s}\}^{K_s}$

Authentikator zum Authentifizieren des Clients C gegenüber dem Server S

- wird von C erzeugt und zusammen mit dem Ticket $T_{c,s}$ an Server S gesendet
- Authentikator $A_c = c, addr, timestamp$ wird von C verschlüsselt mit $K_{c,s}$
- Authentifikation: Empfänger entschlüsselt Authentikator und prüft:
 - IP-Adresse des Senders $\stackrel{?}{=} addr$
 - Gültigkeit der timestamp

Protokollschritte zusammengefasst

Von	An	Nachricht
1. Client	KDC	Joe, TGS, <i>Nonce1</i> (Bem. Nonce ist eine Zufallszahl)
2. KDC	Client	$\{K_{Joe,TGS}, Nonce1\}^{K_{Joe}}, \{T_{Joe,TGS}\}^{K_{TGS}}$
3. Client	TGS	$\{A_{Joe}\}^{K_{Joe,TGS}}, \{T_{Joe,TGS}\}^{K_{TGS}}, NFS, Nonce2$
4. TGS	Client	$\{K_{Joe,NFS}, Nonce2\}^{K_{Joe,TGS}}, \{T_{Joe,NFS}\}^{K_{NFS}}$
5. Client	NFS	$\{A_{Joe}\}^{K_{Joe,NFS}}, \{T_{Joe,NFS}\}^{K_{NFS}}$

Authentifikation des Servers ist auch möglich, wie?

Fazit: Sicherheit von Kerberos? Probleme?

1.4 Microsoft Passport-Konzept

- Single-Sign-on im Internet, seit 1999: Online-Shopping, E-Commerce etc.
- Bestandteil der Microsoft .NET Strategie, Hailstorm-Offensive
- Idee: Internet-Benutzer erhält eine Online-Identität,
einmalige Authentifizierung bei zentralem Passport-Dienst,
Ticketausstellung für registrierte Anbieter-Sites
- vereinfachtes Online Shoppen, Name, Adresse oder auch Kreditkartennummer zentral beim Passport-Server
- basierend auf: SSL, HTTP-Redirect, Cookies, CGI-Scripts JavaScript
- keine spezielle Software notwendig, in Windows XP direkt integriert
Bem. XP-Nutzer müssen sich aber nicht bei Passport registrieren

Passport-Modell mit drei Komponenten:

1. bei einem Passport-Server registrierter **Benutzer/Kunde**
2. **Anbieter** von Web-Inhalten, sogenannte Partner-Sites,

Anbieter müssen sich beim Passport-Dienst registrieren,

3. **Passport Login-Server** sowie zentrale **Datenbasis**,

Speicherung von Kunden-Authentifizierungsdaten, von Profilen, Wallet-Infos (u.a. Kreditkarteninformationen)

Registrierung von Benutzern (z.B. alle Hotmail-Nutzer automatisch!)

- Einrichtung eines Passport-Kontos bei einem Passport-Server aus der Domäne .passport.com
- Benutzer baut via HTTPS eine Verbindung zum Server `www.passport.com` auf
Registrierung über:
 - (1) Einrichten einer E-Mail-Kennung bei MSN Hotmail (automatisch)
 - (2) eine Seite eines Anbieters
 - (3) direktes Registrieren bei `http://www.passport.com`
 - (4) durch die Verwendung des Windows XP Registration Wizards.
- Kunde muss mindestens seine E-Mailadresse sowie sein Passwort angeben
bei Mobiltelefon: Telefonnummer und PIN

- optionale Angabe von Benutzerprofilen: u.a. Namen, Alter, Geschlecht oder auch Beruf
- Benutzer entscheidet, welche Profildaten an Anbieter weitergeleitet werden
- Anbieter erhält immer systeminterne Personal User ID (PUID) des Kunden

Registrierung von Anbietern

- verschiedene Sicherheitsstufen
- niedrigste Stufe: *Standard Sign-in*
z.B. personalisierter Zugriff auf Angebot ohne sicherheitsrelevante Daten
- *Secure Channel Sign-in*: vollständige Absicherung über SSL,
auch abgesicherte Cookie-Übertragung (s.u.)
- *Strong Credential Sign-in*: Standardanmeldung plus vierstellige PIN

Standard-Sign-In-Protokoll

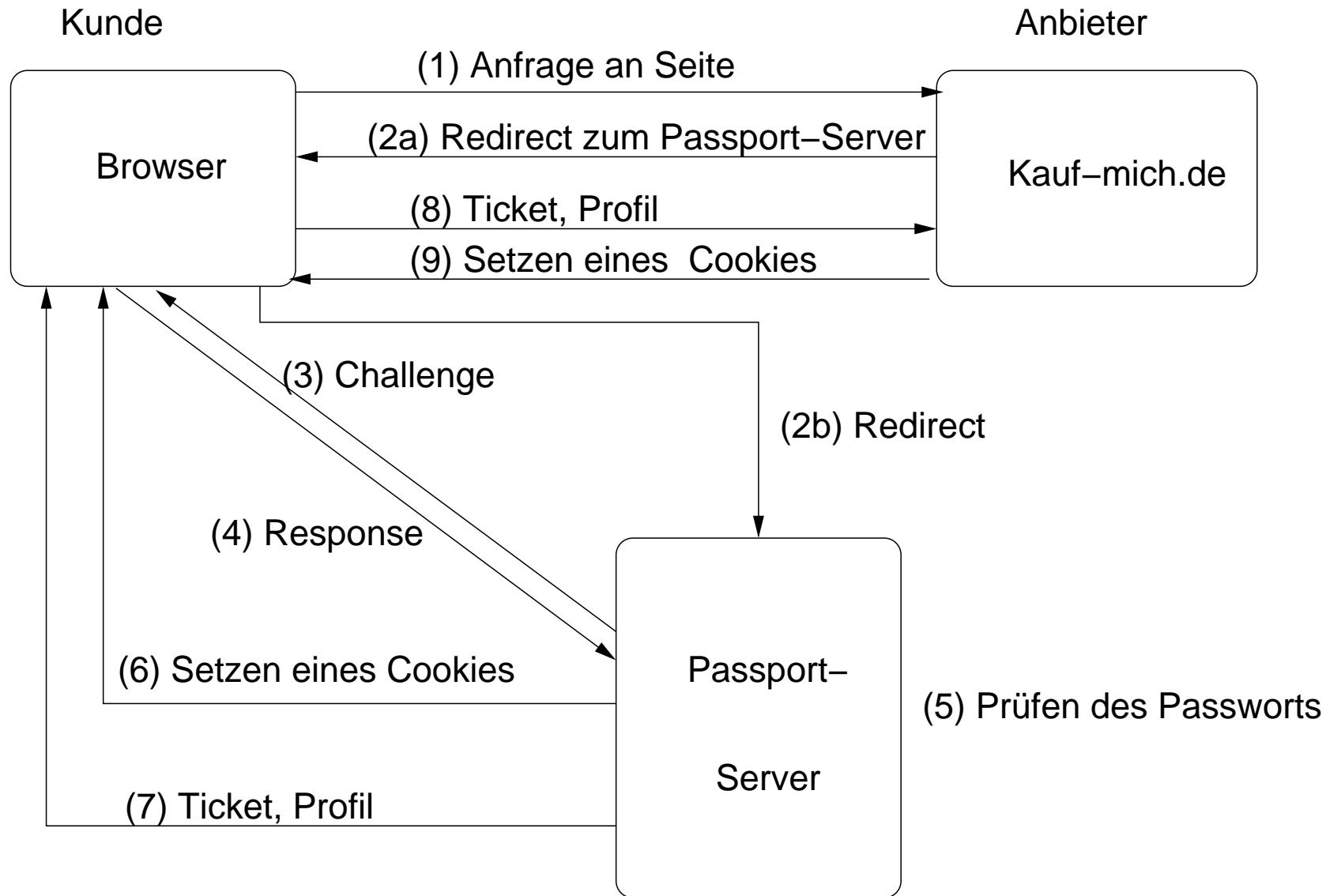
- Kunde klickt auf Web-Seite des Anbieters auf Anmelde-Link
- Redirect zu einem Passport-Login-Server

- Server prüft, ob Anbieter registriert ist
- Server fragt den Kunden nach E-Mail und Passwort (Challenge)
- Antworten (Response) per SSL verschlüsselt
- falls ok, setzen eines Cookie beim Kunden
Cookie enthält das verschlüsselte Kundenpasswort, verschlüsselt mit Server-Schlüssel
- Erstellen eines Zugangstickets in Form eines Cookies,
Informationen in Cookie TripleDES verschlüsselt mit gemeinsamen Schlüssel zw. Anbieter und Passport-Server
- Cookie über als HTTP-Redirect zurück zum Kunden
- Weiterleiten über Kunden-Browser zum Anbieter,
Anbieter: Entschlüsseln, Entnahme der PUID etc.
Über PUID Identifikation eines dedizierten Benutzers
- Anbieter setzt Cookie beim Kunden
enthält verschlüsselte Zugangsdaten des Kunde

- Abmeldung: Link bei Anbieter
Passport-Server: ermittelt alle Anbieter, bei denen der Kunde war,
Anbieter müssen Cookies entfernen (Starten eines Scripts durch Passport-Server),
Passport-Cookie wird entfernt, falls nicht persistent

Wallet-Protokoll: Online Shopping, analog

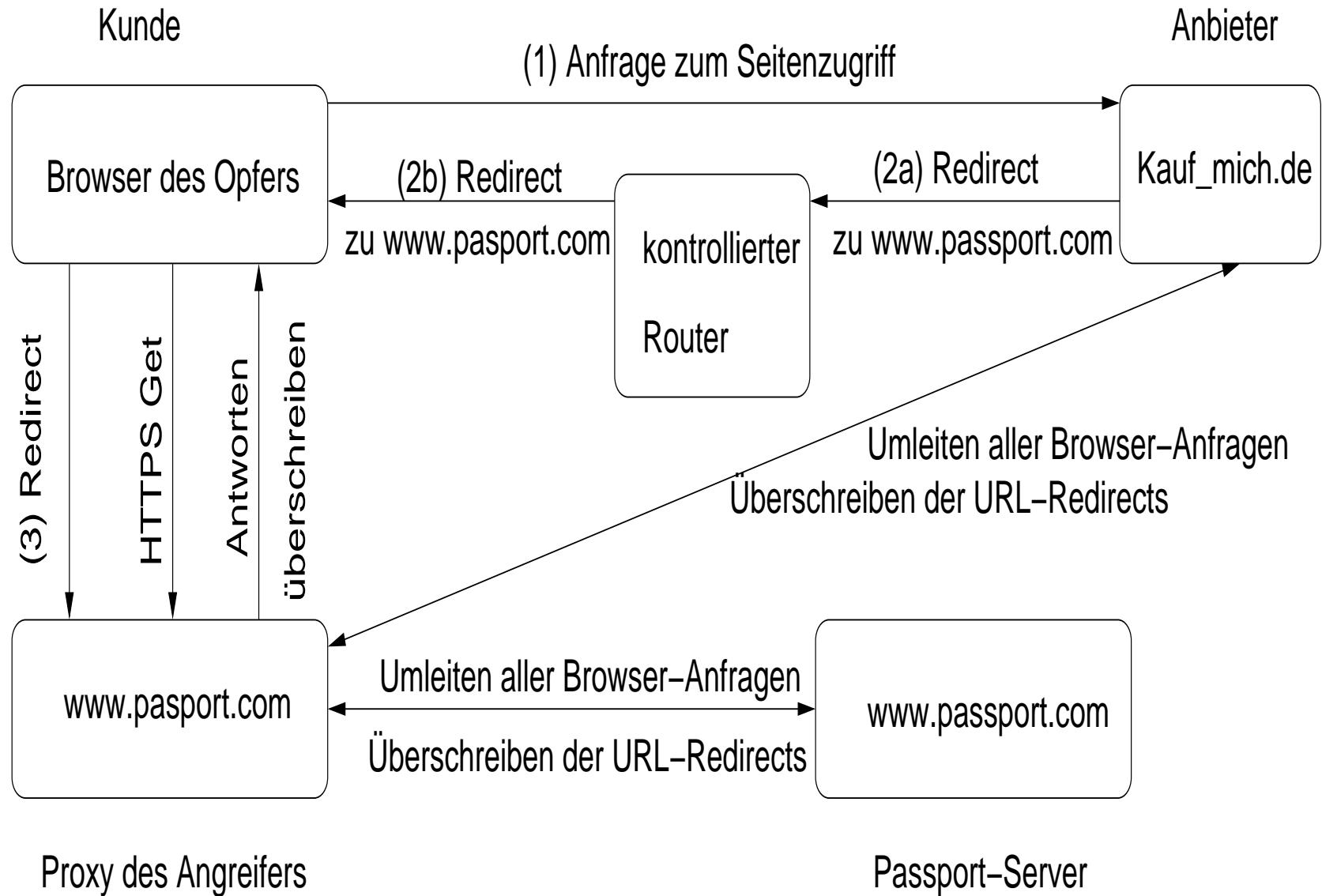
- Re-Authentifizierung zum Bezahlen, falls letztes Authentifizieren länger als 15 Minuten zurückliegt
- manuelles Authentifizieren notwendig (wirklich?!)
z.B. über MSN Messenger automatisch ?!
- Kunde gibt explizit die zu übermittelnden Bezahlinformation frei.
aber weiss er wirklich an wen?!
- Passport-Server erstellt verschlüsselte Bezahlinfos, wiederum Cookie
keiner kommt an die Daten, wirklich?!



Sicherheit des Passport-Konzepts?

- Vergleich mit Kerberos?
- Design-Probleme: u.a. Cookies gelten für alle Passport-Server
Passwort zur Authentifikation für alle Dienste:
z.B. Hotmail Passwort auch für Wallet-Protokoll
Verwendung von JavaScript: Gefahr von Cross-Site-Scripting Angriffen
- Spoofing-Angriffe? z.B. Maskieren des Passport-Servers (siehe übernächste Folie)
- Verschlüsselte Cookies: Schlüsselerneuerung? Schlüsselverteilung?
- Cookie-Lebensdauer: u.a.
persistente Cookie in öffentlichen Rechnern?!
Viren, Würmer, die gespeicherte Cookies auslesen?!
- Sinn der PIN-gesicherten Authentifikation bei Single-Sign-on?
- Zentrale Datenhaltung: wunderbares Angriffsziel
Privacy-Probleme?

- Registrierung von Web-Anbietern beim Passport-Dienst: welche Überprüfungen? Vertrauenswürdig?
- Alternativen: *Liberty Alliance Project*, u.a. Sun, Nokia, Cisco, NTT DoCoMO, Cisco, Entrust, Gemplus, RSA Security, Verisign, General Motors oder auch Bank of America dezentrale Datenhaltung geplant
- Fazit?



Fazit: Authentifikation

- **Korrekte** und **zuverlässige** (wechselseitige) Authentifikation notwendig!
⇒ Grundlage für weitere Kontrollen!
- **Wechselseitige** Authentifikation notwendig! ⇒ Abwehr von Spoofing-Angriffen
- **Einfache**, automatisierte Handhabung von Sicherheitsmechanismen gefordert!
⇒ Voraussetzung für Akzeptanz bei Anwendern
⇒ Biometrie und Smartcards wichtige Basis
- Single-Sign-on, vgl. Kerberos versus Passport-Konzept
- **Differenzierte** Authentifikation (Rechner-, Benutzer-, Prozess-, Anweisungs-Ebene)
⇒ BS-Weiterentwicklungen erforderlich!
⇒ Netzwerk-Protokolle u.a. TCP/IP, IPv6, SSL, SET
- begrenzte **Gültigkeitsdauer** für Schlüsseln, Passworten, ...
Maßnahmen zur Reduktion von Angriffsmöglichkeiten: u.a.
keine geheimen Informationen über unsicheres Medium austauschen