Authentifizierung

Max Linneweber

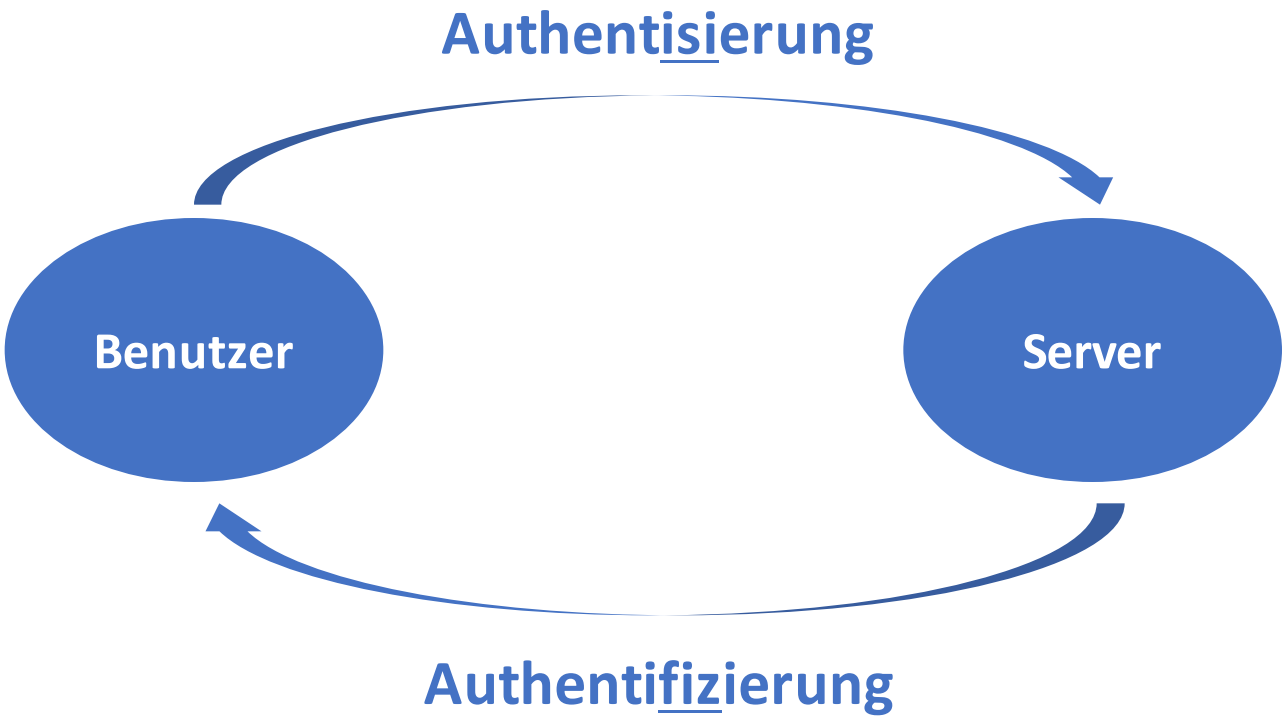
shmector.com –
Free vector art

Gliederung

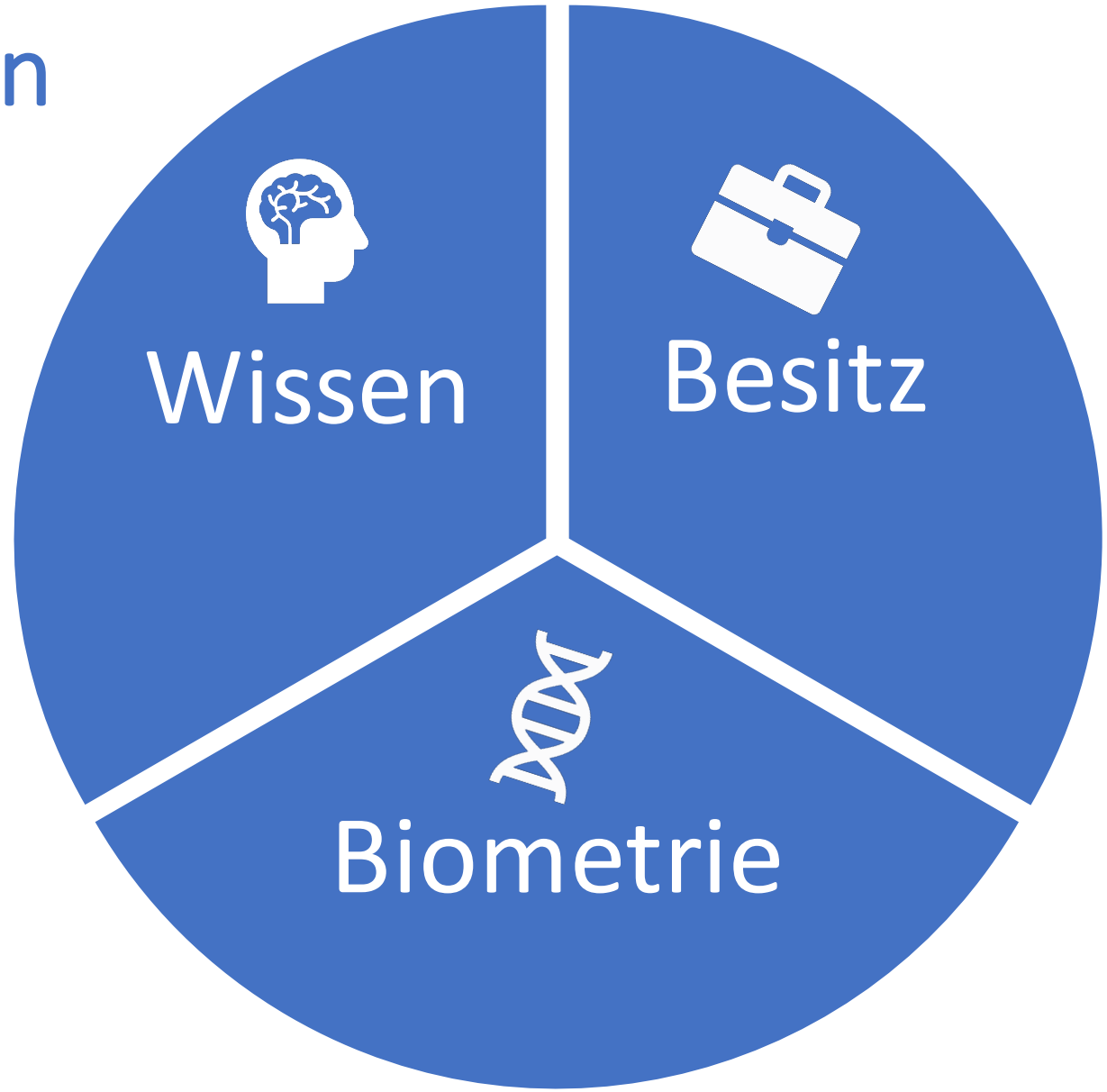
- Was ist Authentifizierung?
- Methoden
  - Authentifikation durch Wissen
  - Authentifikation durch Besitz
  - Authentifikation durch Biometrie
- Fazit – Pro/Contra
- Techniken
- Rechtliche Rahmen
- Diskussion

shmector.com – Free vector art

Was ist Authentifizierung?



Methoden



Authentifikation durch Wissen

Techniken zur Authentifikation
durch spezifisches Wissen

- Passwörter
- PINs
- Sicherheitsfragen
- Einmal-Passwörter

Authentifikation durch Wissen

Techniken zur Authentifikation durch spezifisches Wissen

- Passwörter
- PINs
- Sicherheitsfragen
- Einmal-Passwörter

- Meist verbreitete Authentifikation
- Username + Passwort
- Kryptografische Hashfunktionen zur Verschlüsselungen der gespeicherten Passwörter
- Sicherheit abhängig von Passwortwahl

Authentifikation durch Wissen in der Praxis

- Mangelhaftes oder fehlendes Sicherheitsbewusstsein
  - ➢ Passwort wird unter die Tastatur gelegt oder gar auf den Bildschirm geklebt
- Starke Passwörter werden kaum verwendet
- Keine große Motivation der Nutzer ein komplexes Passwort zu wählen
  - ➢ Kein lohnendes Ziel, kein Schadenspotential usw.

Top 10 der deutschen Passwörter*:

1. hallo
2. passwort
3. hallo123
4. schalke04
5. passwort1
6. qwertz
7. arschloch
8. schatz
9. hallo1
10. ficken

* HPI-Analyse von ca. einer Mrd. Nutzerkonten, die durch Datenlecks zugänglich sind (2016).

Passwörter

Anforderungen:

- Mind. 12 Zeichen (**Groß-, Kleinbuchstaben sowie Sonderzeichen** – sollte kein Wort aus Wörterbuch sein)
- **Kein Eigenname** oder gar Vor- oder Nachname
- Mind. 1 **Sonderzeichen**
- **Keine Zeichenfolgen** z.B. der Tastatur (qwertz)
- Möglichst **viele verschiedene Zahlen und Buchstaben**
- **Regelmäßiges wechseln** (mindestens jährlich)
- System sollte nur eine **geringe Anzahl von Fehlversuchen** akzeptieren

Authentifikation durch Besitz

Authentifikation wird in der Regel

durch Hardware realisiert

- Magnetstreifen- und Chipkarten
- USB-Token
- OTP-Token

Authentifikation durch Besitz

Authentifikation wird in der Regel durch Hardware realisiert

- Magnetstreifen- und Chipkarten
- USB-Token
- OTP-Token

- Weit verbreitete Hardwaretoken, besonders als EC-Karte
- Drei Arten:
  - Magnetstreifenkarte
  - Speicherchipkarte
  - Prozessorchipkarte

Authentifikation durch Besitz

Authentifikation wird in der Regel durch Hardware realisiert

- Magnetstreifen- und Chipkarten
- USB-Token
- OTP-Token

- Technik eines Prozessorchipkarte
- Vorteil:
  - Kein Lesegerät notwendig
  - USB-Speicher zusatznutzen

Authentifikation durch Besitz

Authentifikation wird in der Regel durch Hardware realisiert

- Magnetstreifen- und Chipkarten
- USB-Token
- OTP-Token

- OTP = One time pads
- Erzeugt durch Knopfdruck Einmalpasswörter
- Keine Zusätzliche Hardware notwendig

https://www.microcosm.com/products/oath-otp-authentication-tokens

Authentifikation durch biometrische Merkmale

Unter **biometrischen Merkmalen** versteht man **physiologische** oder **verhaltenstypische Eigenschaften** einer Person.

Anforderungen:

- Universalität
- Eindeutigkeit
- Beständigkeit
- Quantitative Erfassbarkeit
- Performanz
- Akzeptanz
- Fälschungssicherheit

https://www.expertenderit.de/blog/windows-10-unterst%C3%BCtzt-biometrische-authentifizierung

Authentifikation durch biometrische Merkmale

Funktionsweise

- Biometrische Techniken arbeiten alle nach gleichen Schema.
- Analyse von **Referenzwerten** mittels Sensoren
- Ermittlung von **charakteristischen Eigenschaften** aus den Referenzwerten
- Bei der Authentifikation wird der Referenzwert mit dem zu autorisierenden Nutzer vergleichen

- Fingerabdruck
- Handgeometrie
- Iris und Retina
- Gesichtserkennung
- Stimme
- Viele neue Techniken in Forschung

Fazit der Authentifikationstechniken

Authentifikation durch Wissen

Vorteile:

- Einfach zu implementieren
- Theoretisch sicher
- Keine zusätzliche Technik

Nachteile:

- Stark abhängig von dem gewählten Passwort
- Schwierig zu merken bei vielen verschiedenen Zugängen
- Leicht zu übertragen

Authentifikation durch Besitz

Vorteile:

- Kein Merken
- Vertrautheit (Bankkarte)
- Hohe Sicherheit

Nachteile:

- Schnittstelle muss vorhanden sein
- Aufwendiger in der Umsetzung
- Hardware muss transportiert werden

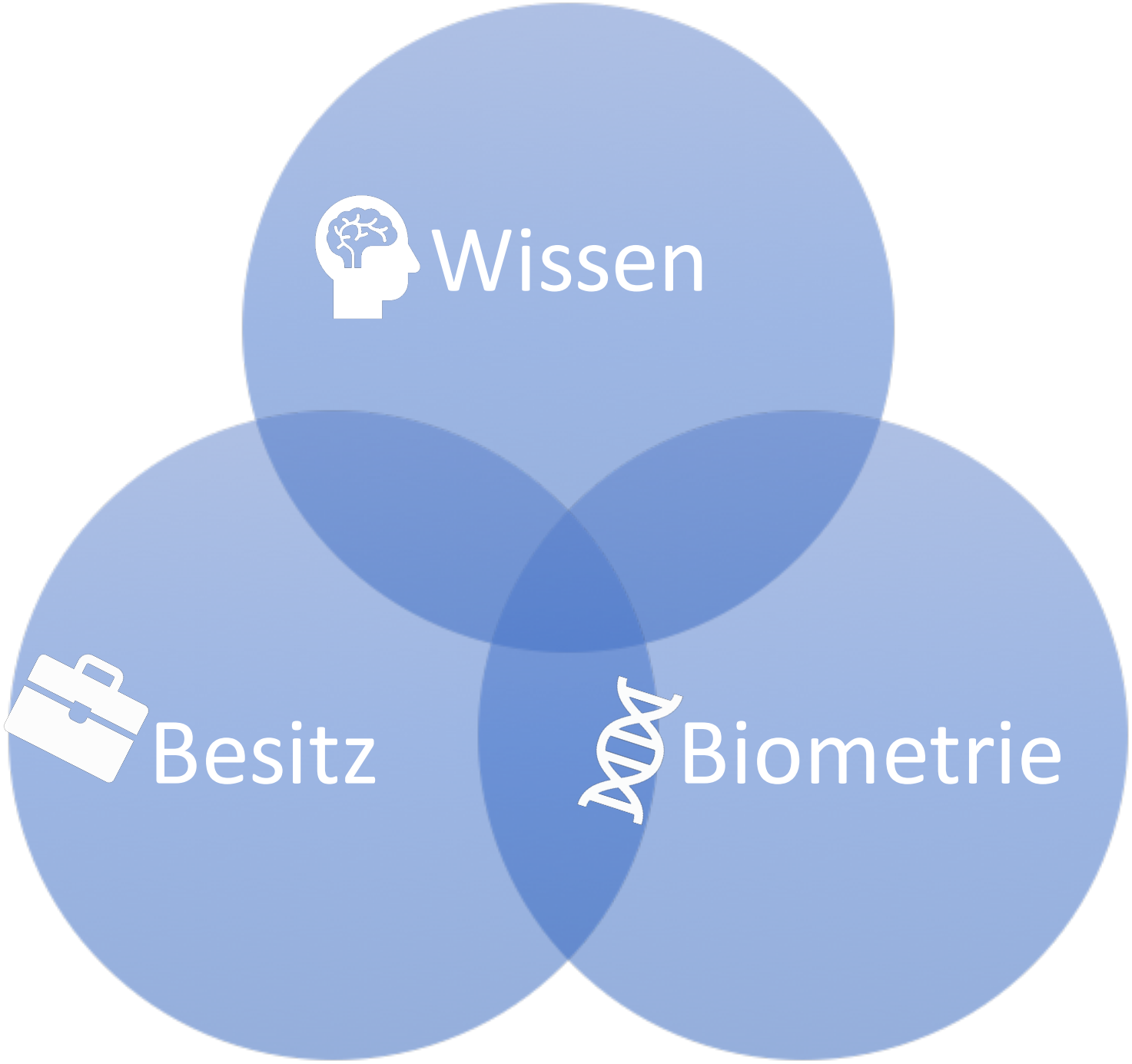
Authentifikation durch Biometrie

Vorteile:

- Hohe Sicherheit
- Kein Transport/Merken notwendig

Nachteile:

- Aufwendig in der Umsetzung
- Zusätzliche Hardware
- Hohe Kosten


Wissen
Besitz
Biometrie

Techniken

Einfache Authentifizierung	Two-Factor-Authentifizierung	Multi-Faktor-Authentifizierung
Username + Passwort	Zusätzliche Merkmale durch Gegenstand	Information, Gegenstand, biometrisch

Rechtliche Grundlagen

BSI – Bundesamt für Sicherheit in der Informationstechnik:

- M 4.133 Geeignete Auswahl von Authentikationsmechanismen
  - Eindeutige Identifizierung und Authentisierung
  - Speicherung der Authentisierungsinformationen nur für autorisierte Benutzer
  - Daten dürfen nur für eindeutig identifizierte und authentisierte Nutzer verfügbar sein
  - Für sicherheitskritische Anwendungen sollten starke Authentisierung verwendet werden – Zwei-Faktor-Authentisierung (Passwort + Einmalpasswort oder Chipkarte)
- Vieles mehr (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04133.html)

Diskussion

- **Was wäre eurer Meinung nach eine Sinnvolle Lösung, um die Sicherheit zu erhöhen?**
- **Welche der drei Authentifizierungsmethoden findet ihr am sinnvollsten und warum?**
- **Wie wird sich die Authentifizierung in Zukunft verändern? – Zukunftsvisionen?**

Quellen

- Claudia Eckert: IT-Sicherheit Konzepte-Verfahren-Protokolle
- IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html
- Security Insider: https://www.security-insider.de/was-ist-authentifizierung-a-617991/
- Schneider, Jan, Katrin Franke, and Bertram Nickolay. "Biometrische Authentifikation." *E-Commerce und E-Payment*. Gabler Verlag, 2001. 123-135.
- Maus, Thomas. "Das Passwort ist tot—lang lebe das Passwort!." *Datenschutz und Datensicherheit-DuD* 32.8 (2008): 537-542.