Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Authentikationsverfahren

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Inhalt

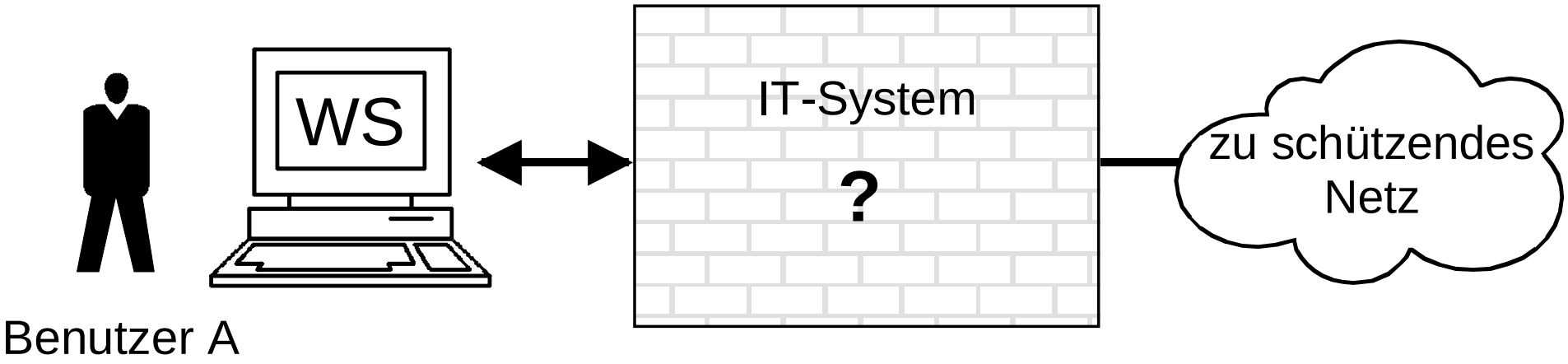
- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- FIDO
- Zusammenfassung

Inhalt

- **Identifikation und Authentikation**
  - Generelle Authentikationsverfahren
  - Passwort-Verfahren - Passwortregeln
  - Einmal-Passwort-Verfahren
  - Challenge-Response-Verfahren
  - Biometrische Verfahren
  - Authentikationsverfahren mittels Mobilfunk
  - AuthService – if(is)
  - FIDO
  - Zusammenfassung

Identifikation und Authentikation
→ Das Problem

Wer ist tatsächlich Benutzer A ?



- Wenn ein Nutzer Zugang haben möchte, muss er sich dem IT-System gegenüber
  - **identifizieren** und
  - **authentisieren**

Identifikation und Authentikation
→ Identifikation

- Die **Identifikation** ist die Überprüfung eines vorgelegten, kennzeichnenden Merkmals, z.B. des Benutzernamens.
- Eine Person wird eindeutig durch die Angabe von Vorname, Nachname, Geburtsort und Geburtstag identifiziert.
- In Deutschland wird die Eindeutigkeit der Identifikation von den Standesämtern garantiert.
- Eine Identifikation muss immer innerhalb eines Systems (Organisation) abgesprochen sein, damit sie eindeutig ist.
- Damit eine solche Absprache mit verschiedenen Benutzern zustande kommt, müssen klar definierte Regeln eingehalten werden.
- Ein Beispiel:
  - CCITT »Recommendation« X.509 bzw. ISO 9594-8
  - Ein Konzept eindeutiger, kennzeichnender Namen oder »distinguishing identifier«

Identifikation und Authentikation
→ Authentikation

- **Authentikation** bezeichnet einen Prozeß, in dem überprüft wird, ob »jemand« oder »etwas« echt oder berechtigt ist.
- Authentikation bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität.
- Die Überprüfung des Personalausweises einer Person ist eine solche Authentikation.
- Was muss und kann z.B. identifiziert und authentisiert werden ?
  - Kommunikationspartner: z.B. Benutzer, Prozesse, Instanzen, das Security Management
  - Kommunikationsmedien: z.B. Workstation, Serversysteme, Firewall-Elemente (Packet Filter, Application Gateway, Proxy, Security Management), Security Token usw.
  - Nachrichten: z.B. Mails, Dateien, Java-Applets usw.

Inhalt

- Identifikation und Authentikation
- **Generelle Authentikationsverfahren**
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- FIDO
- Zusammenfassung

Generelle Authentikationsverfahren → Übersicht (1/2)

- **Passwort-Verfahren**
  - Einfachste Authentikationsverfahren
  - Wenn das Passwort im Klartext über das Internet übertragen wird, dann kann es mitgelesen und mißbräuchlich verwendet werden
  - Passwortregeln müssen eingehalten werden

- **Einmal-Passwort**
  - Jedes Passwort wird nur einmal verwendet
  - Zwei unterschiedliche Methoden:
    - Passworte werden im Vorfeld bestimmt und verteilt (z.B. TAN-Listen)
    - Benutzer kann sie nach einem definierten Verfahren berechnen

Generelle Authentikationsverfahren → Übersicht (2/2)

- **Challenge-Response-Verfahren**
  - Benutzer muss sich spontan kryptographisch beweisen
  - Dazu braucht er einen Schlüssel und ein Verfahren
  - Z.B. Zufallszahl als Challange, Signatur dieser als Response

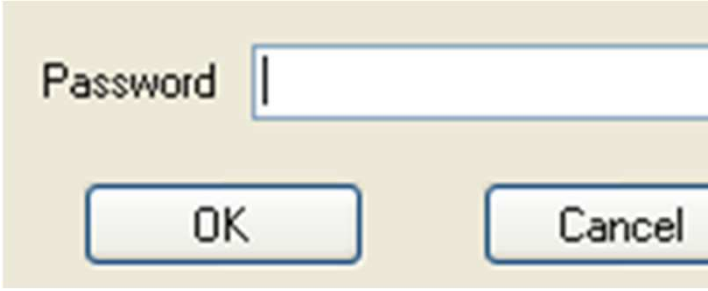
- **Biometrische Verfahren**
  - Identifikation und Authentifikation mittels biometrischer Merkmale
    - Aktiv: Stimme, Unterschrift, Gestik, Tippverhalten
    - Passiv: Fingerabdruck, Retina, Iris, Gesicht, Ohr
  - Zur Authentikation im Internet kaum anwendbar
  - Nutzbar als Zugangskontrolle (Pässe, Türen, USB-Token)

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- **Passwort-Verfahren - Passwortregeln**
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- FIDO
- Zusammenfassung

Passwort-Authentisierung
→ Dilemma

- **Passworte, Passworte, … sind das Authentisierungs-Mittel im Internet!**
  - Passwort-Probleme
    - Verwendung von schlechten Passwörtern, oder
    - ein gutes Passwort wird für viele Dienste verwendet
    - Passworte werden im Klartext in HTTP-Sessions und in E-Mails über das Internet übertragen!
    - Key-Logger (Malware)
    - Passwort-Reset-Mechanismen sind sehr unsicher



- **Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld!**
  - D.h. neben unterschiedlichen Passwörtern müssen wir uns auch oft noch unterschiedliche Identitäten merken!

- **Phishing-Problem** verursacht einen sehr großen Schaden (BKA)

Passwort-Verfahren
→ Probleme (1/3)

- Durch die Masse der benötigten Zugänge für einen Nutzer werden oftmals „unsichere“ Passwörter verwendet (E-Mail, Shops, Foren etc.).
- Diese meist sehr kurzen und oftmals mehrmals verwendeten Passwörter machen es potentiellen Angreifern besonders einfach.
- Ein zusätzlicher Faktor ist die steigende Rechenleistung von PCs im Privatbereich
  - Brauchten früher Hochleistungsrechner noch Jahrzehnte, sind aktuelle PCs um ein vielfaches schneller und erledigen manche Aufgaben sehr schnell

Passwort-Verfahren
→ Probleme (2/3)

- Beispiel SHA-1 (one-way-hash)
- 800 Millionen Hashes / Sekunde mit einem normalen 4-Kern-CPU und einer Grafikkarte aus dem High-End-Bereich
- Annahme: 84 Zeichen und Offline Angriff (hash liegt direkt auf dem PC)

Länge	Höchstlebensdauer	Zeit zum vollst. durchsuchen
4	0	62 ms
5	0	5 Sek.
6	0	7 Min.
7	11 Sek.	10 Std.
8	15 Min.	36 Tage
9	21 Std.	8 Jahre
10	75 Tage	693 Jahre
11	17 Jahre	58 234 Jahre
12	1 467 Jahre	4 891 644 Jahre
13	123 269 Jahre	410 898 092 Jahre
14	10 354 631 Jahre	34 515 439 748 Jahre

Passwort-Verfahren
→ Probleme (3/3)

- Beispiel LAN-Manager (one-way-hash für Windows Anmeldungen)
- 2 Mrd. Hashes / Sekunde (Applikationsbeschleuniger mit vier GPUs)
- Annahme: 96 Zeichen (Online Angriff, Hash liegt auf entferntem Rechner, der ggf noch zusätzliche Beschränkungen hat)

Länge	Höchstlebensdauer	Zeit zum vollst. durchsuchen
4	0	42 ms
5	0	4 Sek.
6	0	7 Min.
7	0	10 Std.
8	36 Sek	42 Tage
9	57 Min	11 Jahre
10	96 Std	1 054 Jahre
11	369 Tage	101 192 Jahre
12	97 Jahre	9 714 449 Jahre
13	9 325 Jahre	932 587 150 Jahre
14	895 283 Jahre	89 528 366 368 Jahre

Passwort-Verfahren
→ Empfehlungen (1/3)

- **Nachlässig:**
  - Weniger als 8 Zeichen
  - Wörter, die in Wörterbüchern zu finden sind

  ⇒ Bieten praktisch keinen Schutz

- **Niedrig:**
  - 8 oder 9 Zeichen
  - Mindestens zwei der folgenden Arten enthalten:
    - Großschreibung
    - Kleinschreibung
    - Zahlen
    - Sonderzeichen
  - Keine sinnvollen Wörter
  - Lebensdauer maximal 90 Tage

  ⇒ Geringe Sicherheit

Passwort-Verfahren
→ Empfehlungen (2/3)

- **Mittel:**
  - 10 oder 11 Zeichen
  - Drei der unter „Niedrig“ aufgeführten Arten enthalten
  - Lebensdauer maximal 60 Tage

- **Hoch:**
  - 12 bis 15 Zeichen
  - Alle 4 Arten unter „Niedrig“ müssen erfüllt sein
  - Lebensdauer maximal 30 Tage

- **Sehr hoch:**
  - Mindestens 16 Zeichen
  - Kein „aussprechbares“ Wort („n8“ = „night“ etc)
  - Lebensdauer maximal 2 Wochen

Passwort-Verfahren
→ Empfehlungen (3/3)

- Betrachtung der Sicherheit der unterschiedlichen Stufen:
  - *mit einem einzelnen High-End-PC

Passwort-Stärke	Vollständige Suche*	Passwort-Lebensdauer	erfasster Suchraumanteil* innerhalb der Lebensdauer
niedrig (8)	104 Tage	90 Tage	86,2336%
mittel (10)	2 635 Jahre	60 Tage	0,0062%
hoch (12)	24 Millionen Jahre	30 Tage	0,000000338%
sehr hoch (16)	2 Billiarden Jahre	14 Tage	0,000000000000001859%

- Die Kombination von Passwort-Stärke und Lebensdauer sorgt dafür, dass deutlich mehr Rechenaufwand betrieben werden muss.
- Bei mittlerer Sicherheit werden schon 16 000 Systeme für zwei Monate benötigt!

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- **Einmal-Passwort-Verfahren**
- Challenge-Response-Verfahren
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- FIDO
- Zusammenfassung

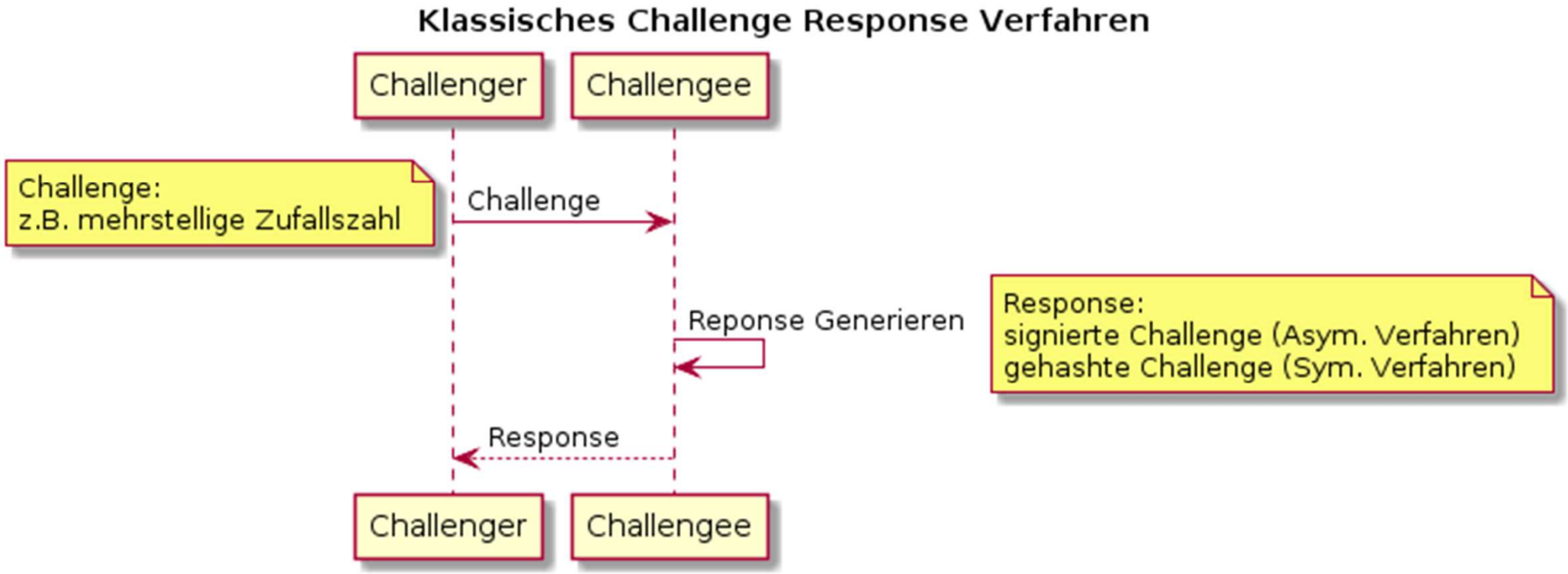
Einmal-Passwort-Verfahren
→ Übersicht

- Ein Einmalpasswort (engl. One-Time Password - OTP) ist ein Authentifikationsverfahren bei dem ein Passwort nur einmal für eine Session benutzt werden kann.
- Damit wird ausgeschlossen, dass ein Angreifer ein Passwort abhören und erneut verwenden kann (Replay-Attacken). „Man in the Middle Attacken“ sind aber immer noch möglich!
- Im Prinzip gibt es dafür zwei Möglichkeiten zur Umsetzung.
  - **Vorgenerierte Listen**
    - Z.B. werden vorgenerierte Listen verwendet, die dem Benutzer vorher über einen sicheren Kanal übertragen worden sein müssen.
    - Die geschieht zum Beispiel bei den TANs des PIN/TAN-Verfahrens.
  - **Kennwortgeneratoren**
    - Z.B. werden kryptographische Hash-Funktionen zur Generierung von nur kurzzeitig gültigen Einmalpasswörtern verwendet. Alternative: Zeitgesteuerte Generatoren
    - Beispiele sind SecurID von der Firma RSA Security oder das von Bellcore entwickelte S/Key.

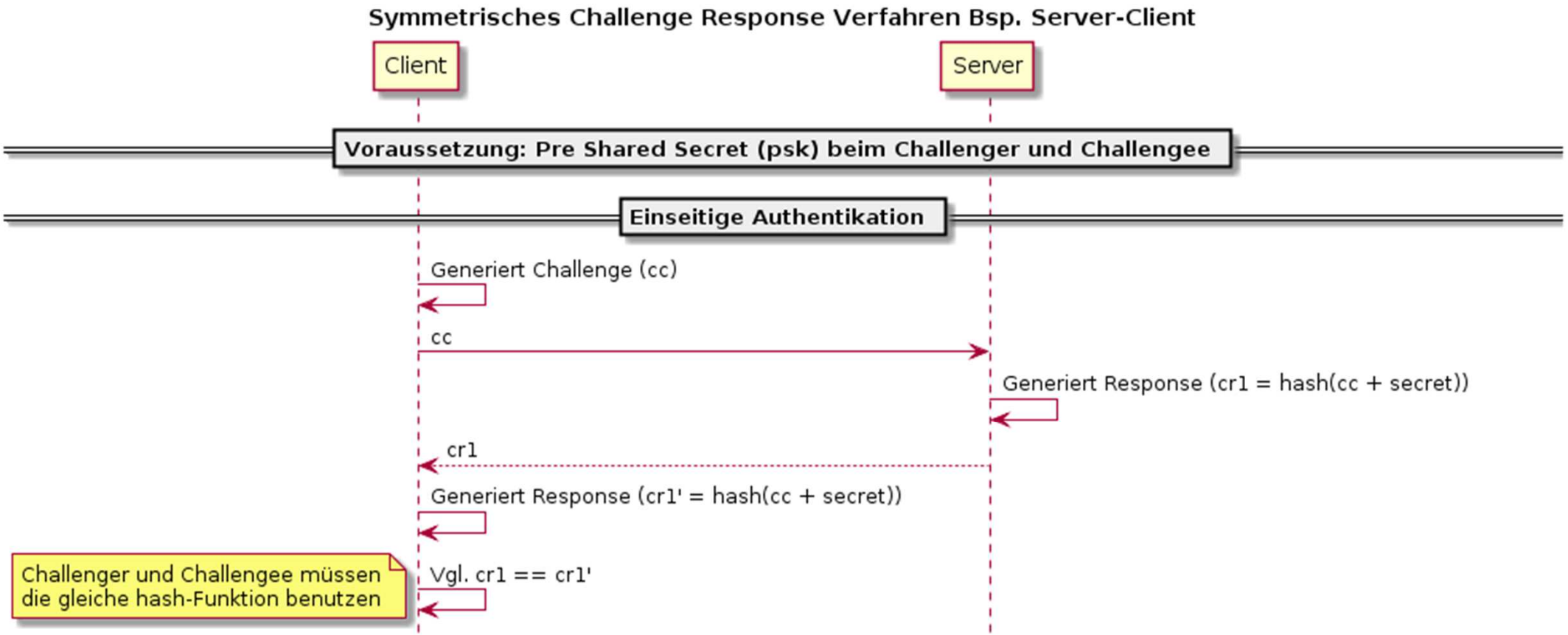
Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- **Challenge-Response-Verfahren**
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- FIDO
- Zusammenfassung

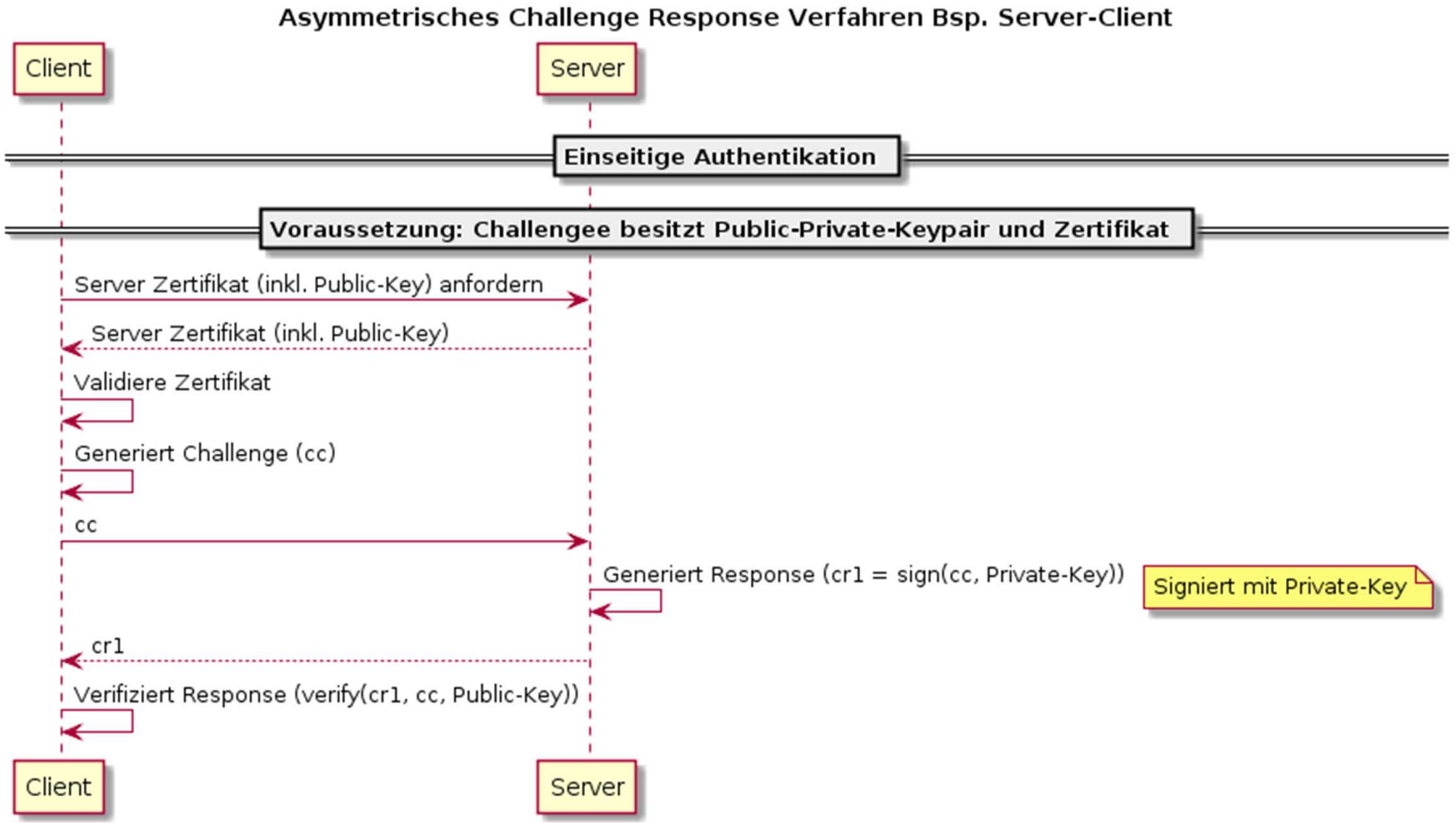
Challenge-Response-Verfahren
→ Generelle Idee



Challenge-Response-Verfahren
→ symmetrisch mit PSK



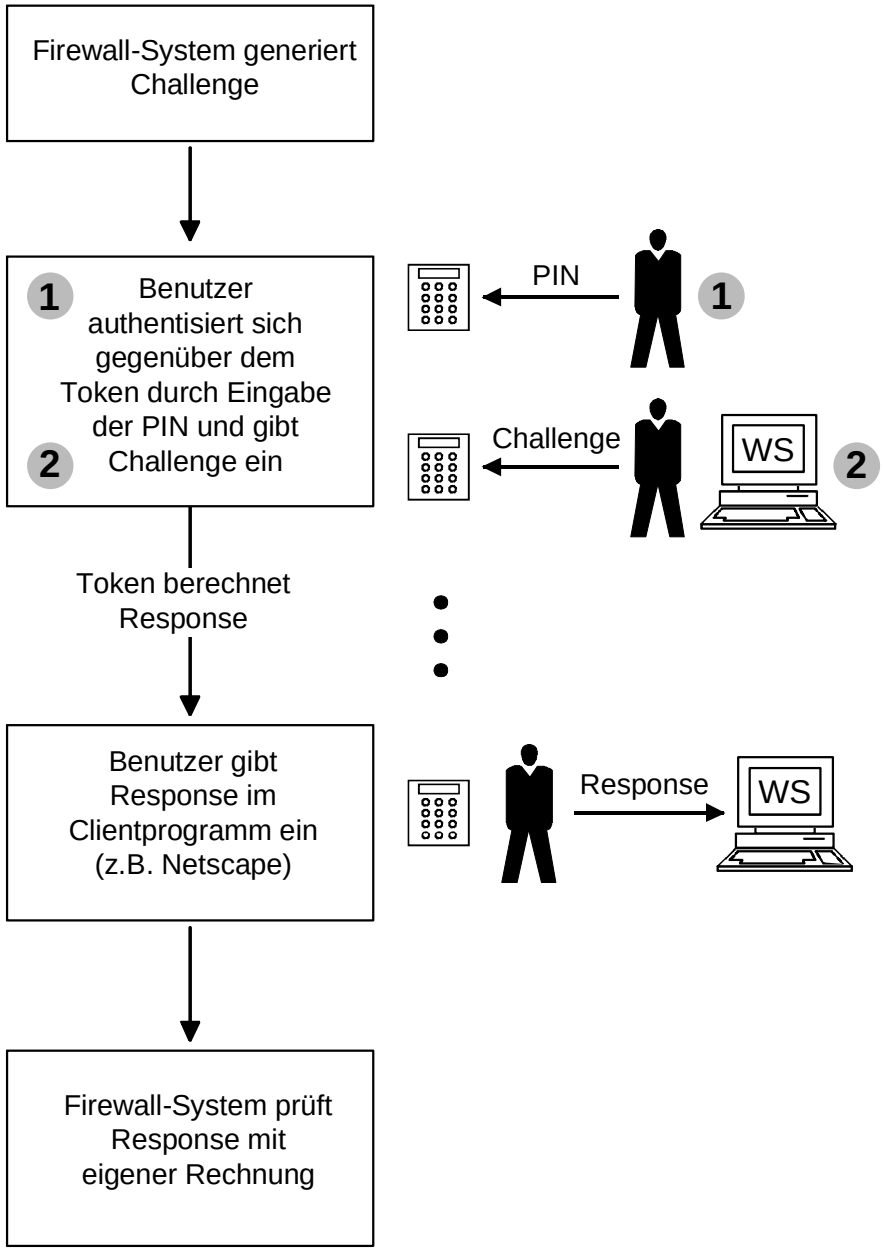
Challenge-Response-Verfahren
→ mit Public-Private-Key und Zertifikaten



Security Token (1/3)
→ Verfahren

- Benutzer hat ein persönliches Security Token
- Z.B. ein Firewall-System hat ein Sicherheitsmodul, welches Callenges für die Benutzer/Security Token berechnet
- Die Firewall sendet eine Challenge an den Benutzer
- Der Benutzer berechnet mit Hilfe des Security Tokens die Response
- Das Sicherheitsmodule muss überprüfen, ob die Response zur Challenge passt.

Security Token (2/3)
→ Ablauf



Security Token (3/3)
→ Bewertung

- **Vorteile eines Security Tokens**
  - Das Verfahren stellt keine besondere Anforderung an die Hardware und Software des Benutzers
  - Der Austausch von Challenge und Response wird über Anzeige und Tasten des Rechnersystems und des Security Token durchgeführt
  - Dieses Verfahren ist besonders sicher, da das Security Token eine sichere Hardware ist

- **Nachteile eines Security Tokens**
  - Für den Benutzer ist das Security-Token-Verfahren aufwendig, da es in mehreren Schritten durchgeführt wird
    - Aktivieren des Security Tokens
    - Eingabe der Challenge und
    - Eingabe der Response

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- **Biometrische Verfahren**
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- FIDO
- Zusammenfassung

Biometrischen Merkmalen

Aktive Merkmale (Verhalten)	Passive Merkmale (physiologisch)
Unterschriftendynamik	Irismuster
Lippenbewegung beim Sprechen	Fingerabdruck
Stimmerkennung	Gesichtserkennung
Bewegung (Gangartzyklus)	Retinamuster
Anschlagdynamik auf Tastaturen	DNA
	Thermogramm
	Handgeometrie
	Form des Ohres
	Geruch

Nutzbarkeit von biometrischen Merkmalen

- Jede physiologische oder verhaltensbedingte Eigenschaft kann als biometrisches Merkmal zur Personenidentifikation verwendet werden, sofern sie folgende Anforderungen erfüllt:
- **Universalität:**
  - jede Person muss dieses Merkmal besitzen
- **Einmaligkeit:**
  - keine zwei oder mehr Personen mit gleichem Merkmal dürfen existieren (Zwillinge)
- **Erfassbarkeit:**
  - diese Eigenschaft ist quantitativ messbar.

Akzeptanzraten (1/2)

- **FAR = False Acceptance Rate**
  - Sicherheitsmerkmal
  - Erkennung einer nichtberechtigten Person als berechtigt

$$FAR = \frac{\text{Anzahl der Vergleiche nicht affiner Merkmale, die einen Match ergeben}}{\text{Gesamtanzahl der Vergleiche nicht affiner Merkmale}}$$

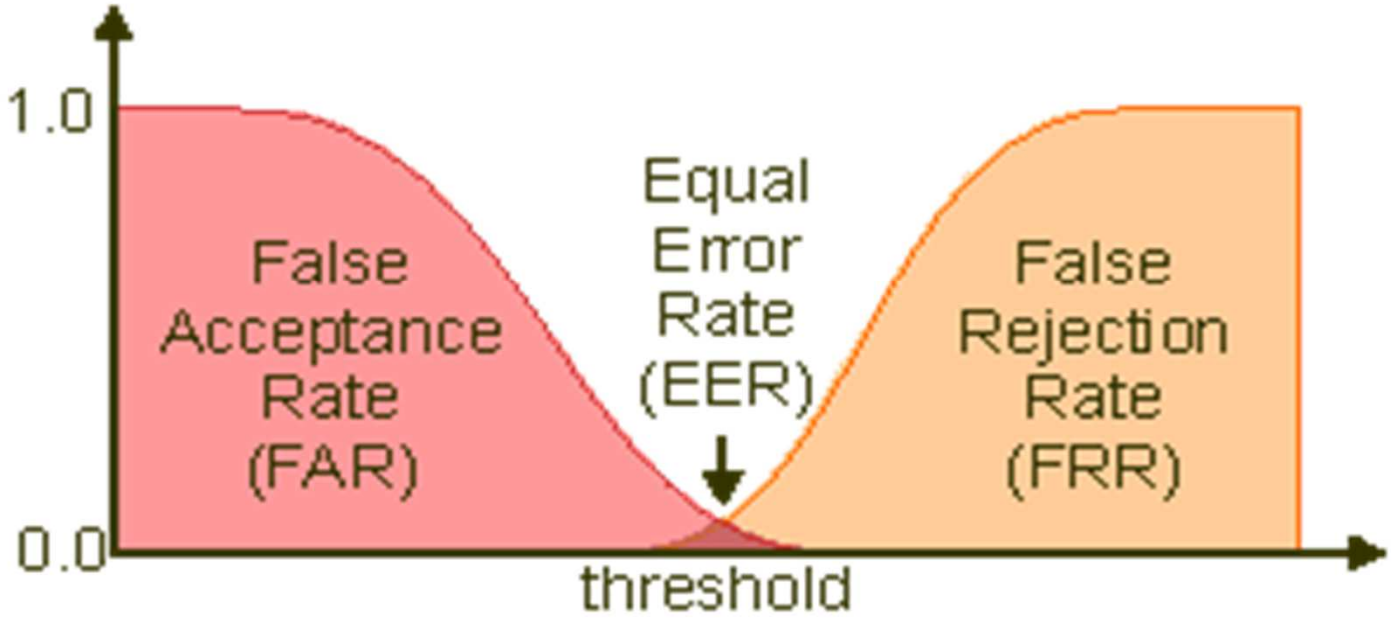
- **FRR = False Rejection Rate**
  - Komfortmerkmal
  - Unberechtigte Abweisung berechtigter Personen

$$FRR = \frac{\text{Anzahl der Vergleiche affiner Merkmale, die einen NON-Match ergeben}}{\text{Gesamtanzahl der Vergleiche affiner Merkmale}}$$

***Affinität**: Zwei Aufnahmen eines biometrischen Merkmals werden genau dann als affin bezeichnet, wenn sie vom selben Körper aufgenommen wurden.*

Akzeptanzraten (2/2)

- EER = Equal Error Rate
  - Akzeptanz und Rückweisung gleich groß

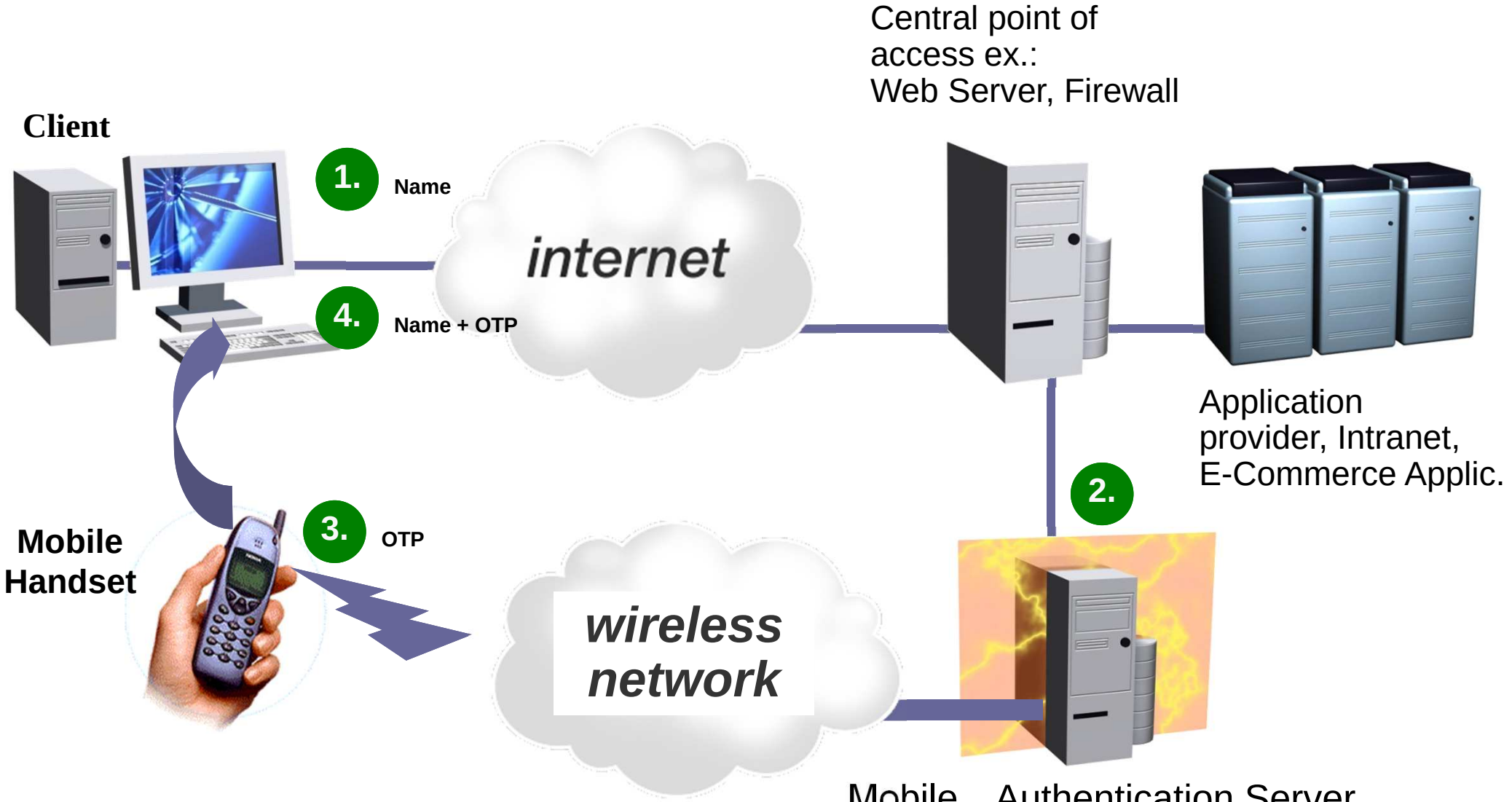


- Je niedriger die EER, desto besser die Leistung des Systems und desto geringer die Gesamtfehlerrate

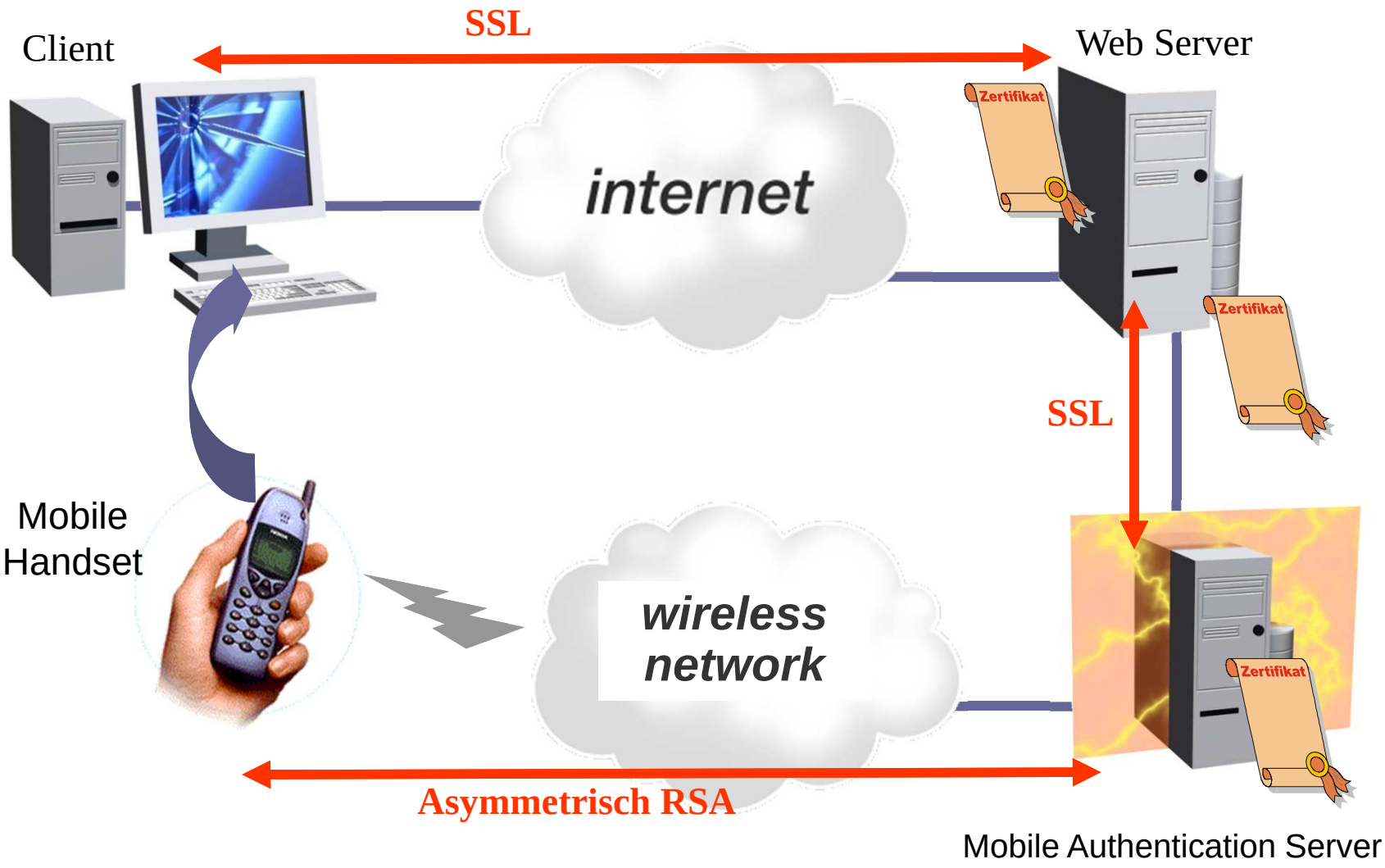
Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren
- **Authentikationsverfahren mittels Mobilfunk**
- AuthService – if(is)
- FIDO
- Zusammenfassung

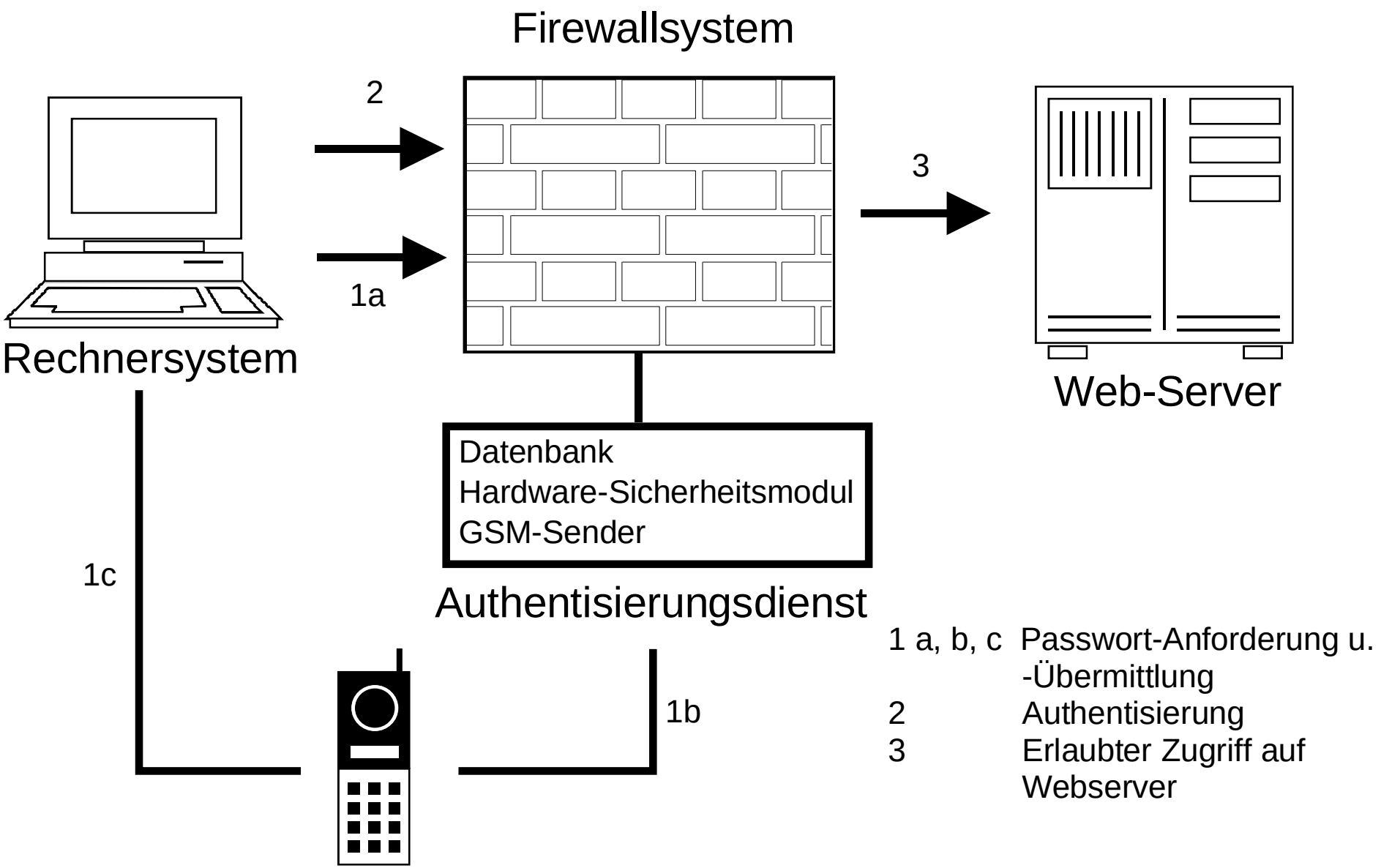
Authentikationsverfahren mittels Mobilfunk
→ Überblick (1/2)



Authentikationsverfahren mittels Mobilfunk
→ Überblick (2/2)



Authentikationsverfahren mittels Mobilfunk



1 a, b, c	Passwort-Anforderung u. -Übermittlung
2	Authentisierung
3	Erlaubter Zugriff auf Webserver

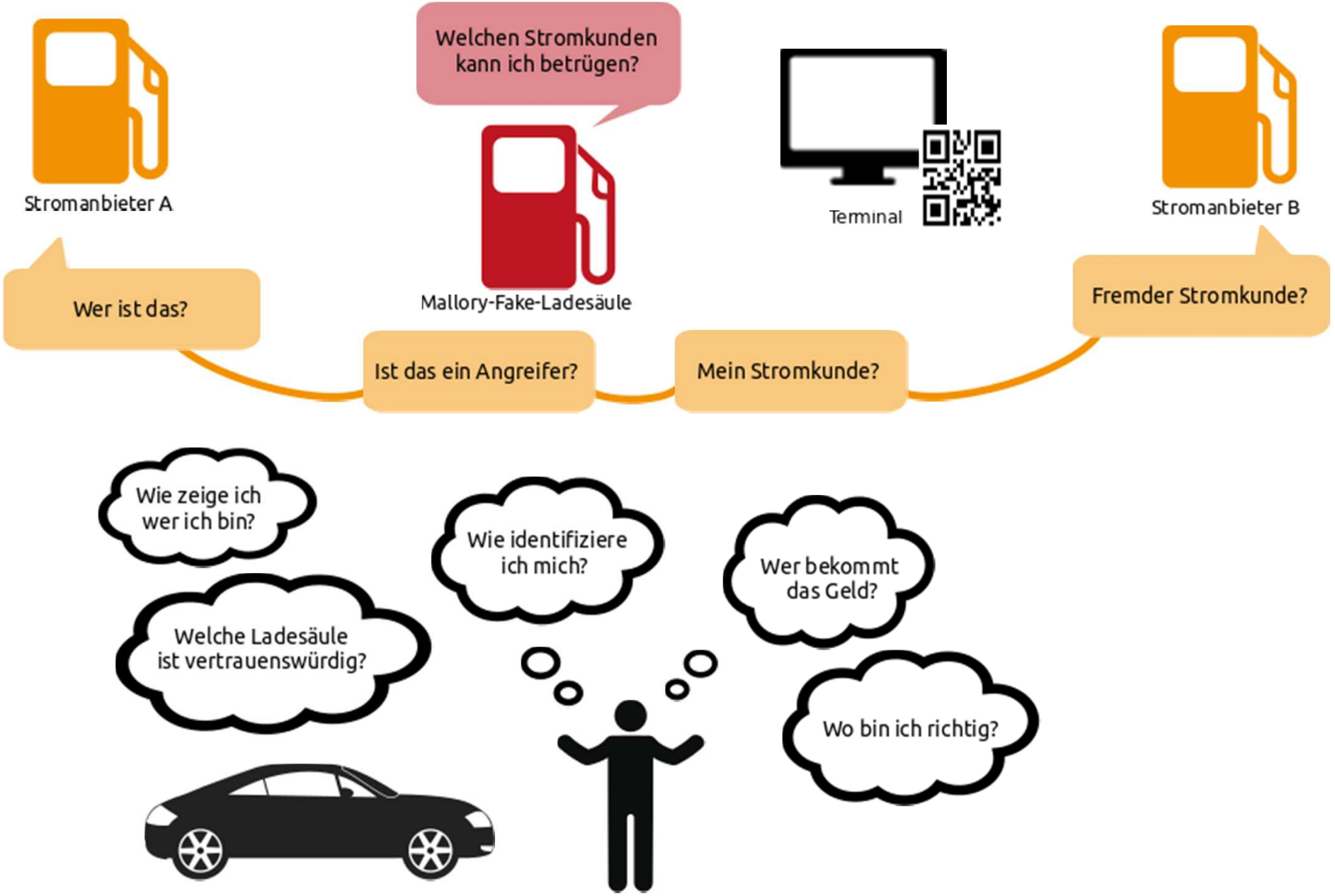
Authentikationsverfahren mittels Mobilfunk
→ Bewertung

- **Einmal Passwort**
  - Keine Speicherung des Passwortes notwendig
  - Individuelle Generierung on Demand
  - Kryptographisch starke Passwörter
- **Administration**
  - Kein Vergessen von Passwörtern mehr
    - Benutzerkomfort
    - Kostenersparnisse
  - Administration beinhaltet nur das Registrieren von Benutzern
- **Nutzung von vorhandener Infrastruktur**
  - Mobiltelefon
  - keine Software und deren Installation/Wartung auf der Client Seite notwendig
  - kann für mehrere Anwendungen verwendet werden

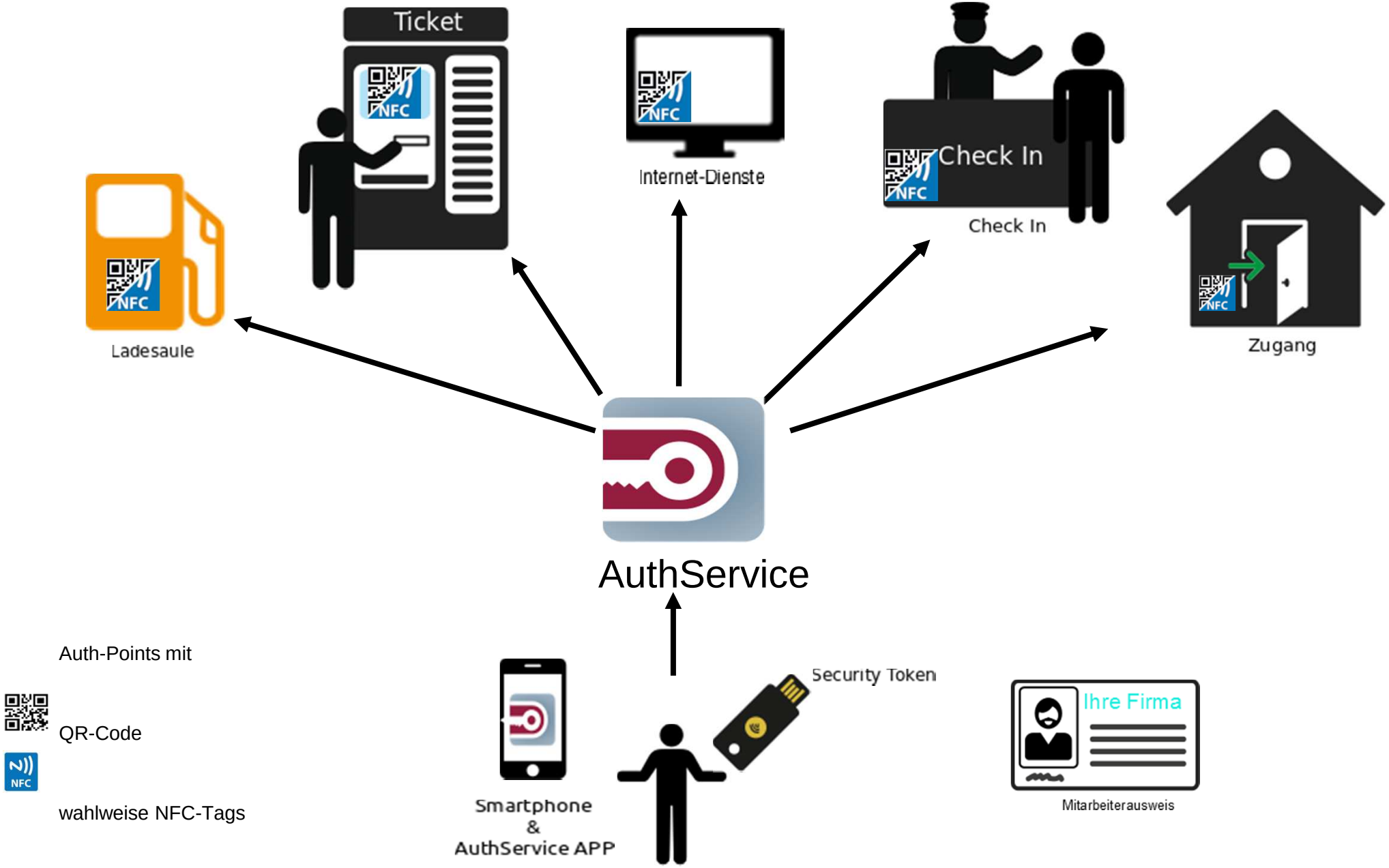
Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- **AuthService – if(is)**
- FIDO
- Zusammenfassung

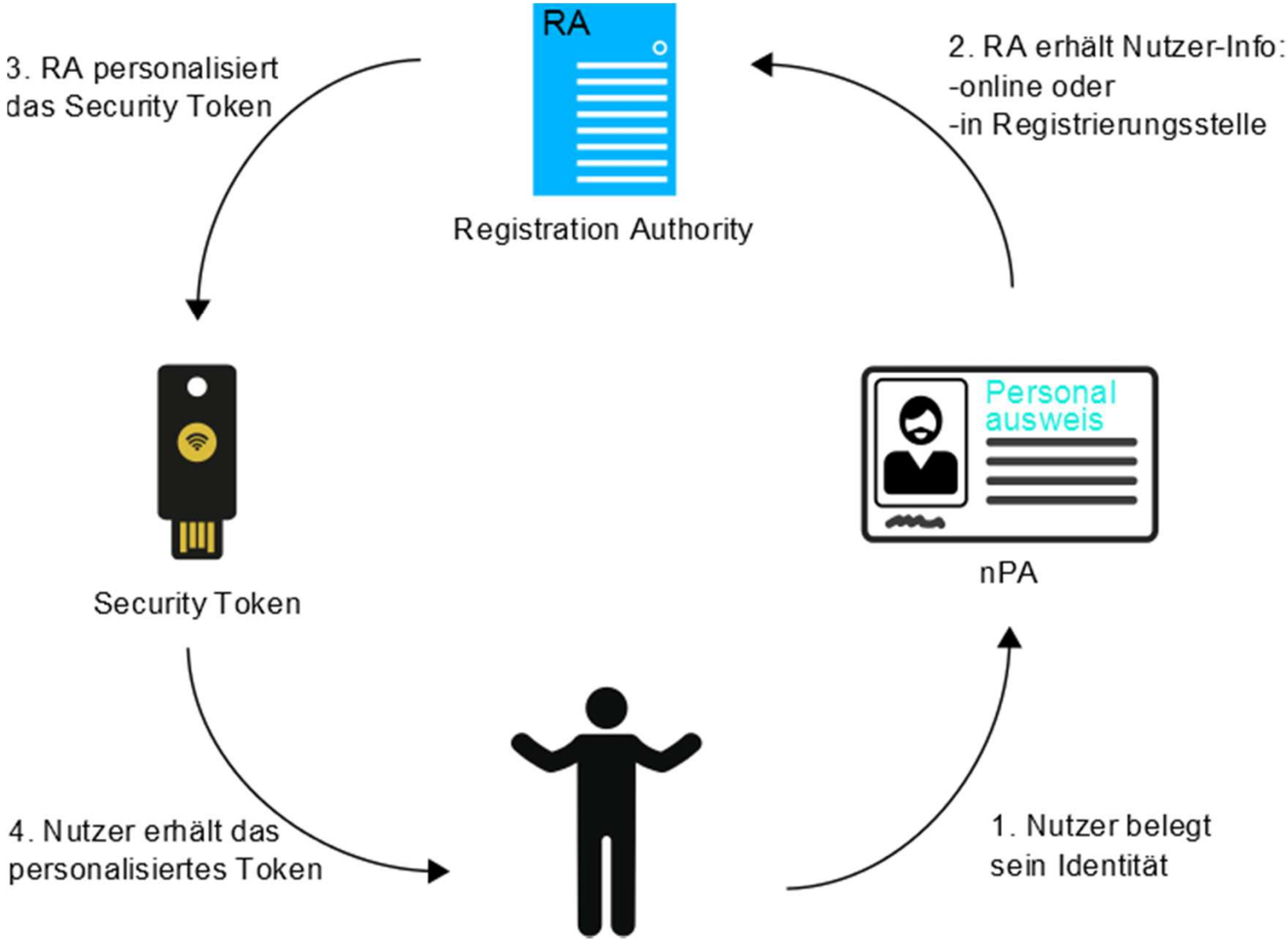
AuthService
→ Ursprung in der eMobility



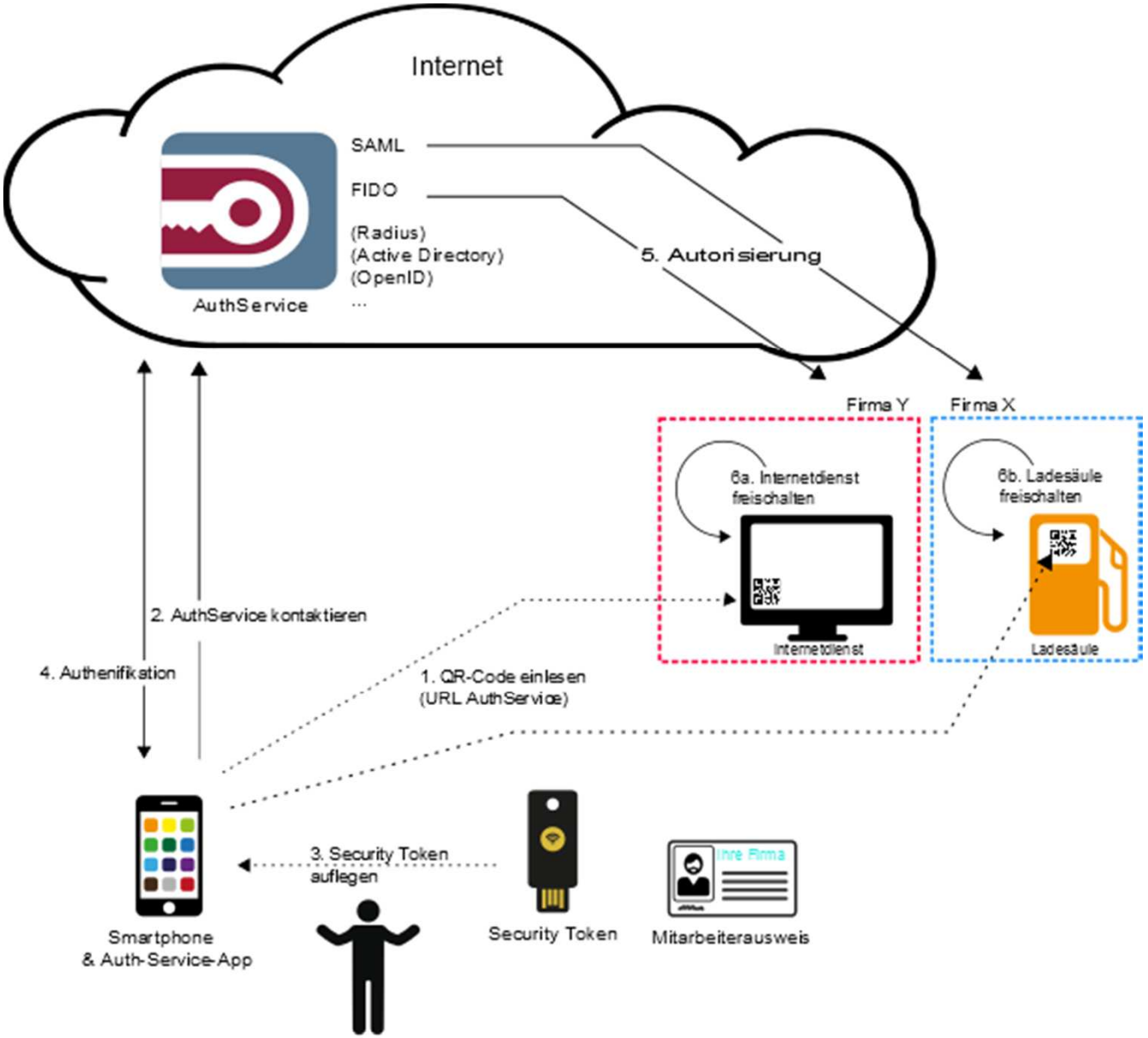
AuthService
→ Vielfältiger Einsatz



AuthService
→ Verwaltungsinstanz



AuthService
→ Identifikations- u. Authentikations-Provider

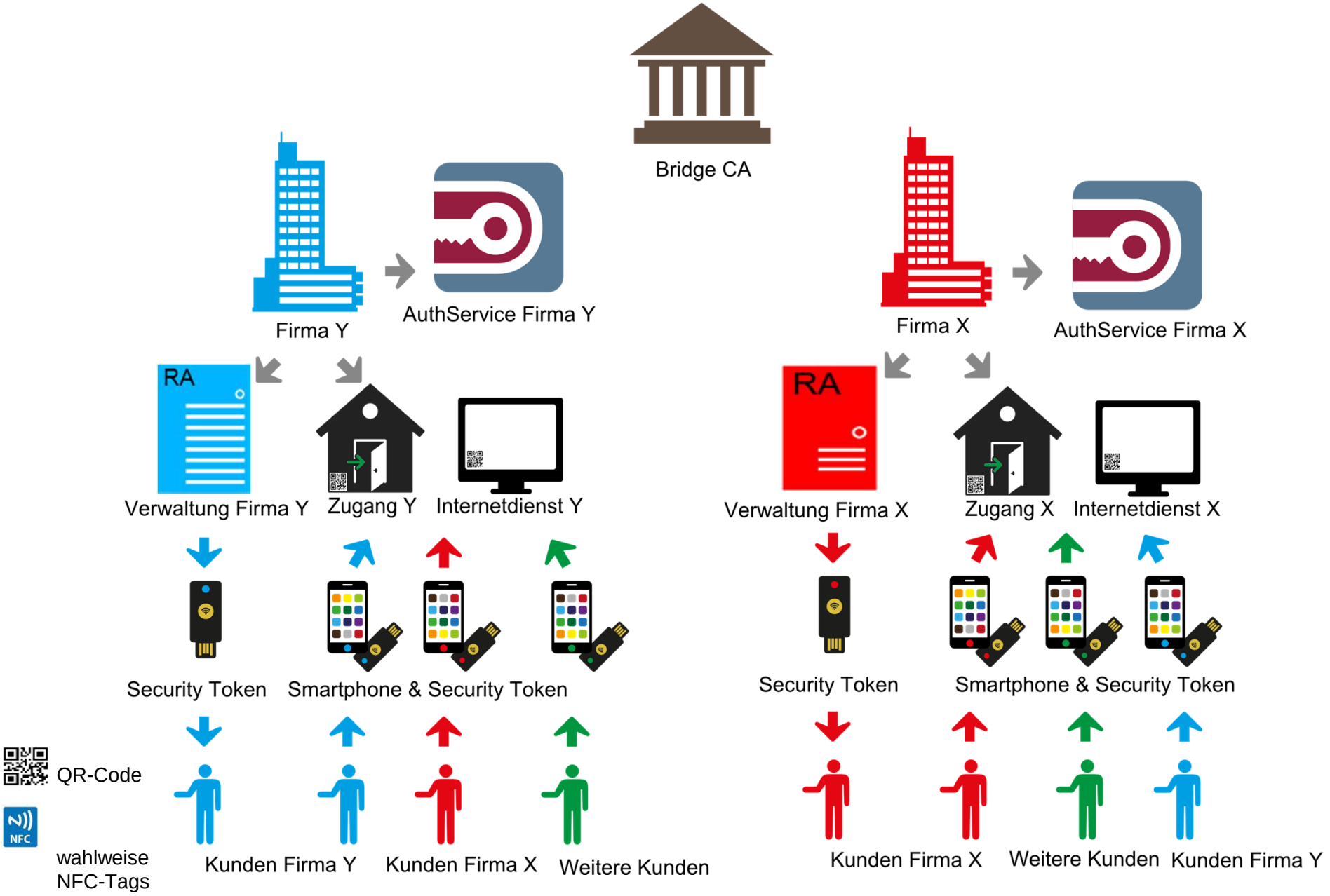


Auth-Points mit

QR-Code

wahlweise NFC-Tags

AuthService
→ für alle Dienste



AuthService
→ Zusammenfassung

- Security Token & AuthService APP & Webservice AuthService
  - Kryptographisch gesichert
  - Sichere Identifikation und starke Authentikation
    - Security Level abhängiger Einsatz von Besitz und Wissen
    - Überall sicheren Zugang gewähren
      - PC, Cloud, Automaten, Terminals, Gebäudezugang (Tür)
  - Zukünftig online: Bezahltoken & Vertragsabschluss

- Organisations- und Bereichs-übergreifender Einsatz
  - Security Token in Unternehmens PKI eingebunden
  - BridgeCA für kryptographisches Roaming
  - Einsatzbereiche: Kunden- & Mitarbeiterausweise & Gebäudeschlüssel !

AuthService
→ Einbindung

- Kostengünstige Einbindung in vorhandene Infrastruktur
  - AuthService: Webservice (1 „Rechner“) im Backend genügt
- PC & Terminals (keine Erweiterung notwendig)
- Dienst (z.B. WWW Server):
  - PHP-, Javascript- oder Plugin-Erweiterung
- Authentifizierungs- & Autorisierungsumfeld weiter einsetzbar
  - z.B. Radius, Active-Directory, **FIDO, OpenID, SAML,** …
- Security Token als Kunden-/Mitarbeiterausweis einsetzbar
- AuthService: SmartPhone APP und Security Token

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- **FIDO**
- Zusammenfassung

Wer oder was ist die FIDO Alliance?

- FIDO steht für Fast Identity Online
- FIDO Alliance besteht aus mehreren Mitglieder unter anderem:
  - Google
  - Microsoft
  - Lenovo
  - PayPal,
  - Visa
  - MasterCard
  - NXP
  - Nok Nok Lab
  - …

Ziele der FIDO Alliance

- Bereitstellung einer starken multifaktor Authentikation
  - Aufbauend auf den Fähigkeiten des jeweiligen Geräts, auf dem Authentikation durchgeführt wird
- Wahlmöglichkeiten zwischen verschiedenen Authentikationsmechanismen
- Vereinfachung der Integration neuer Authentikationsmechanismen
- Erweiterbarkeit
- Verwendung offener Standards (wenn möglich)
- Entwicklung neuer offener Standards (wenn notwendig)
- Datenschutz
- Benutzerkomfort

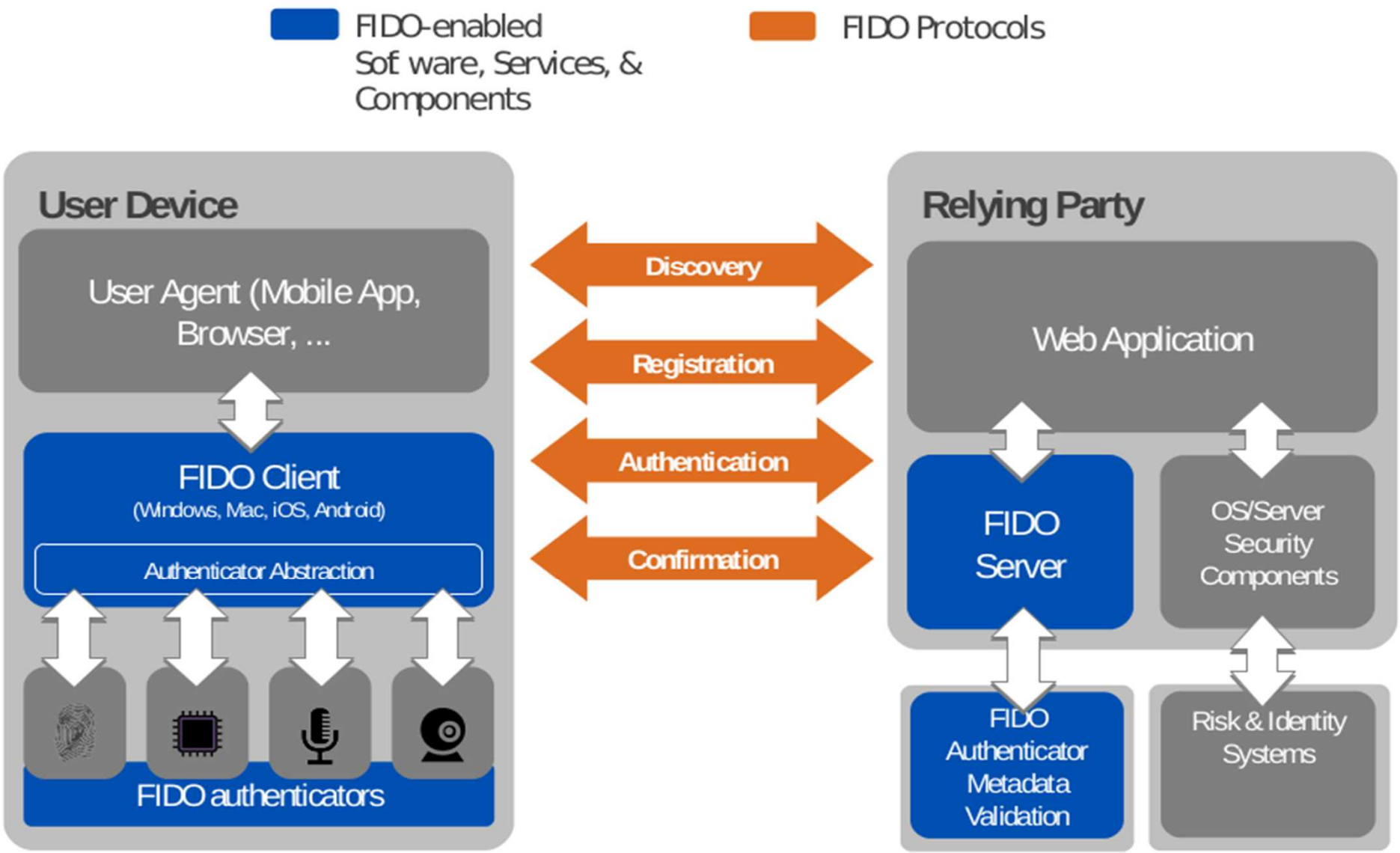
UAF vs. U2F

- Zur Erreichung der genannten Ziele, stellt die FIDO Alliance zwei Spezifikationen bereit:
  - Universal Authentication Framework (UAF)
  - Universal 2nd Factor (U2F)
- **UAF:**
  - Ziel: Bereitstellung passwortloser und multifaktor Sicherheit für Online-Dienste
  - Der User kann einen auf seinem Gerät vorhandenen Auth-Mechanismus wählen und mit einem Online-Dienst registrieren
    - z.B. Gesichtserkennung, Stimme, PIN oder Fingerabdruck
  - Nach der Registrierung kann der entsprechende Auth-Mechanismus für die Anmeldung beim Dienst verwendet werden
  - UAF erlaubt eine Filterung der verwendbaren Auth-Mechanismen durch die den Online-Dienst (=> Vertrauen in bestimmte Mechanismen)

UAF vs. U2F (Forts.)

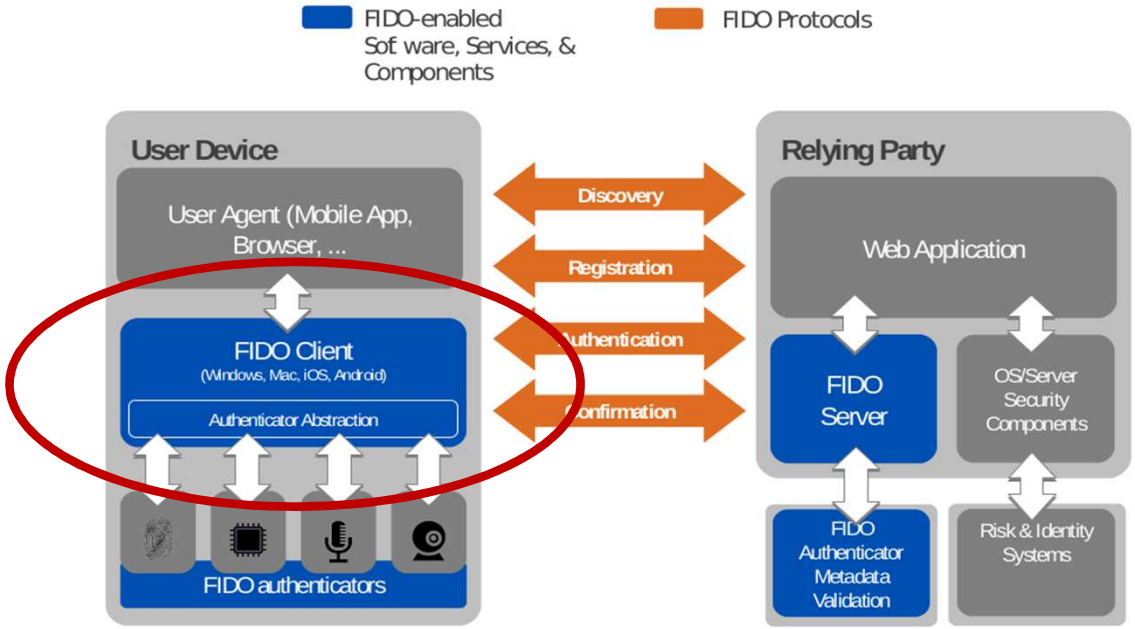
- **U2F**
  - Ziel: Verbesserung der Sicherheit eines Online-Dienstes durch zusätzliche Zwei-Faktor-Authentikation
  - Der User kann sich normal mit seinem gewohnten Mechanismus (Benutzername/Passwort) einloggen
  - Der Online-Dienst kann zu jeder Zeit einen Token (2nd Factor Device; NFC oder USB) vom Benutzer verlangen für weitere Authentikation verlangen
    - Der 2nd Factor muss dementsprechend registriert werden

Architektur



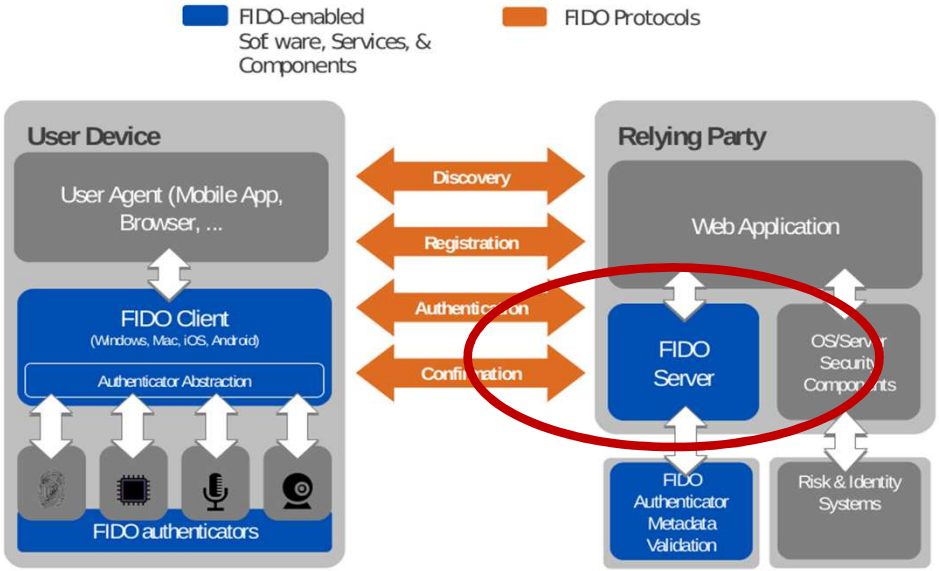
Architektur – FIDO Client

- Realisiert Client-Seite der FIDO Protokolle auf dem Gerät des Benutzers
- Interagiert mit Authenticator und User-Agent auf dem Gerät
- empfängt UAF-Protokoll-Nachrichten vom FIDO Server
- Browser-Plugin für Desktop-PCs
- Android Service
- …



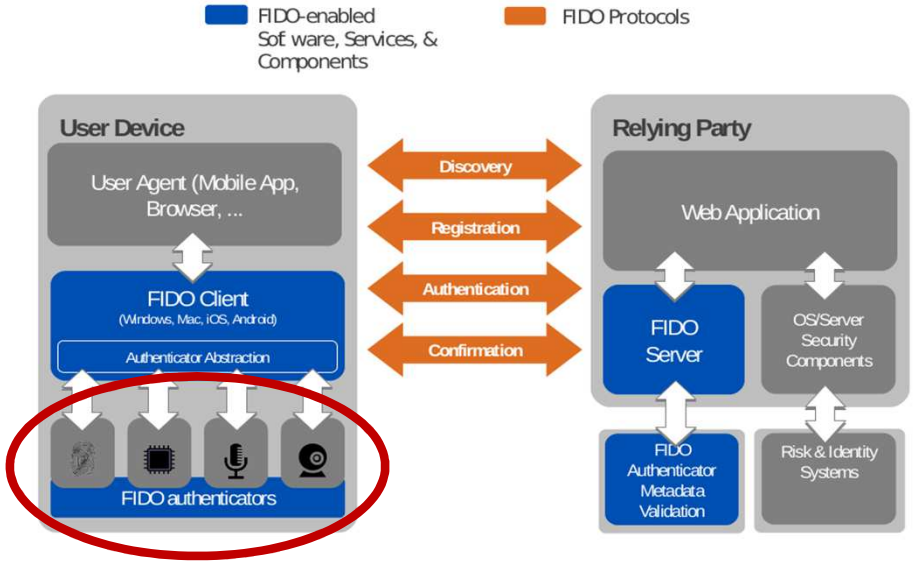
Architektur – FIDO Server

- Realisiert die Server-Seite des Protokolls
- Interagiert mit Online-Diensten
- Sendet UAF-Protokoll-Nachrichten an den FIDO-Client
- Valdiert UAF-Protokoll-Antworten
- Verwaltet FIDO-Benutzerdaten und kennt UserID des Benutzers im Online-Dienst
- Steuert die Filterung der Authentikatoren
- Als Service oder Standalone aufgestellt



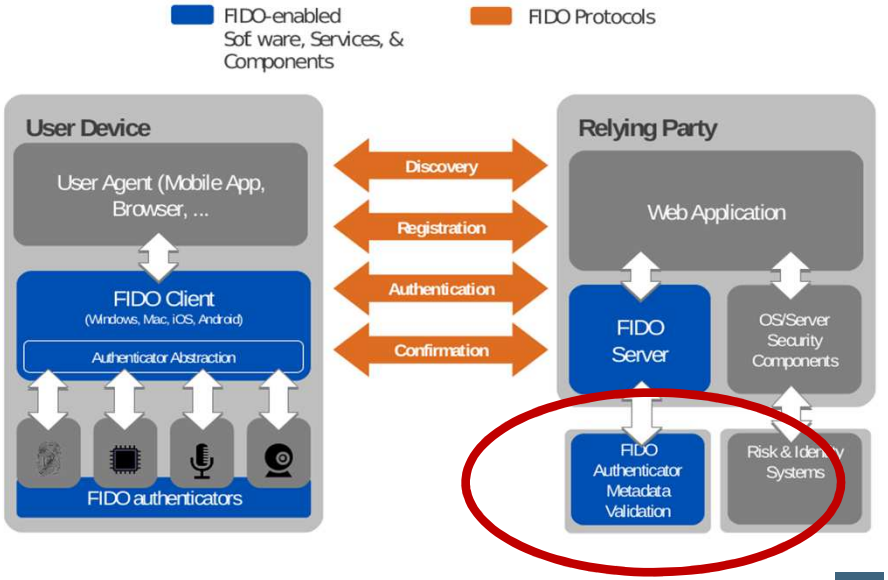
Archtiektur – FIDO Authenticator

- Sichere Entität, die auf dem Gerät des Benutzers vorhanden oder dazu verbunden ist
- Führt die Authentifizierung des Benutzers durch
- Kommuniziert mit Peripherie des Geräts (WebCam, NFC-Reader, Fingerabdrucksensor) um den User zu authentifizieren
- Kann mit externen Services kommunizieren, um den User zu authentifizieren
- Generiert Schlüsselmaterial für Nutzer
- Signiert vom FIDO-Server übermittelte Challenges
- Bereitgestellt als:
  - Dynamic Link Library (DLL; Windows)
  - Share Object (.so; Linux)
  - Service (Smartphone)

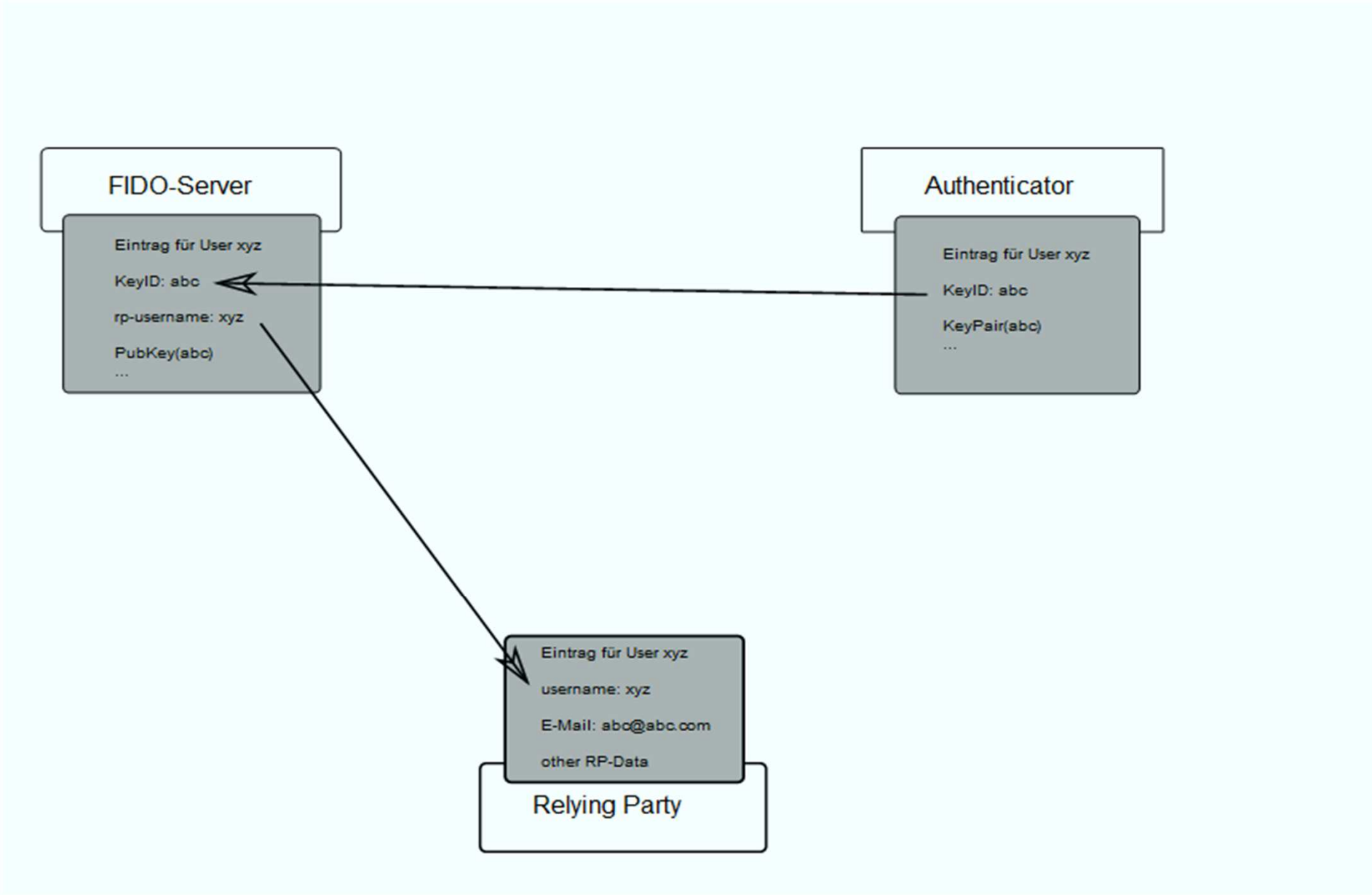


Architektur – Meta-Daten

- Informationen über die bekannten und vertrauten Authenticatoren (IDs, Fähigkeiten etc.)
- IDs der Authentikatoren werden von der FIDO Alliance vergeben (=> nur vertraute Authentikatoren können verwendet werden)
- Bilden die Grundlage für die Filterung der Auswahlmöglichkeiten des Benutzers



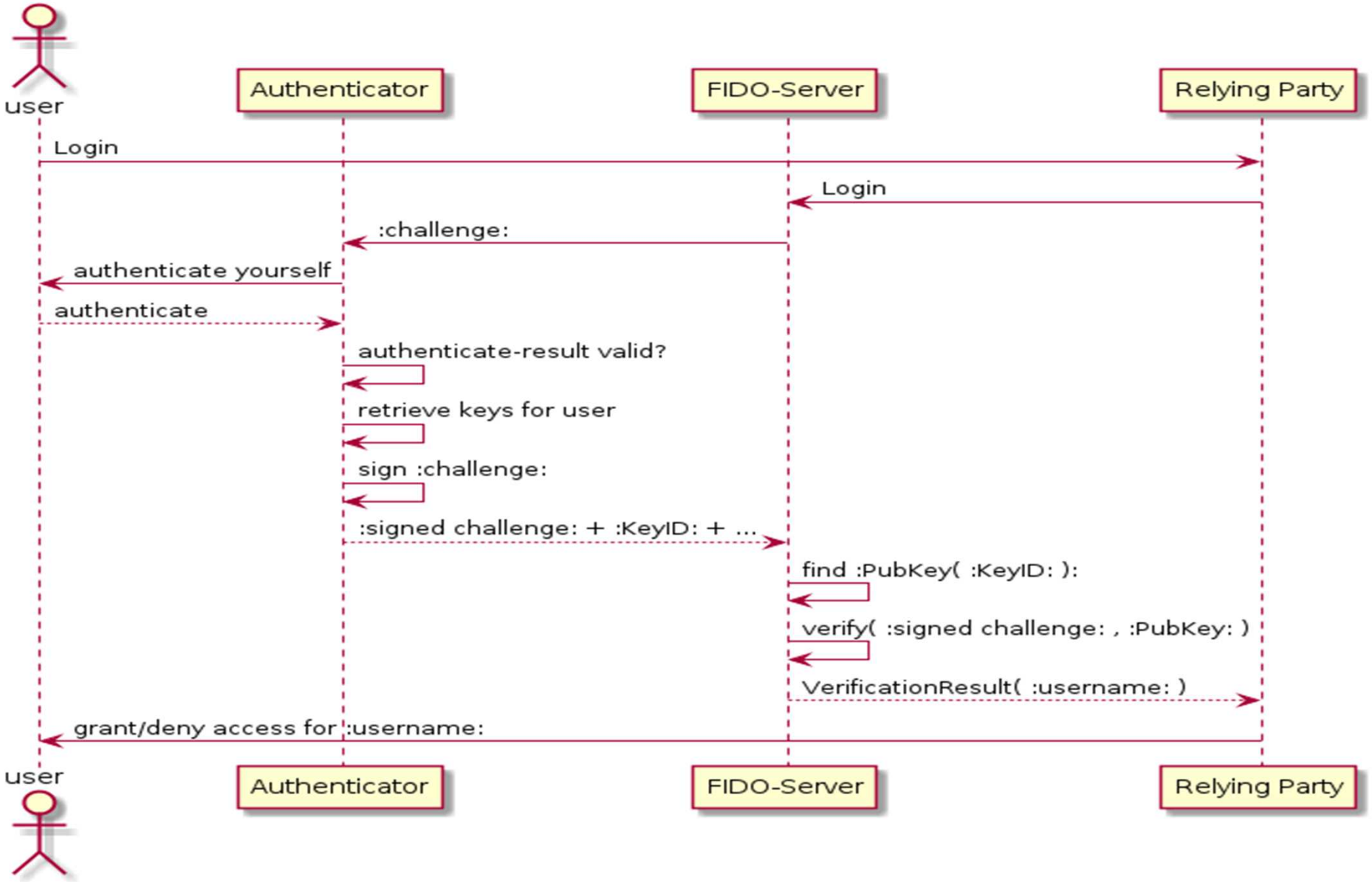
FIDO – Identifikation des Benutzers



FIDO – Identifikation des Benutzers

- Während der Registrierung speichert der Authentikator nur die benutzer-bezogenen Daten, die wichtig für die spätere Authentifizierung sind
  - KeyID (vom Authentikator generiert)
  - Schlüsselmaterial des Benutzers
  - Je nach Implementierung authentikator-spezifische Daten
- KeyID ist in der Datenbank des FIDO Servers mit weiteren Benutzerdaten assoziiert und wird für das Auffinden des Users verwendet
- Benutzerdaten enthalten unter anderem die BenutzerID des Users im Online-Dienst
  - der FIDO Server kann dem Online-Dienst das Authentkations-Ergebnis für den entsprechenden User mitteilen

FIDO – Authentifizierung des Benutzers



FIDO – Authentifizierung des Benutzers

- der Benutzer wird zweimal authentifiziert:
  - Lokal durch den Authenticator
  - Über Challenge-/Response-Verfahren durch FIDO Server
- Beim Login via FIDO UAF übermittelt der FIDO Server eine Challenge an den FIDO Client
- Der User authentifiziert sich lokal gegen den Authentikator
- Bei erfolgreicher Authentifizierung schaltet der Authentikator das Schlüsselmaterial des jeweiligen Benutzers frei und bildet die Signatur zur übermittelten Challenge
- Die generierte Signatur, die verwendete KeyID und Challenge werden an den Server übertragen
- Der Server lokalisiert über die KeyID den entsprechenden PubKey, verifiziert die Signatur (valide => Auth-Erfolg) und übermittelt das Ergebnis zusammen mit der UserID des Users an den Online-Dienst

FIDO - Besonderheiten

- Authentifizierung gegenüber dem FIDO Server und somit des Online-Dienstes ist standardisiert über ein Challenge-/Response-Verfahren
- FIDO-Client-/Authenticator-Specific-Module-Fuktionalität ist standardisiert
  - nur in Spezialfällen ist es wirklich notwendig spezielle Komponenten mit **erweiteter** Funktionalität zu implementieren
- Authentifizierung gegenüber dem Authentikator ist vom Hersteller abhängig
  - Auf welche Art und Weise der User vom Authentikator authentifiziert wird geht über die Spezifikation hinaus

FIDO UAF Protokolle

- FIDO Protokolle dienen dem Transport der Informationen zwischen den einzelnen Beteiligten
- Insgesamt gibt es 4 Arten:
  - Registration (Auffinden und Registrierung von Authentikatoren bei Online-Diensten)
  - Authentication (Authentifizierung eines Benutzers)
  - Confirmation (neben Authentifizierung zusätzliche Bestätigung einer bestimmten Transaktion)
  - Deregistration (De-Registrierung)

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren
- Authentikationsverfahren mittels Mobilfunk
- AuthService – if(is)
- FIDO
- **Zusammenfassung**

Authentikationsverfahren
→ Zusammenfassung

- Authentikationsverfahren sind die Grundlage für die Identifikation und Authentikation von Nutzern.
- Zunehmend wird es wichtiger, Authentikationsverfahren zu verwenden, die in der globalen handelnden Gesellschaft über staatliche Grenzen und Verantwortungsbereiche hinaus verwendet werden können.
- In DE haben wie den nPA (nächste Vorlesung)

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Authentikationsverfahren

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de