Hochschule Düsseldorf
University of Applied Sciences

HSD

Sicherheitsstandards Identifikation und Authentifikation

Modul D3.2

Referent: Dr. Jörg Cosfeld

Passwortverfahren - Gefahren

Einmal Passwort Verfahren

- Eine Replay Attacke wird ausgeschlossen

Passwortverfahren - Gefahren

Einmal Passwort Verfahren

- Eine Replay Attacke wird ausgeschlossen

Man in the Middle – ist immer noch möglich!

Passwortverfahren - Gefahren

Einmal Passwort Verfahren

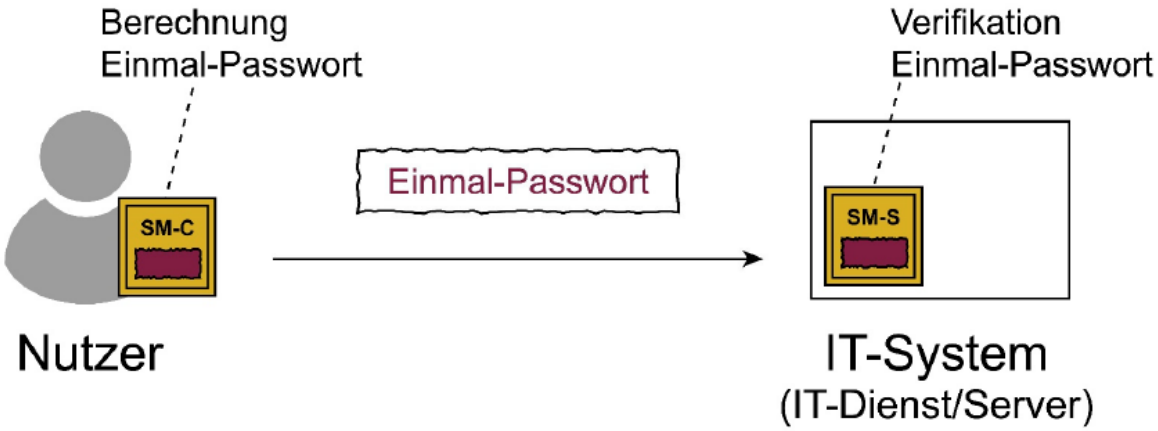
- Eine Replay Attacke wird ausgeschlossen

Man in the Middle – ist immer noch möglich!

Aufwand ist jedoch sehr hoch

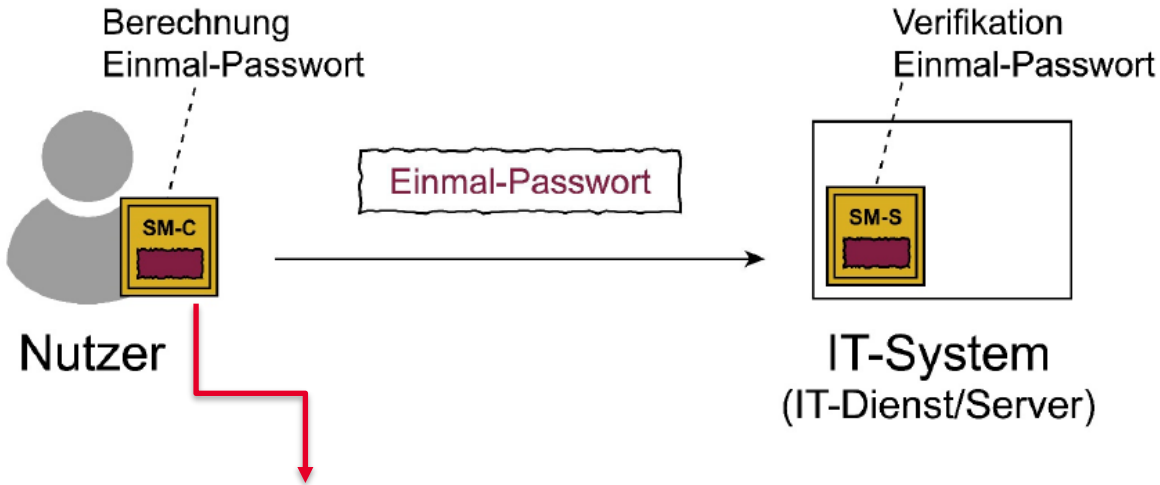
Passwortverfahren - Gefahren

Einmal Passwort Verfahren



Passwortverfahren - Gefahren

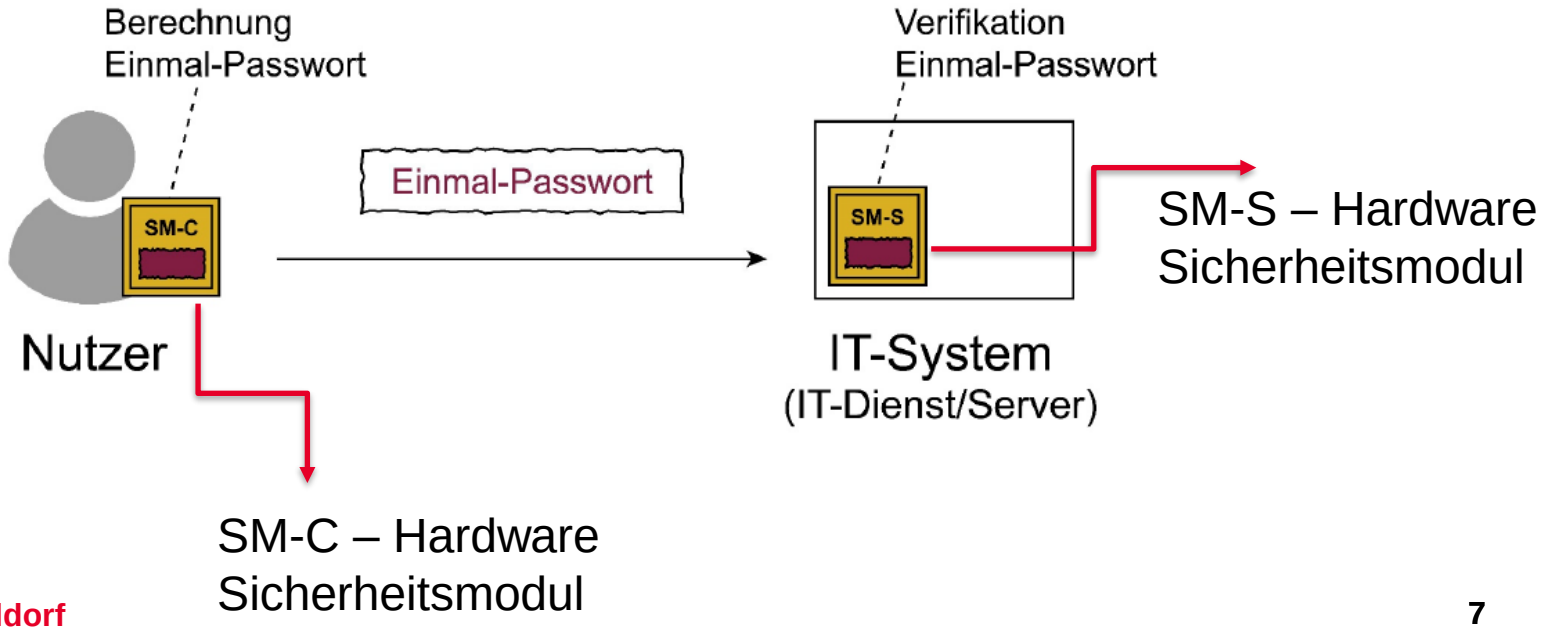
Einmal Passwort Verfahren



SM-C – Hardware Sicherheitsmodul

Passwortverfahren - Gefahren

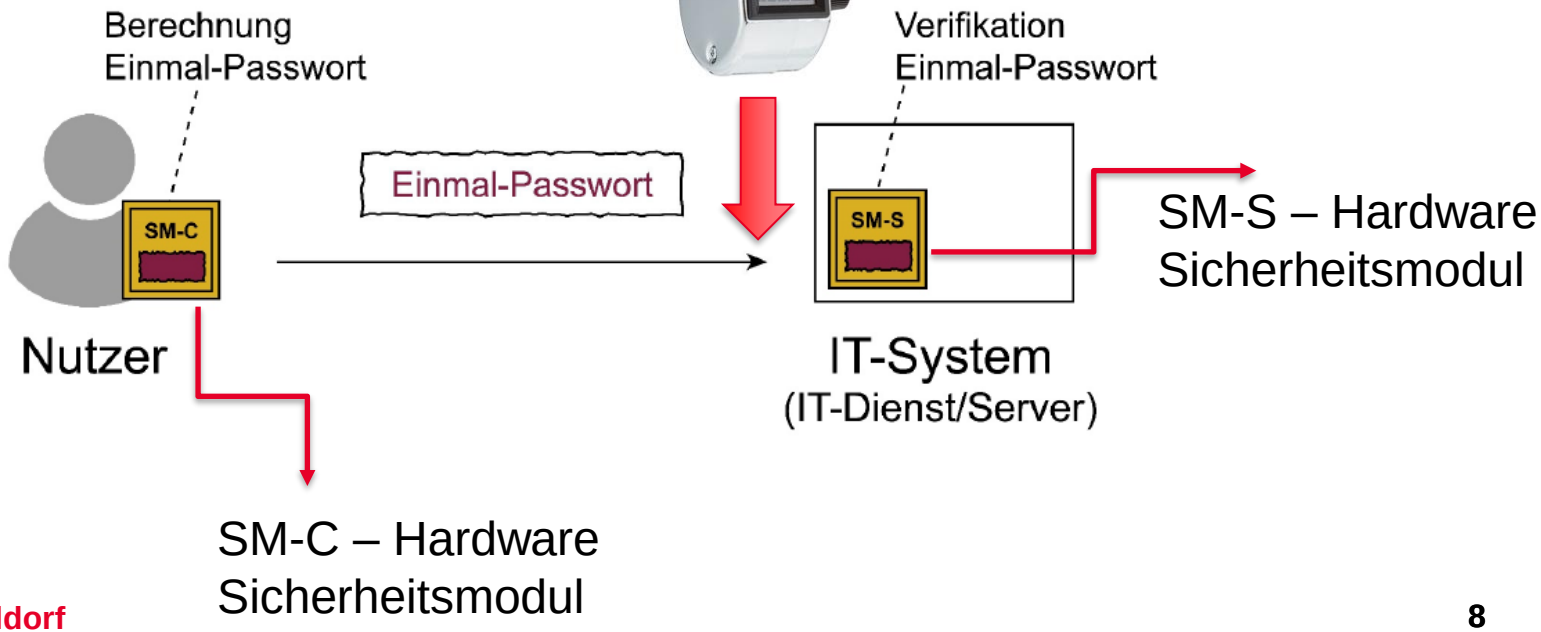
Einmal Passwort Verfahren



Passwortverfahren - Gefahren

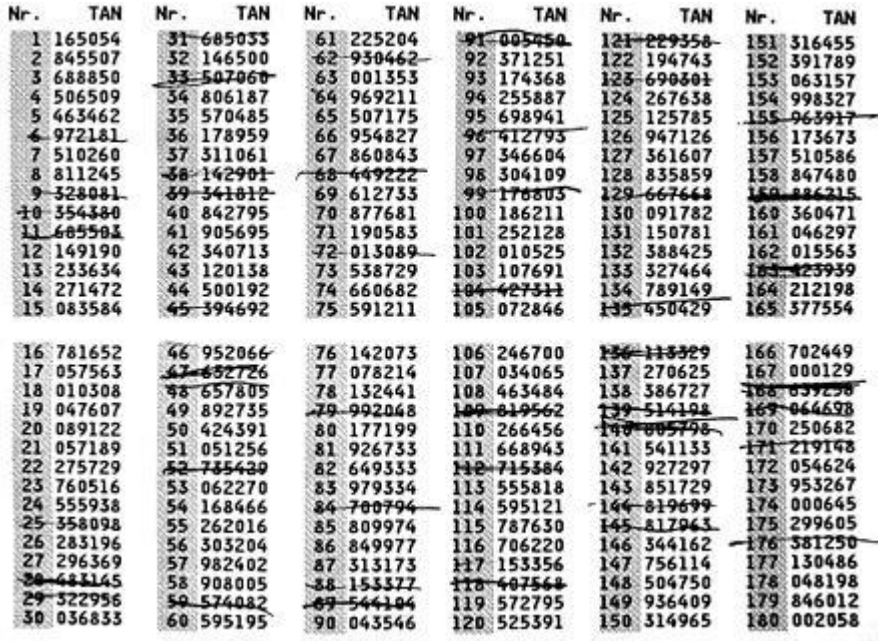
Einmal Passwort Verfahren

Wie oft gibt der User das PW ein?



Passwortverfahren - Gefahren

Einmal Passwort Verfahren



Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN
1	165054	31	685033	61	225204	91	005450	121	229358	151	316455
2	845507	32	146500	62	930462	92	371251	122	194743	152	391789
3	688850	33	507060	63	001353	93	174368	123	690301	153	063157
4	506509	34	806187	64	969211	94	255887	124	267638	154	998327
5	463462	35	570485	65	507175	95	698941	125	125785	155	963917
6	972181	36	178959	66	954827	96	412793	126	947126	156	173673
7	510260	37	311061	67	860843	97	346604	127	361607	157	510586
8	811245	38	142901	68	449222	98	304109	128	835859	158	847480
9	328081	39	341812	69	612733	99	176803	129	667668	159	886215
10	354380	40	842795	70	877681	100	186211	130	091782	160	360471
11	685503	41	905695	71	190583	101	252128	131	150781	161	046297
12	149190	42	340713	72	013089	102	010525	132	388425	162	015563
13	233634	43	120138	73	538729	103	107691	133	327464	163	423939
14	271472	44	500192	74	660682	104	427311	134	789149	164	212198
15	083584	45	394692	75	591211	105	072846	135	450429	165	377554
16	781652	46	952066	76	142073	106	246700	136	113329	166	702449
17	057563	47	652726	77	078214	107	034065	137	270625	167	000129
18	010308	48	657805	78	132441	108	463484	138	386727	168	839258
19	047607	49	892735	79	992048	109	819562	139	514198	169	064698
20	089122	50	424391	80	177199	110	266456	140	805798	170	250682
21	057189	51	051256	81	926733	111	668943	141	541133	171	219148
22	275729	52	785439	82	649333	112	715384	142	927297	172	054624
23	760516	53	062270	83	979334	113	555818	143	851729	173	953267
24	555938	54	168466	84	700794	114	595121	144	819699	174	000645
25	358098	55	262016	85	809974	115	787630	145	817963	175	299605
26	283196	56	303204	86	849977	116	706220	146	344162	176	381250
27	296369	57	982402	87	313173	117	153356	147	756114	177	130486
28	483145	58	908005	88	153377	118	407568	148	504750	178	048198
29	322956	59	574082	89	544104	119	572795	149	936409	179	846012
30	036833	60	595195	90	043546	120	525391	150	314965	180	002058

Passwortverfahren - Gefahren

Einmal Passwort Verfahren

- Auch hier Einsatz von Hash-Funktionen
  - Es folgt: kurzzeitig gültiges Einmal PW

Einmal-Passwort = f (Zeit || GX)

f: Kryptographische Funktion (One-Way-Hashfunktion, Verschlüsselungsverfahren)
Zeit: Eine relative oder absolute Zeitangabe
GX: Geheimnis des Nutzers (X)

Passwortverfahren - Gefahren

Einmal Passwort Verfahren

- Auch hier Einsatz von Hash-Funktionen
  - Es folgt: kurzzeitig gültiges Einmal PW

Einmal-Passwort = f (Zeit || GX)

f: Kryptographische Funktion (One-Way-Hashfunktion, Verschlüsselungsverfahren)
Zeit: Eine relative oder absolute Zeitangabe
GX: Geheimnis des Nutzers (X)

Beide Seiten müssen f und GX kennen!

Passwortverfahren - Gefahren

Einmal Passwort Verfahren

- Auch hier Einsatz von Hash-Funktionen
  - Es folgt: kurzzeitig gültiges Einmal PW

Einmal-Passwort = f (Zeit || GX)

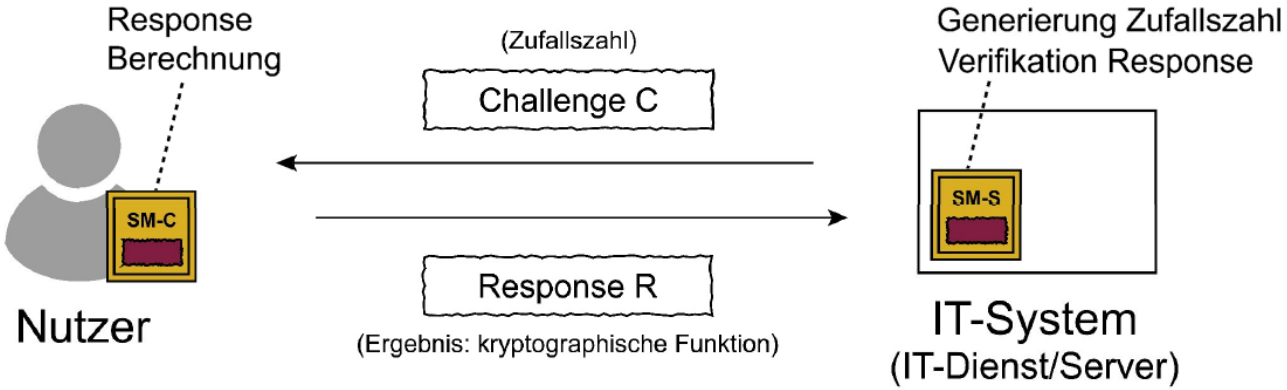
f: Kryptographische Funktion (One-Way-Hashfunktion, Verschlüsselungsverfahren)
Zeit: Eine relative oder absolute Zeitangabe
GX: Geheimnis des Nutzers (X)

GX = H (Nutzername || Master-Schlüssel) → Wird auf beiden Seiten berechnet.

Passwortverfahren - Gefahren

Challenge-Response Verfahren

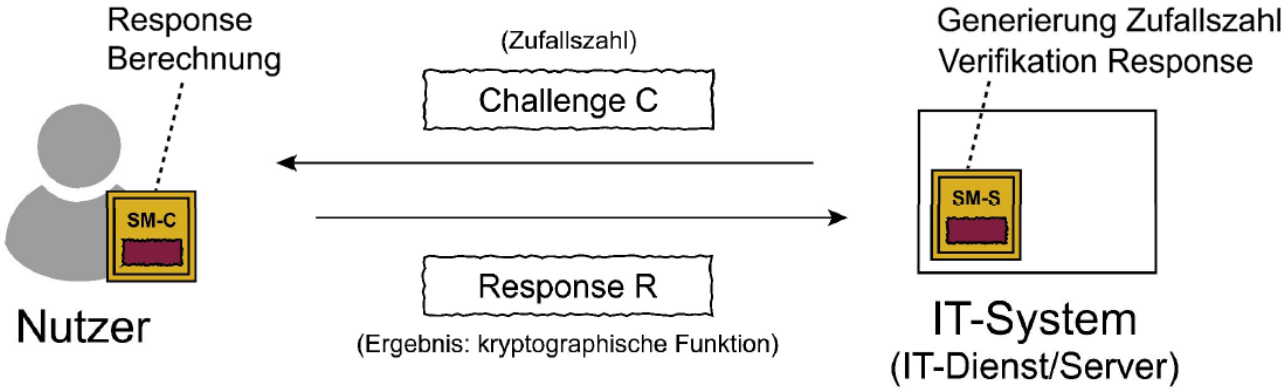
Durchführung einer spontanen kryptographischen Operation



Passwortverfahren - Gefahren

Challenge-Response Verfahren

Durchführung einer spontanen kryptographischen Operation

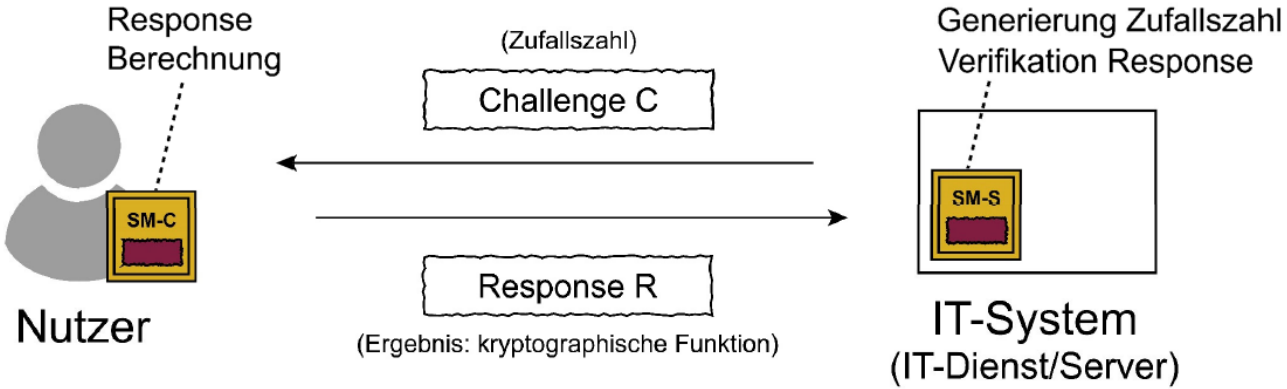


SM-C und SM-S wieder vorhanden

Passwortverfahren - Gefahren

Challenge-Response Verfahren

Durchführung einer spontanen kryptographischen Operation



SM-C und SM-S wieder vorhanden

Kryptologische Funktion in SM-C und SM-S berechnet

Passwortverfahren - Gefahren

Challenge-Response Verfahren

Durchführung einer spontanen kryptographischen Operation

$$\text{Response} = H (C \,||\, G_X)$$

H: One-Way-Hashfunktion
C: Zufallszahl (Challenge), die gehasht werden soll
G_X: Geheimnis des Nutzers (X), dessen Besitz bewiesen werden soll

$$G_X = H (C \,||\, \text{Master-Schlüssel})$$

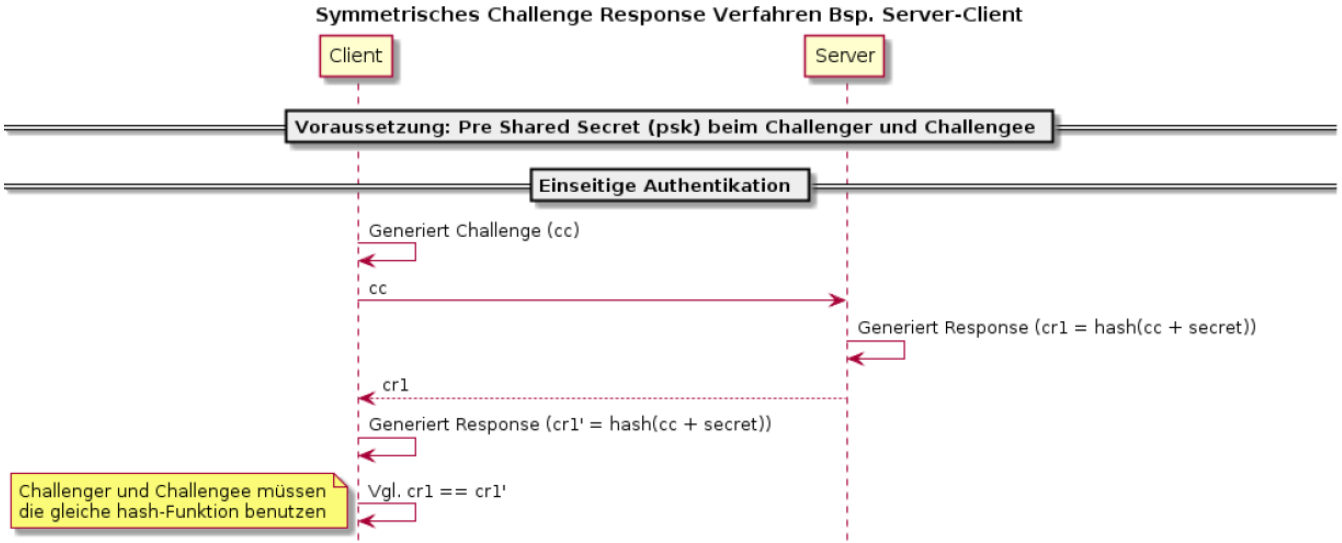
SM-C und SM-S wieder vorhanden

Kryptologische Funktion in SM-C und SM-S berechnet

Passwortverfahren - Gefahren

Challenge-Response Verfahren

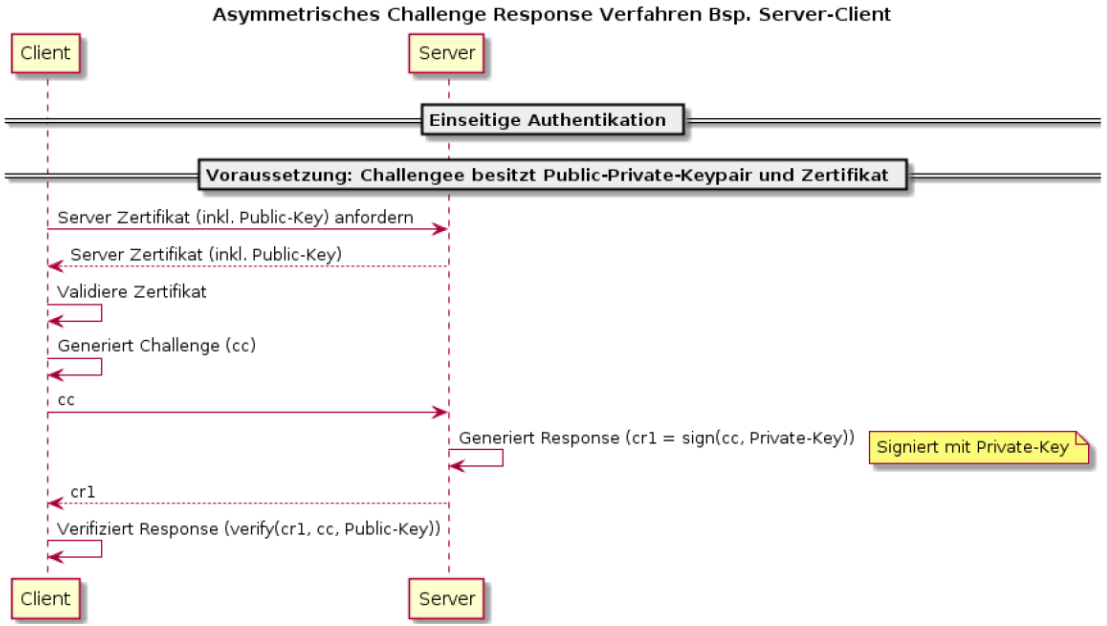
Durchführung einer spontanen kryptographischen Operation



Passwortverfahren - Gefahren

Challenge-Response Verfahren

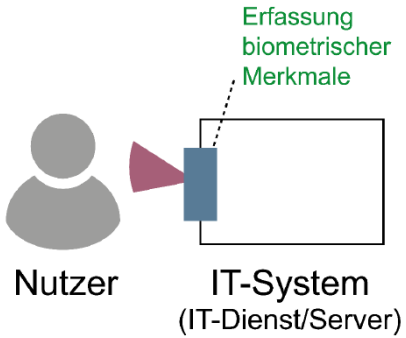
Durchführung einer spontanen kryptographischen Operation



Passwortverfahren - Gefahren

Biometrisches Verfahren

Es werden physiologische oder verhaltenstypische, also personengebundene Charakteristika verwendet.

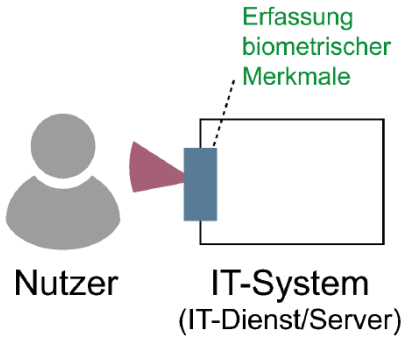


Passwortverfahren - Gefahren

Biometrisches Verfahren

Es werden physiologische oder verhaltenstypische, also personengebundene Charakteristika verwendet.

Biometrische Merkmale können nicht unmittelbar gestohlen und im Allgemeinen nur schwer kopiert werden.



Passwortverfahren - Gefahren

Biometrisches Verfahren

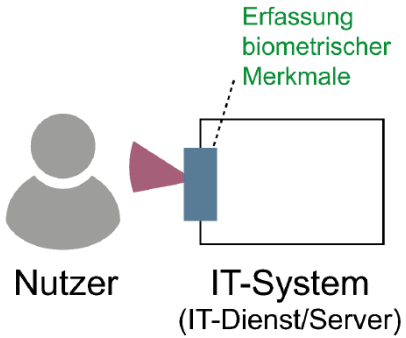
Aktive Merkmale	Passive Merkmale
Unterschriftdynamik	Gesichtserkennung
Schreibverhalten	Retinamuster
Tippverhalten an der Tastatur	Irismuster
Stimmerkennung	Fingerabdruck (Daktylogramm)
Lippenbewegung beim Sprechen	Form des Ohres
Gestik/Mimik beim Sprechen	Handgeometrie
Bewegung (Gangartzyklus)	Venenmuster auf dem Handrücken
	Geruch
	DNA
	Thermogramm

Passwortverfahren - Gefahren

Biometrisches Verfahren

$$FAR = \frac{fälschlich\ akzeptierte\ Zugriffe}{unberechtigte\ Zugriffsversuche}$$

Erkennung einer nichtberechtigten Person als berechtigt



Passwortverfahren - Gefahren

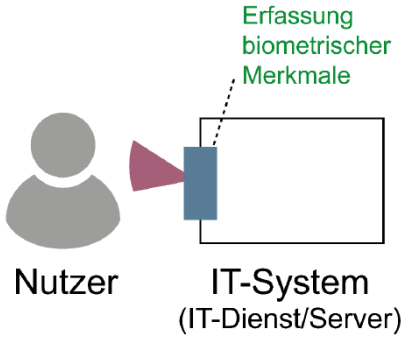
Biometrisches Verfahren

$$FAR = \frac{fälschlich\ akzeptierte\ Zugriffe}{unberechtigte\ Zugriffsversuche}$$

Erkennung einer nichtberechtigten Person als berechtigt

$$FRR = \frac{fälschlich\ zurückgewiesene\ Zugriffe}{berechtigte\ Zugriffsversuche}$$

Unberechtigte Abweisung berechtigter Personen



Passwortverfahren - Gefahren

Biometrisches Verfahren

$$FAR = \frac{fälschlich\ akzeptierte\ Zugriffe}{unberechtigte\ Zugriffsversuche}$$

Erkennung einer nichtberechtigten Person als berechtigt

$$FRR = \frac{fälschlich\ zurückgewiesene\ Zugriffe}{berechtigte\ Zugriffsversuche}$$

Unberechtigte Abweisung berechtigter Personen

Gewisser Spielraum muss erlaubt sein.

Es gibt immer eine Wahrscheinlichkeit der Falsch oder Nichtakzeptanz

Passwortverfahren - Gefahren

Biometrisches Verfahren

$$FAR = \frac{fälschlich\ akzeptierte\ Zugriffe}{unberechtigte\ Zugriffsversuche}$$

Erkennung einer nichtberechtigten Person als berechtigt

$$FRR = \frac{fälschlich\ zurückgewiesene\ Zugriffe}{berechtigte\ Zugriffsversuche}$$

Unberechtigte Abweisung berechtigter Personen

Gewisser Spielraum muss erlaubt sein.

Kryptographischer Schlüssel kann nicht abgeleitet

Passwortverfahren - Gefahren

Biometrisches Verfahren

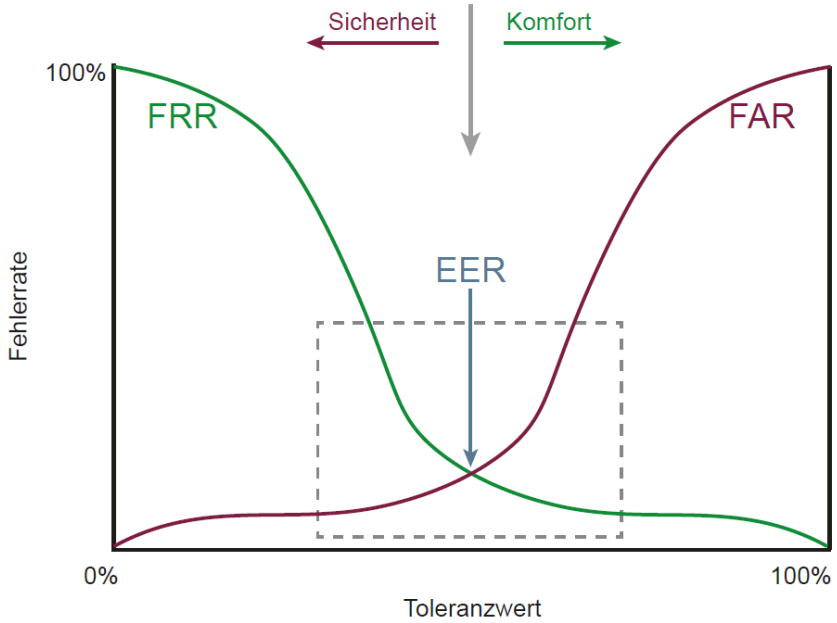
Einführung der **Equal Error Rate**

Je höher der Sicherheitsbereich ist, umso mehr fälschliche Abweisungen sollten toleriert werden.

Passwortverfahren - Gefahren

Biometrisches Verfahren

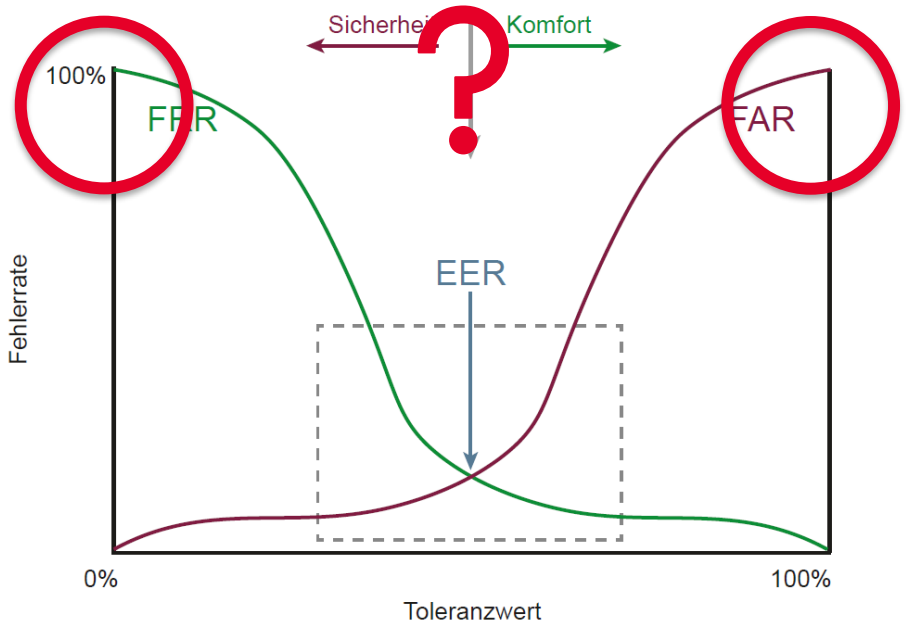
Einführung der **Equal Error Rate**



Passwortverfahren - Gefahren

Biometrisches Verfahren

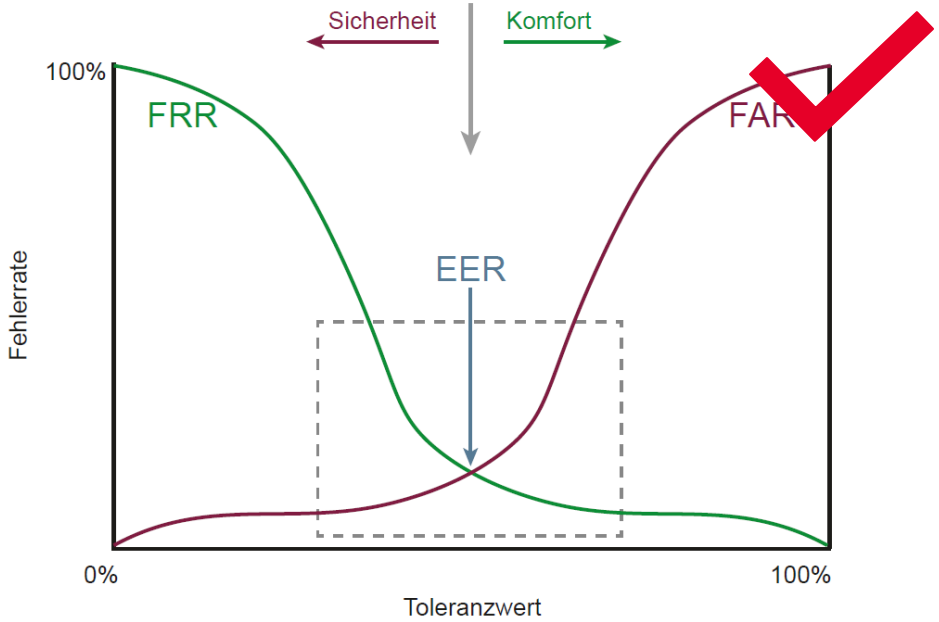
Einführung der **Equal Error Rate**



Passwortverfahren - Gefahren

Biometrisches Verfahren

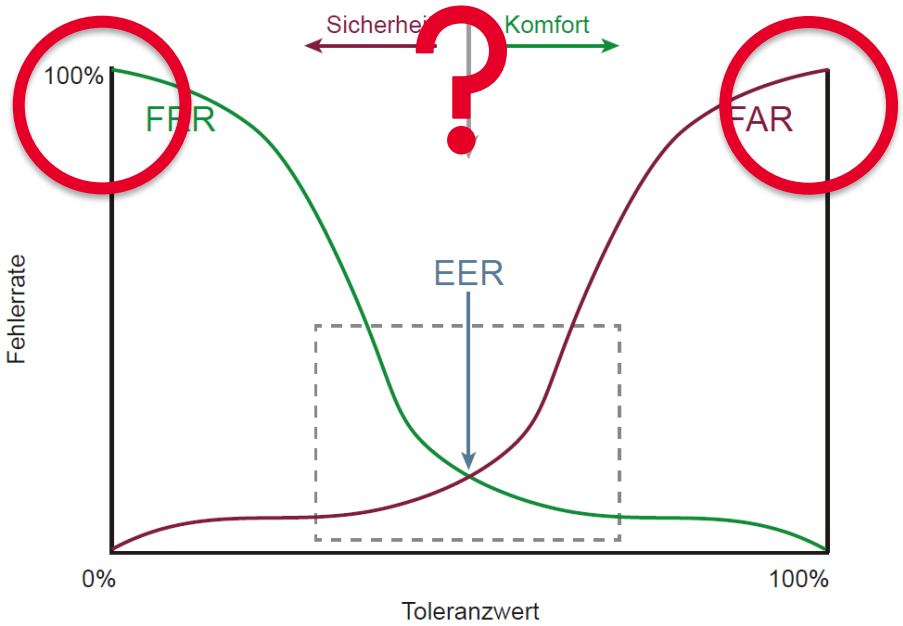
Einführung der **Equal Error Rate**



Passwortverfahren - Gefahren

Biometrisches Verfahren

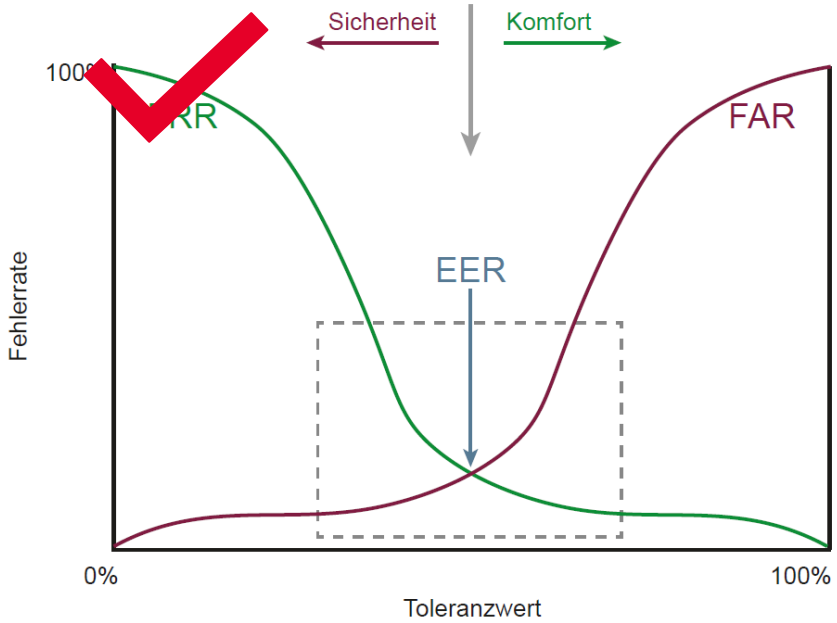
Einführung der **Equal Error Rate**



Passwortverfahren - Gefahren

Biometrisches Verfahren

Einführung der **Equal Error Rate**



Passwortverfahren - Gefahren

Biometrisches Verfahren

Einführung der **Equal Error Rate**

Rank	Accuracy	Convenience	Cost	MOC integration
1	DNA	Voice	Voice	Finger
2	Iris	Face	Signature	Voice
3	Retina	Signature	Finger	
4	Finger	Finger	Face	
5	Face	Iris	Iris	
6	Signature	Retina	Retina	
7	Voice	DNA	DNA	

Beste Lösung ⇨

Schlechteste Lösung ⇨

Fahndung nach Schwerverbrechern

Hochsicherheitsanwendungen

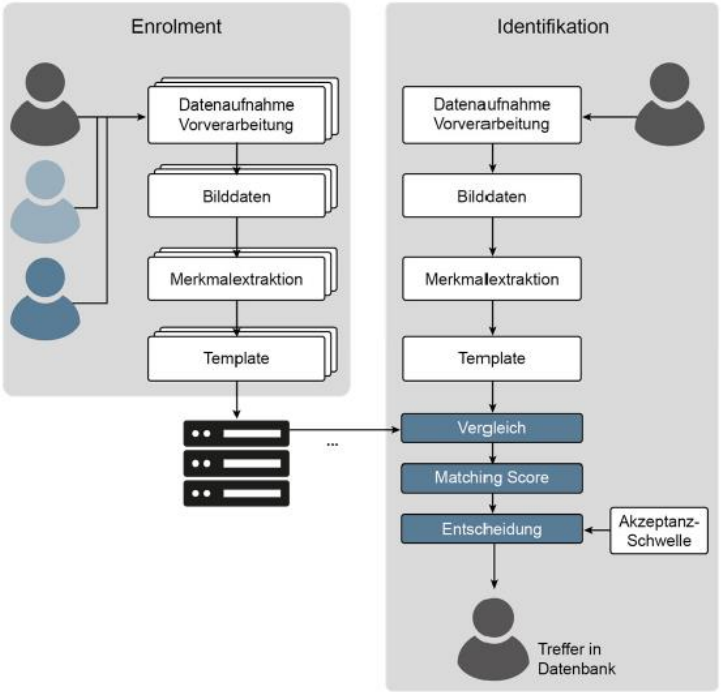
Alltägliche Sicherheitsanforderungen

Morgan Keegan RAYMOND JAMES

Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Prozess gleicht auf verschiedene Datenbanken zu

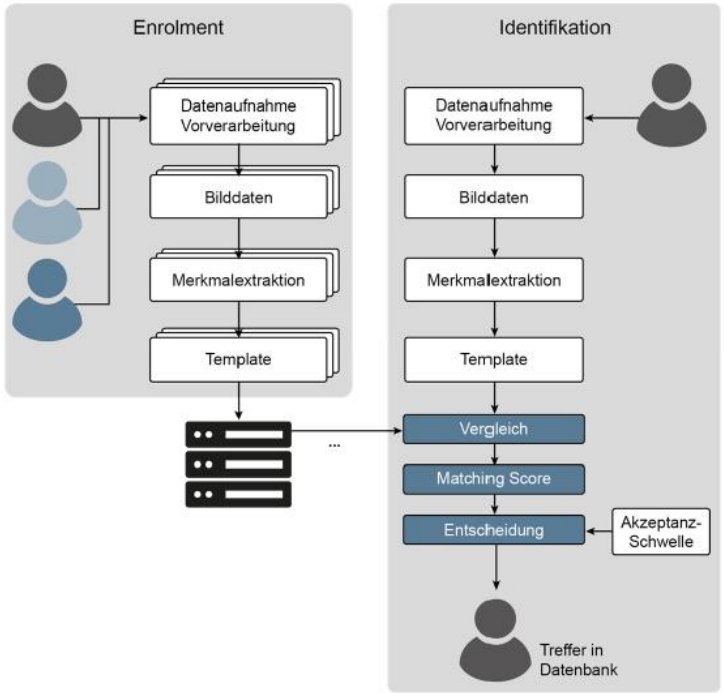


Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Prozess gleicht auf verschiedene Datenbanken zu

Mitarbeiter wird eingepflegt

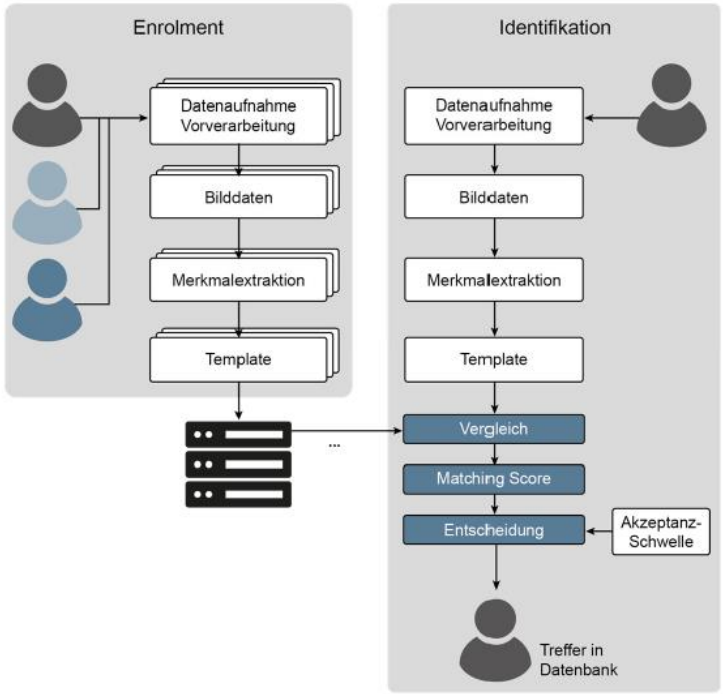


Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Prozess gleicht auf verschiedene Datenbanken zu

Mitarbeiter wird eingepflegt



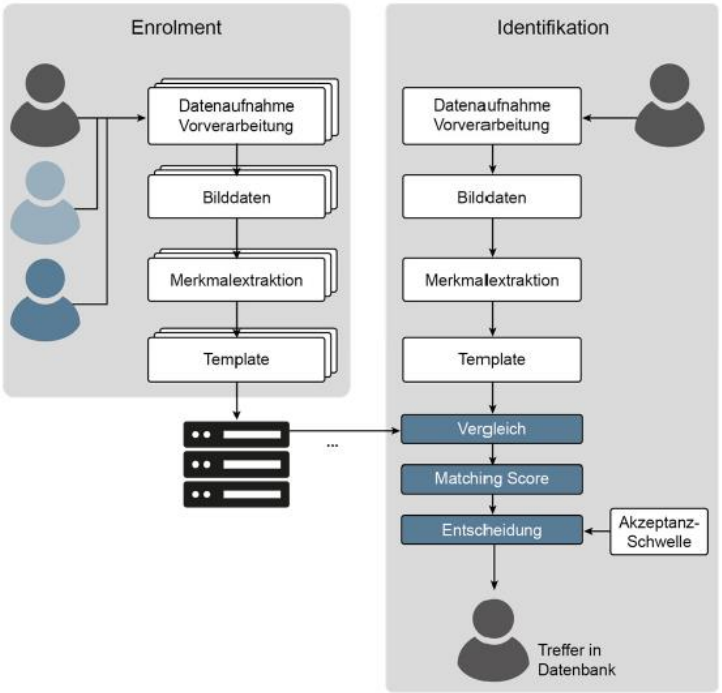
Reicht der Score aus?

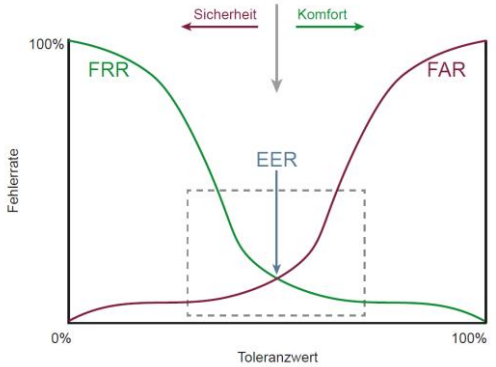
Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Prozess gleicht auf verschiedene Datenbanken zu

Mitarbeiter wird eingepflegt





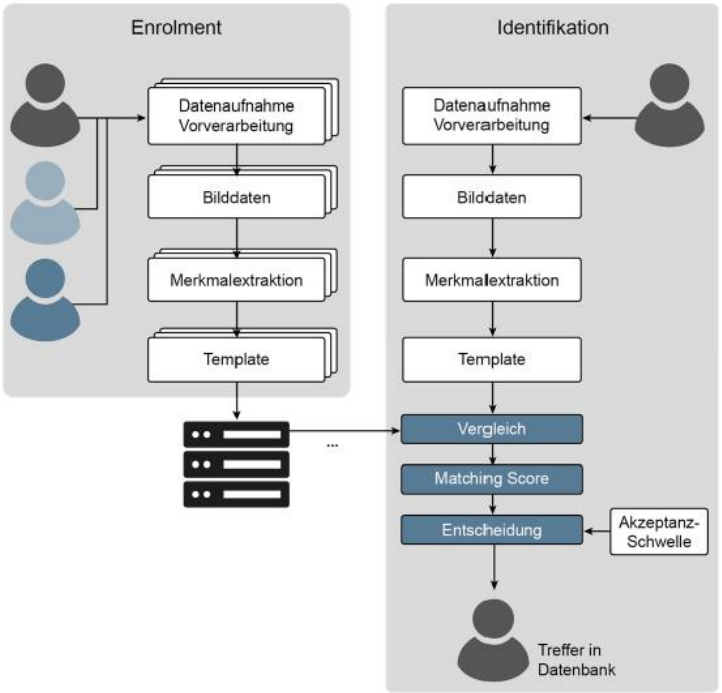
Reicht der Score aus?

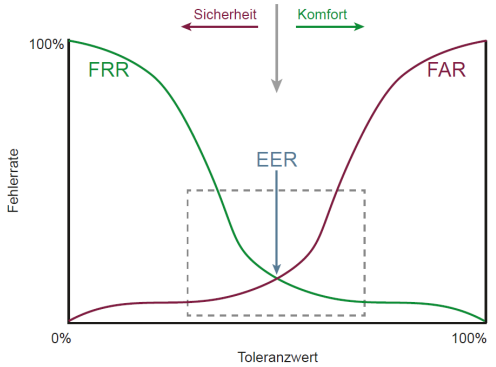
Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Prozess gleicht auf verschiedene Datenbanken zu

Mitarbeiter wird eingepflegt



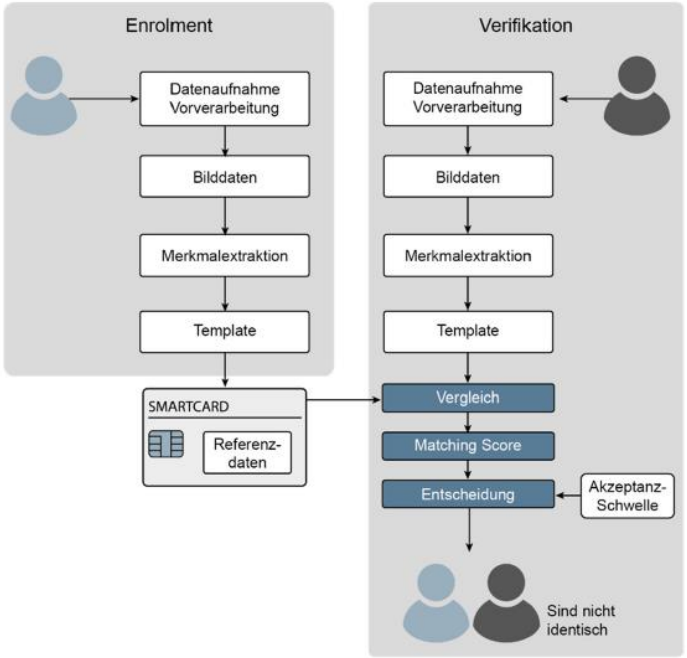


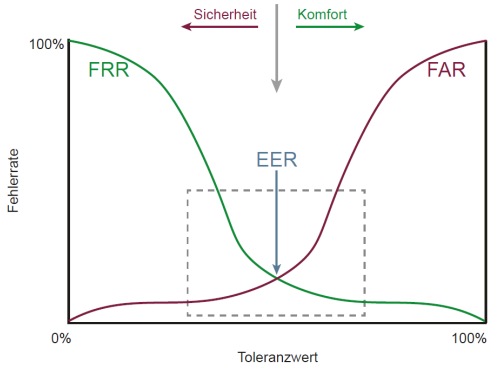
Reicht der Score aus?

Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Smartcard als Medium



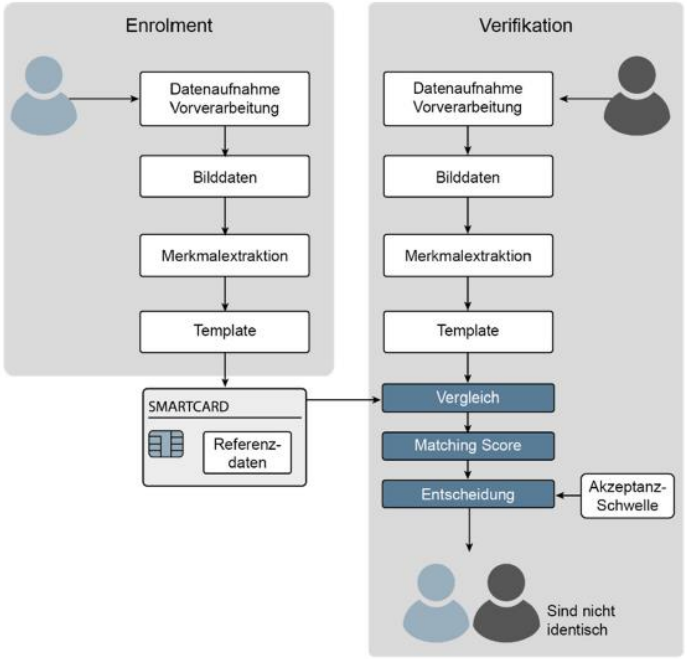


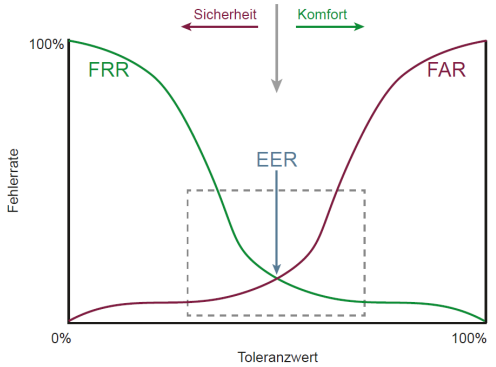
Reicht der Score aus?

Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Wo packen Angreifer hier an?



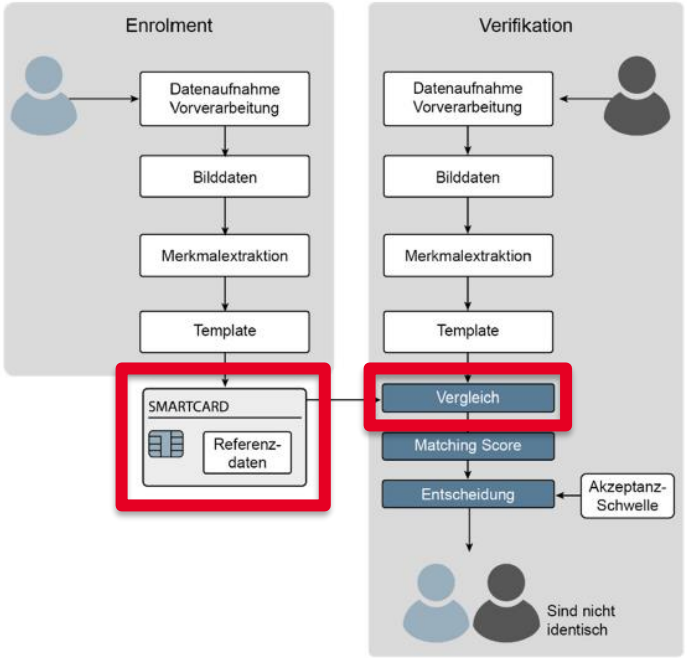


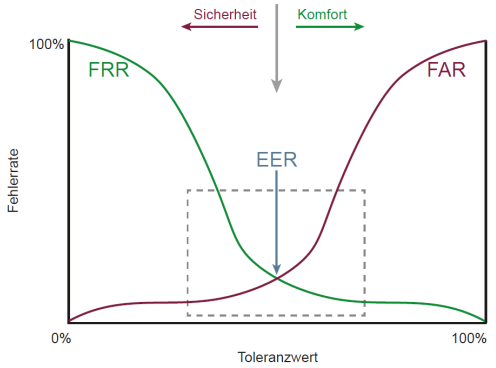
Reicht der Score aus?

Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Wo packen Angreifer hier an?





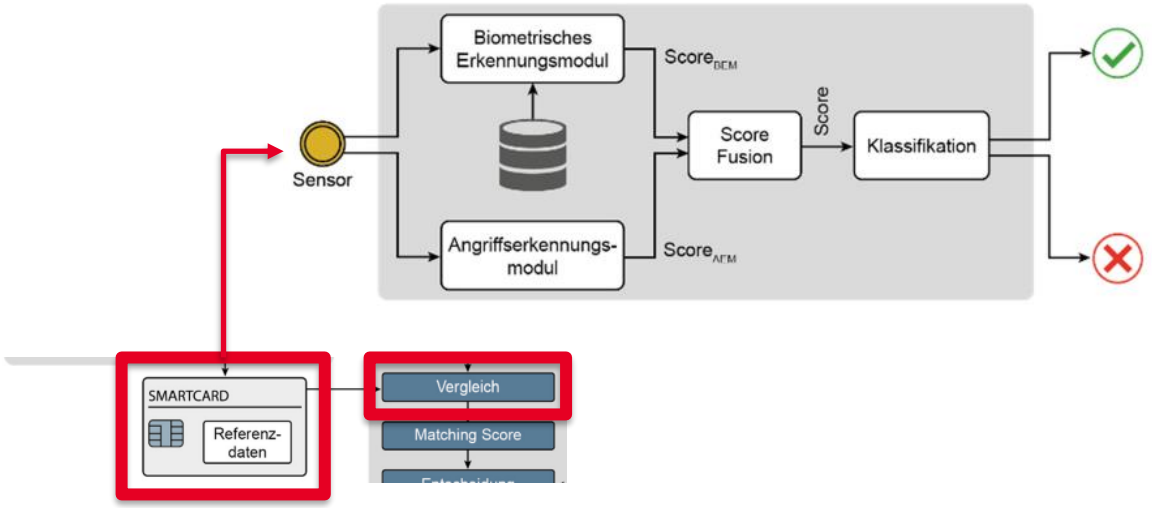
Manipulation der Smartcard oder dem Vergleich

Reicht der Score aus?

Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Wo packen Angreifer hier an?

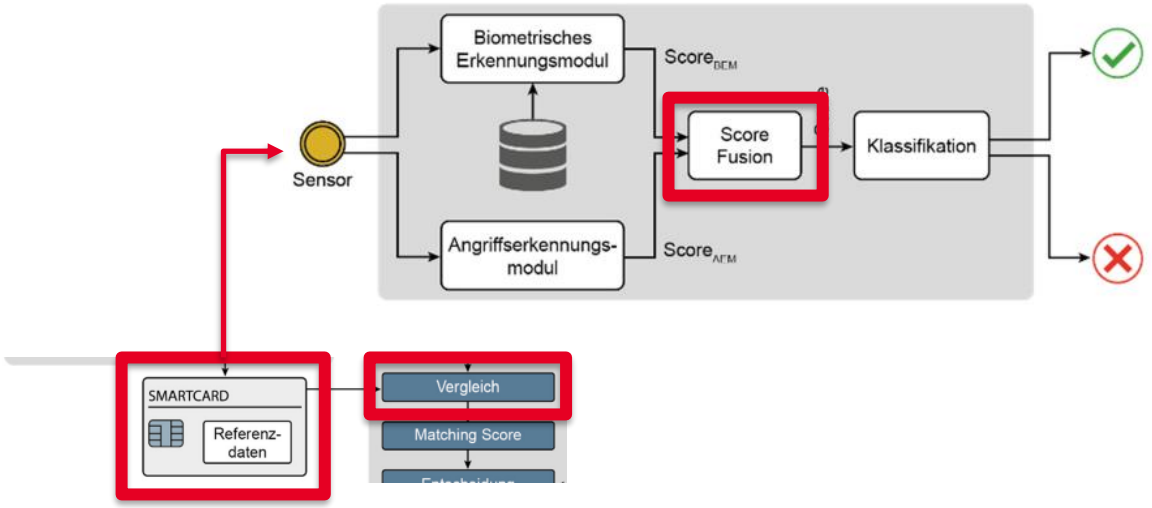


Manipulation der Smartcard oder dem Vergleich

Passwortverfahren - Gefahren

Biometrisches Verfahren – Anwendungen

Wo packen Angreifer hier an?



Manipulation der Smartcard oder dem Vergleich

Mehrfaktor Authentifizierung

Generelle Idee:

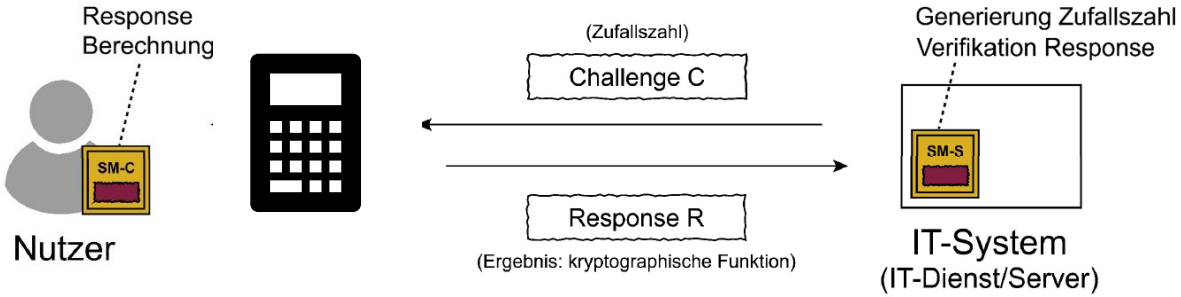
Verwendet unterschiedliche und insbesondere unabhängige Klassen von Authentifizierungsverfahren.

Kombination aus den Verfahren der letzten Vorlesungen.

Mehrfaktor Authentifizierung

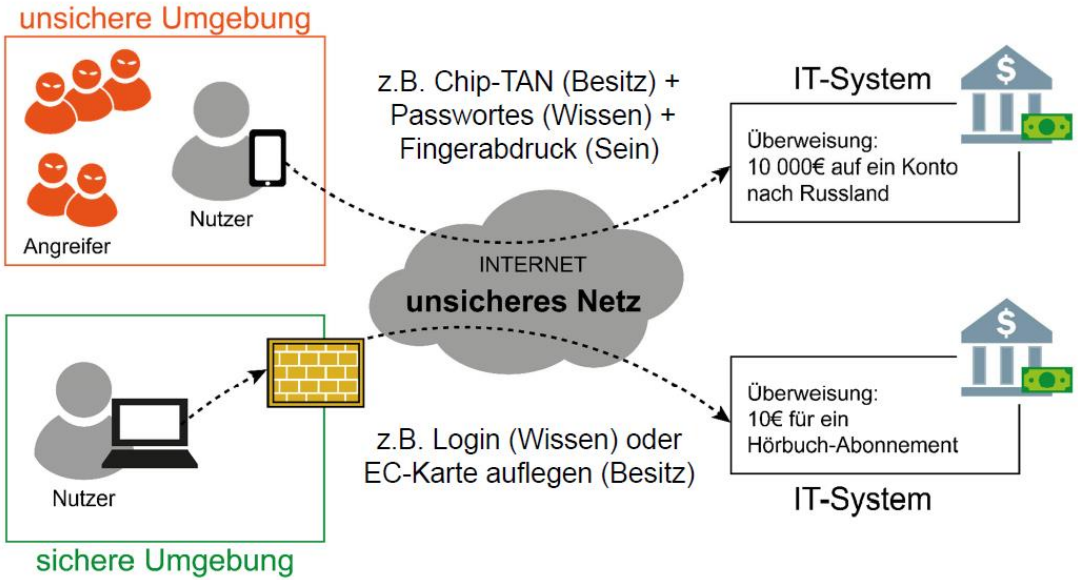
Generelle Idee:

Verwendet unterschiedliche und insbesondere unabhängige Klassen von Authentifizierungsverfahren.

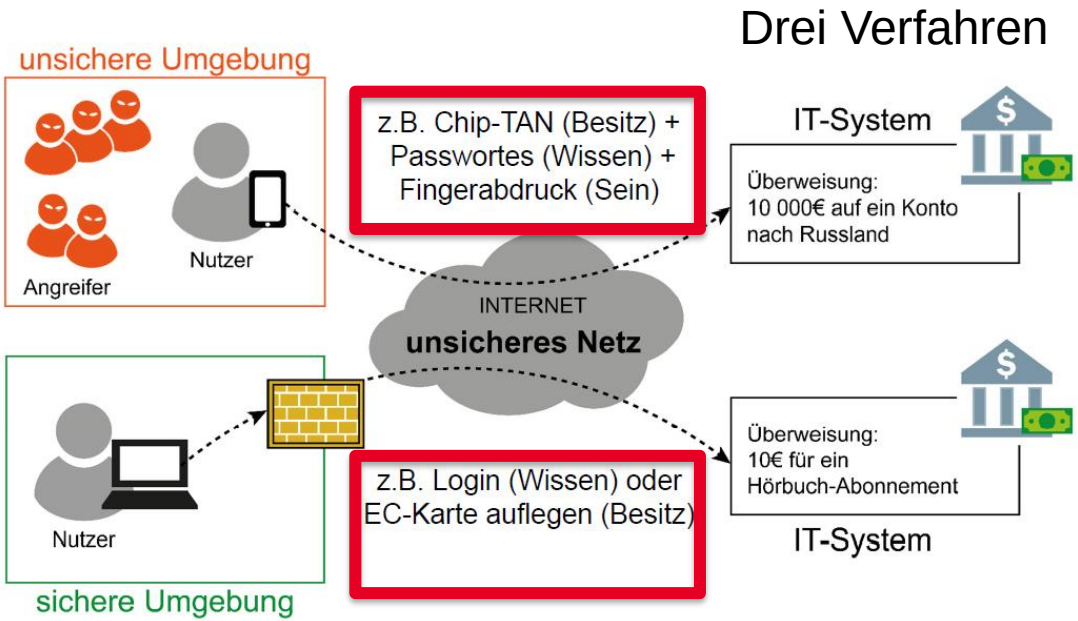


Sicherheitsmodul SM-C muss mit PIN Eingabe aktiviert werden.

Mehrfaktor Authentifizierung



Mehrfaktor Authentifizierung

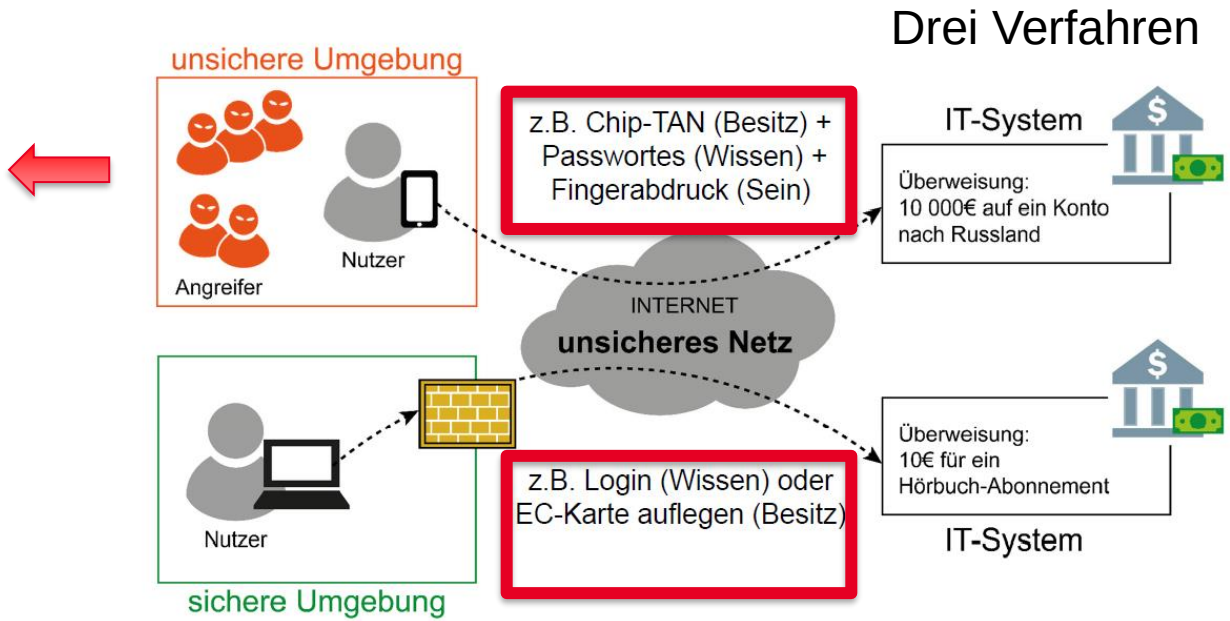


Ein Verfahren +
wird zu oder

Mehrfaktor Authentifizierung

Probleme treten auf.

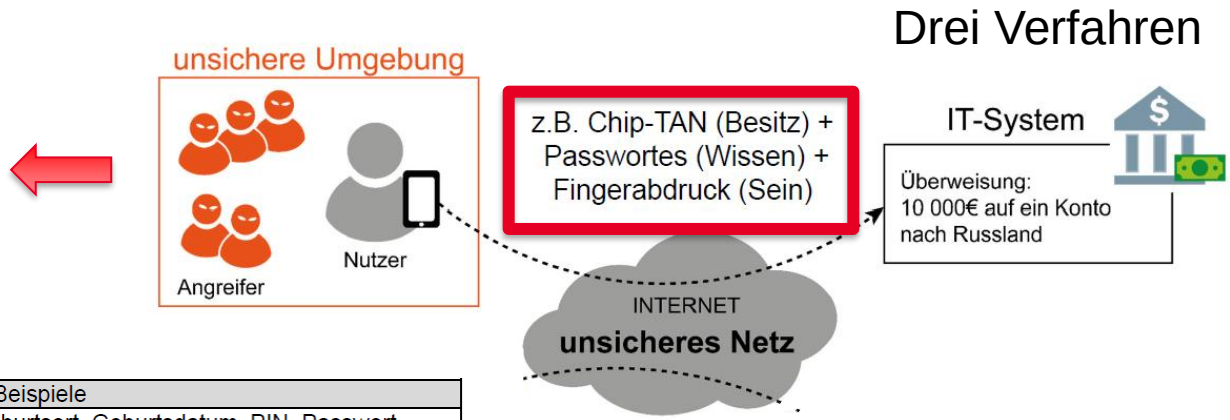
Was machen Sie?



Mehrfaktor Authentifizierung

Probleme treten auf.

Was machen Sie?



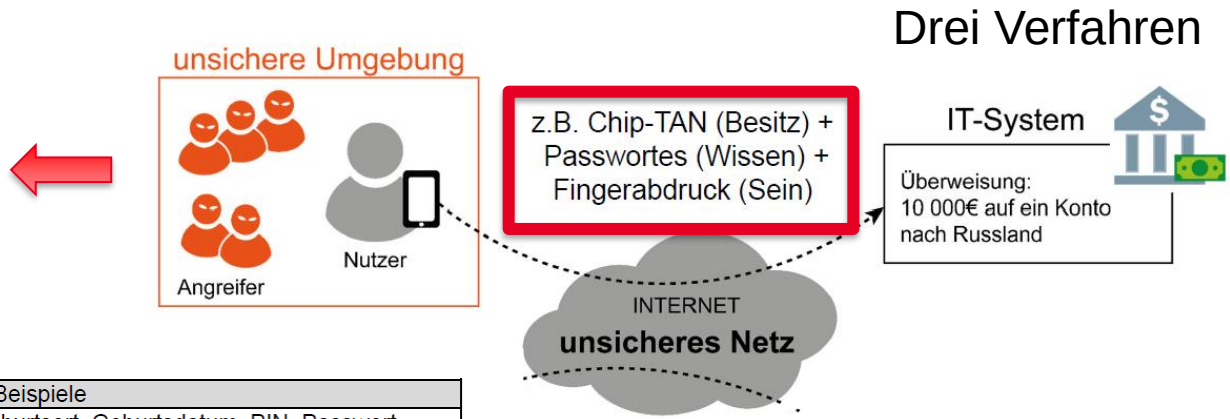
Faktor	Beispiele
Wissen	Benutzername, Kundennummer, Geburtsort, Geburtsdatum, PIN, Passwort
Besitz	Kryptographische Schlüssel, Hard –und Software Token, Sicherheitsmodule, Smartcards
Inhärenz	Unterschrift, Fingerabdruck, Stimme, Tippverhalten, Mausbewegungen
Verhalten	**Vergangene Transaktionen, verwendete Geräte, Besuchte Orte, verwendete Softwareversionen, Aktivitäten in sozialen Medien, Timing**

Verhalten wird definiert.

Mehrfaktor Authentifizierung

Probleme treten auf.

Was machen Sie?



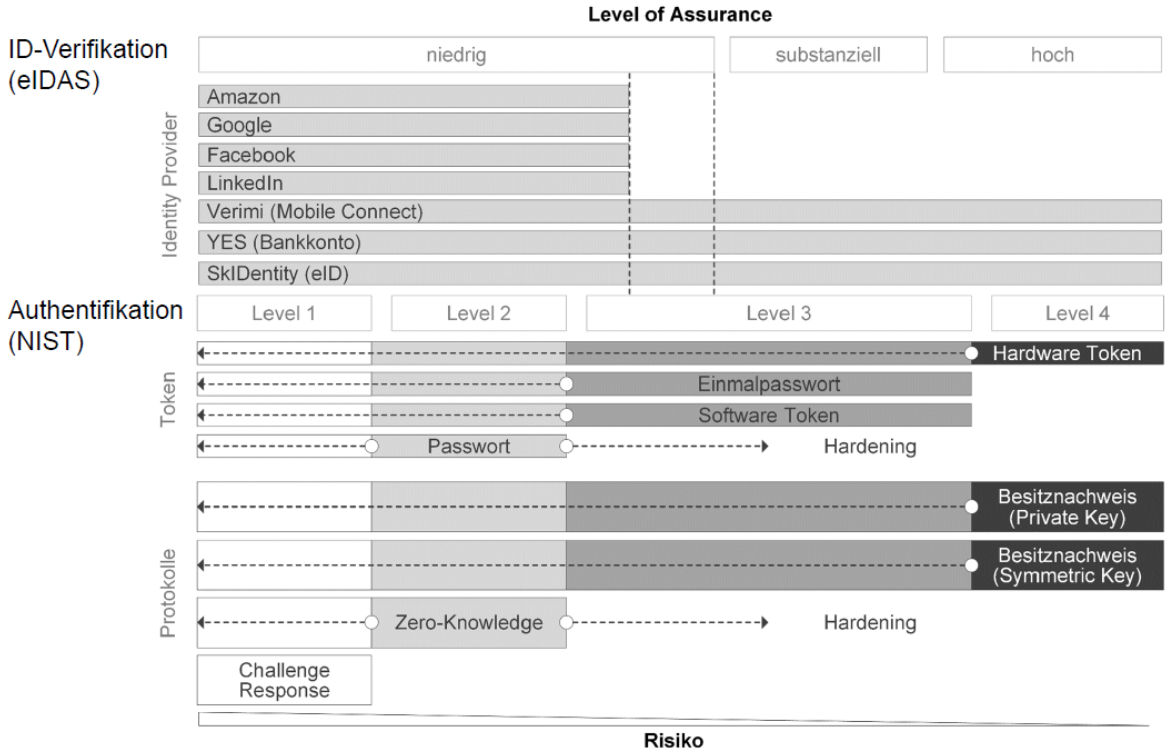
Faktor	Beispiele
Wissen	Benutzername, Kundennummer, Geburtsort, Geburtsdatum, PIN, Passwort
Besitz	Kryptographische Schlüssel, Hard –und Software Token, Sicherheitsmodule, Smartcards
Inhärenz	Unterschrift, Fingerabdruck, Stimme, Tippverhalten, Mausbewegungen
Verhalten	**Vergangene Transaktionen, verwendete Geräte, Besuchte Orte, verwendete Softwareversionen, Aktivitäten in sozialen Medien, Timing**

Verhalten wird definiert.

Mehrfaktor Authentifizierung

Niedrige Level setzten auf PW

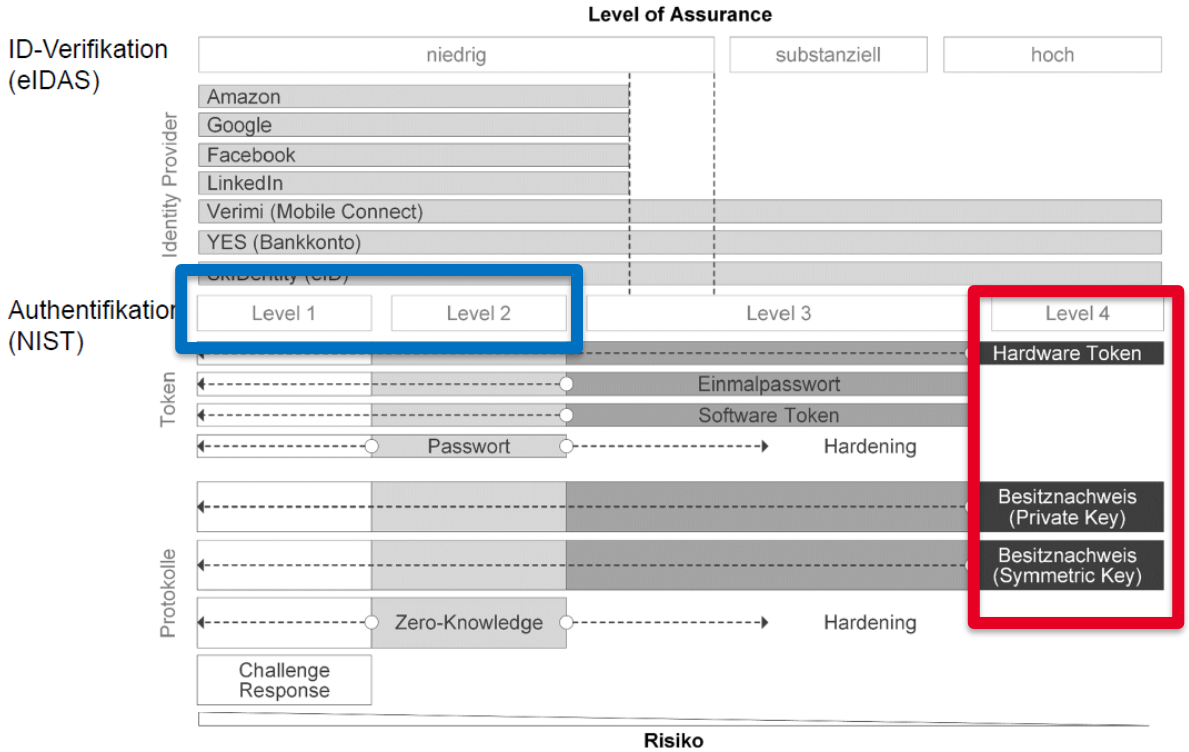
Hohe Level auf Hardware-Nachweise



Mehrfaktor Authentifizierung

Niedrige Level setzten auf PW

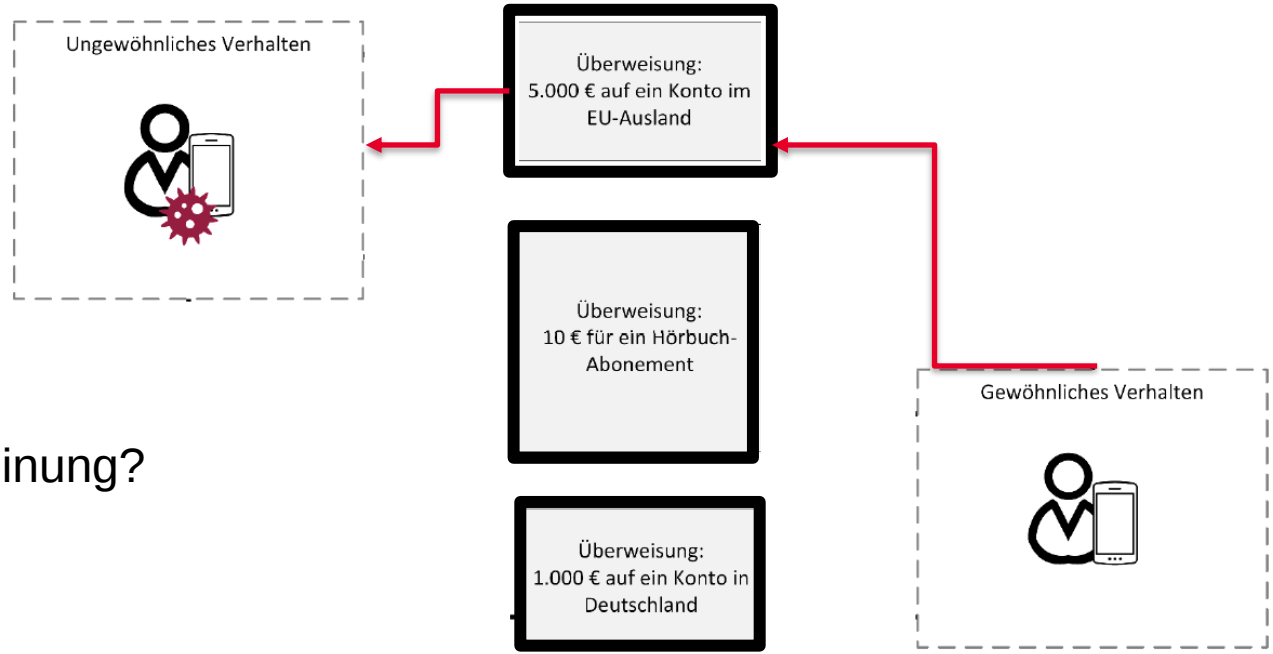
Hohe Level auf Hardware-Nachweise



Mehrfaktor Authentifizierung

Ihre Meinung?

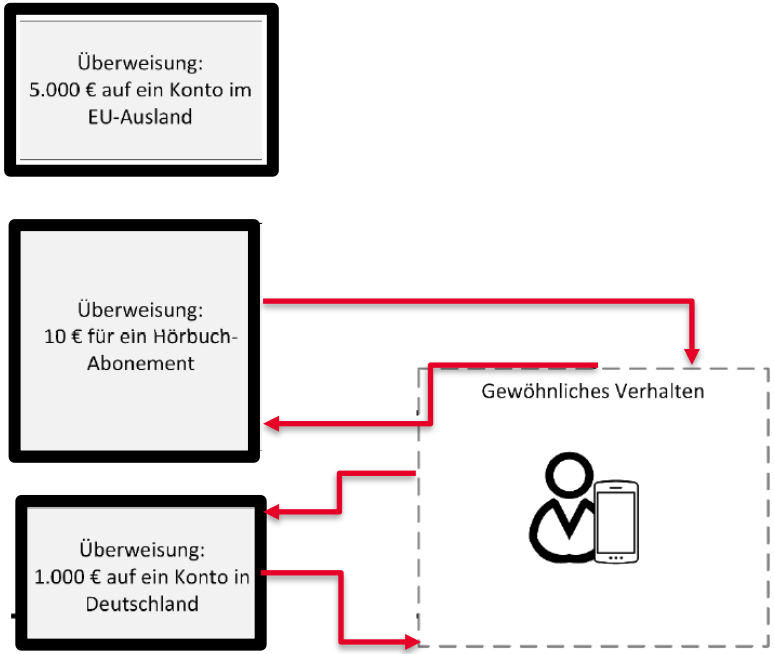
Mehrfaktor Authentifizierung



Ihre Meinung?

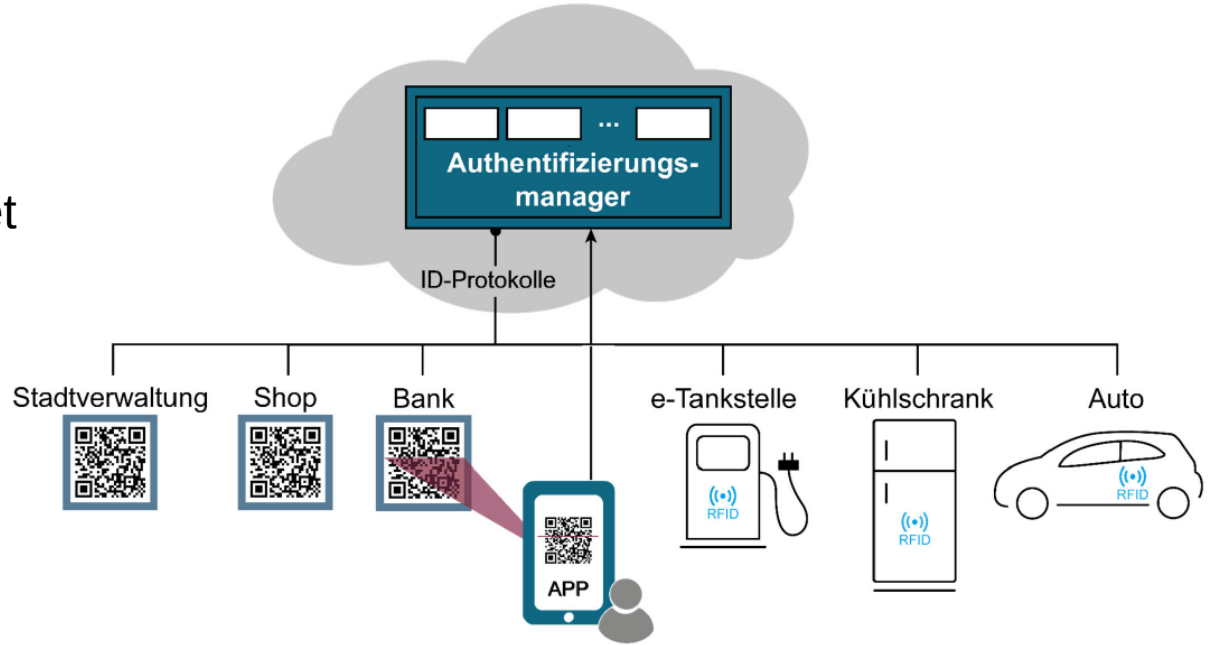
Mehrfaktor Authentifizierung

Ihre Meinung?



Moderne Authentifizierungssysteme

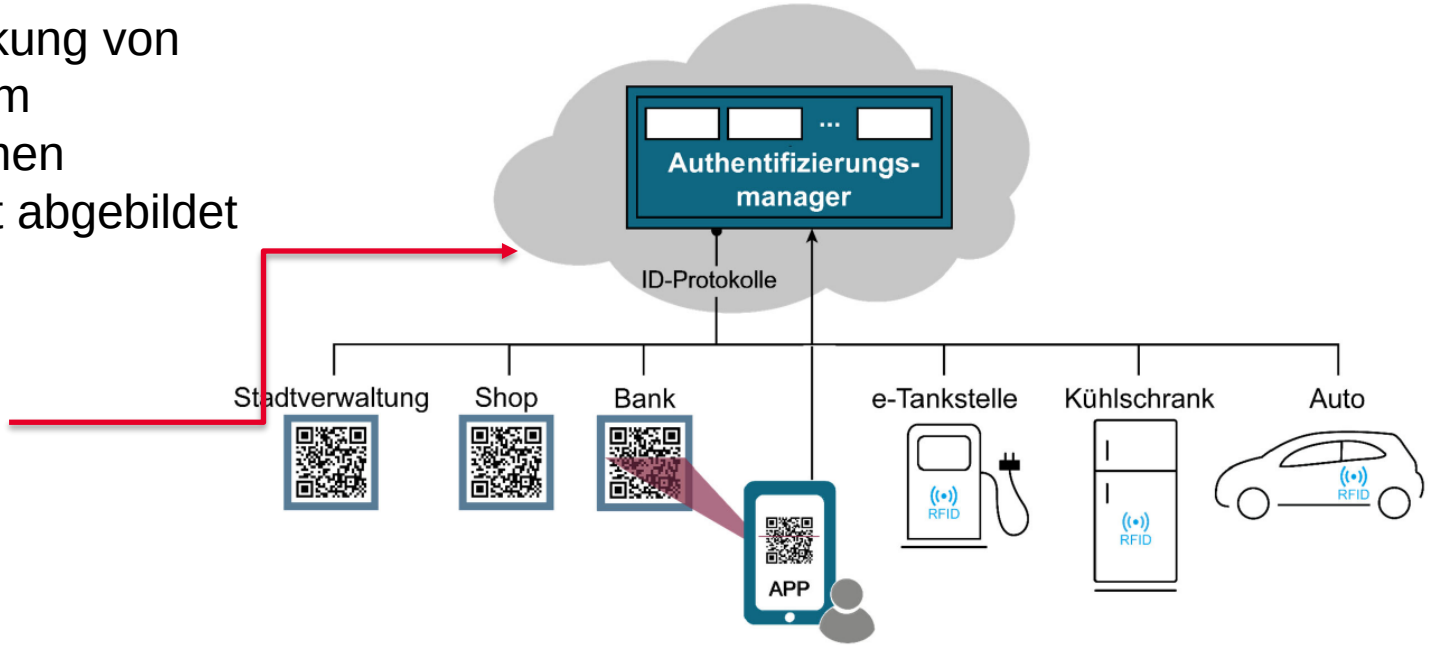
Verschlankung von dem was im Unternehmen kompliziert abgebildet wird.



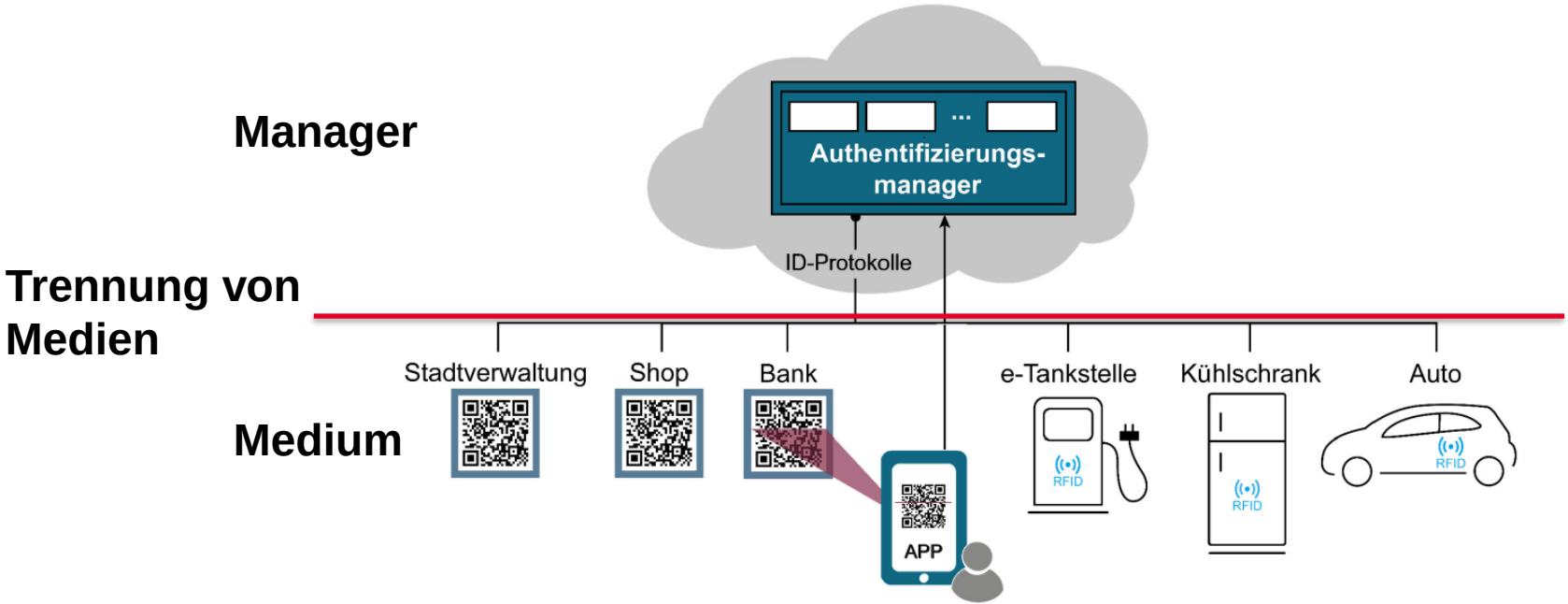
Moderne Authentifizierungssysteme

Verschlankung von dem was im Unternehmen kompliziert abgebildet wird.

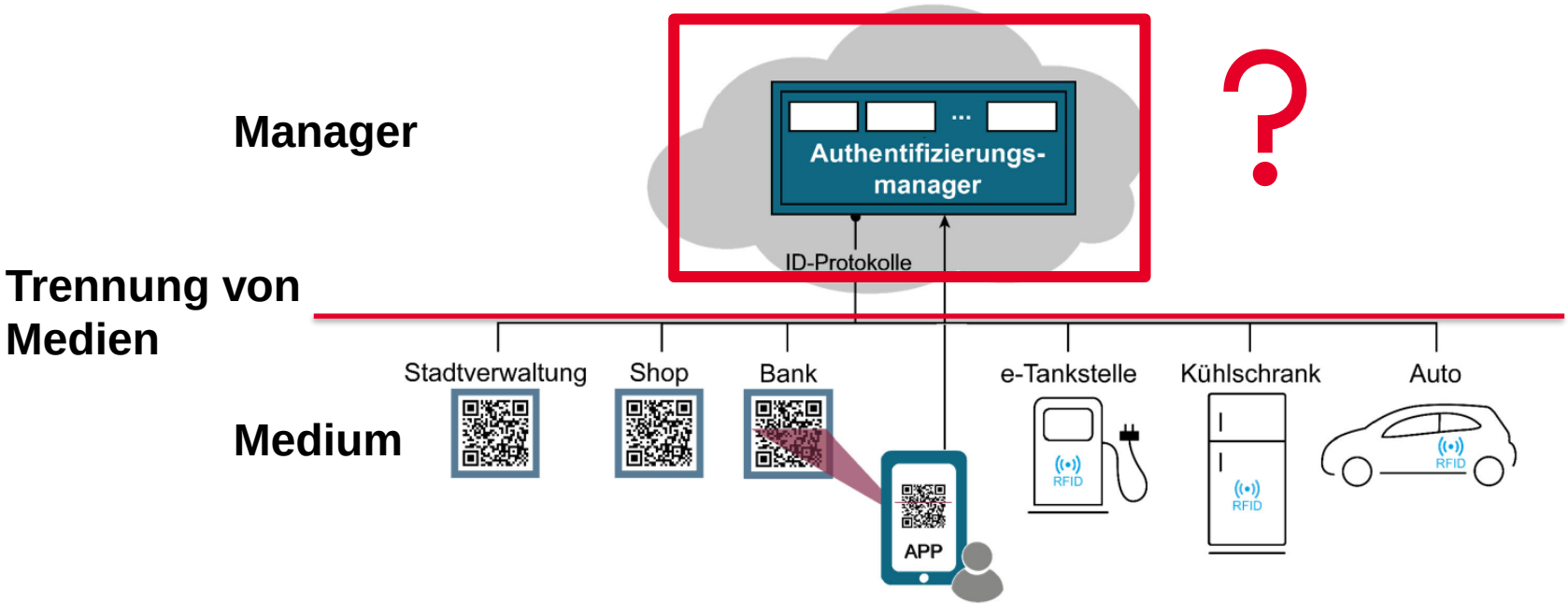
Cloud



Moderne Authentifizierungssysteme



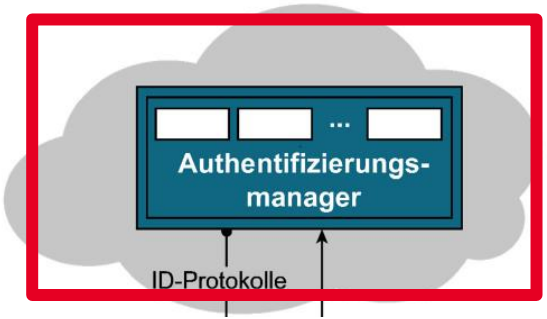
Moderne Authentifizierungssysteme



Moderne Authentifizierungssysteme

Vermittelt zwischen User und Programm.

- Liefert QR-Code an den Dienstanbieter
- Versichert den Dienstanbieter dass der User authentifiziert ist

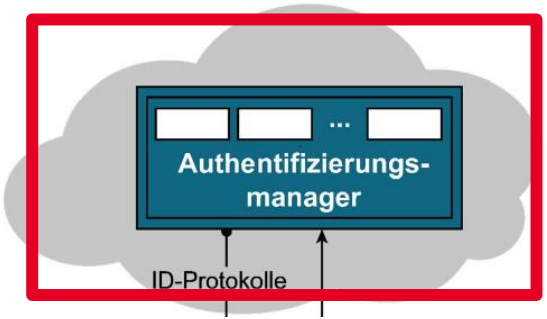


?

Moderne Authentifizierungssysteme

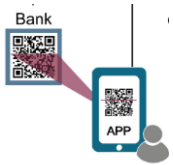
Vermittelt zwischen User und Programm.

- Liefert QR-Code an den Dienstanbieter
- Versichert den Dienstanbieter dass der User authentifiziert ist



?

App agiert dann SM-S und SM-C.



PIN

PKI

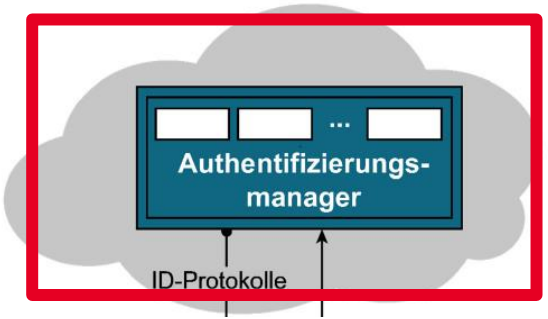
Adaptiv

Biometrische Verfahren

Moderne Authentifizierungssysteme

Vermittelt zwischen User und Programm.

- Liefert QR-Code an den Dienstanbieter
- Versichert den Dienstanbieter dass der User authentifiziert ist



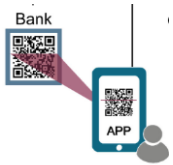
?

App agiert dann SM-S und SM-C.

Apple Pay

PIN

PKI

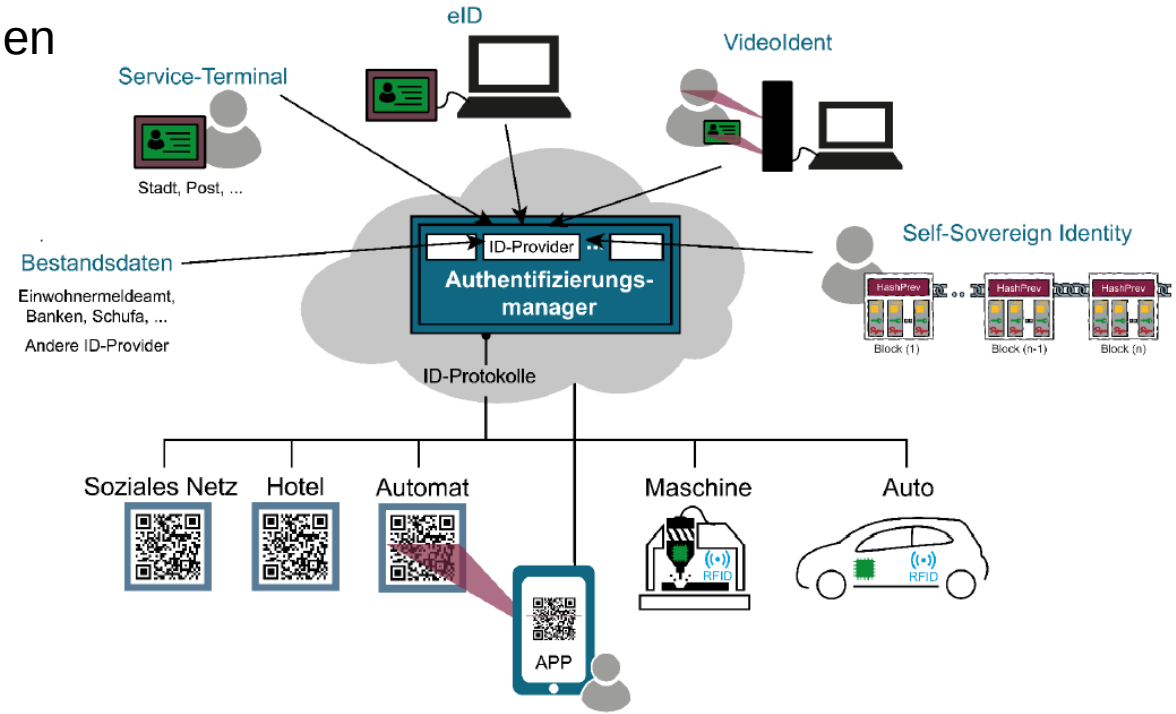


Adaptiv

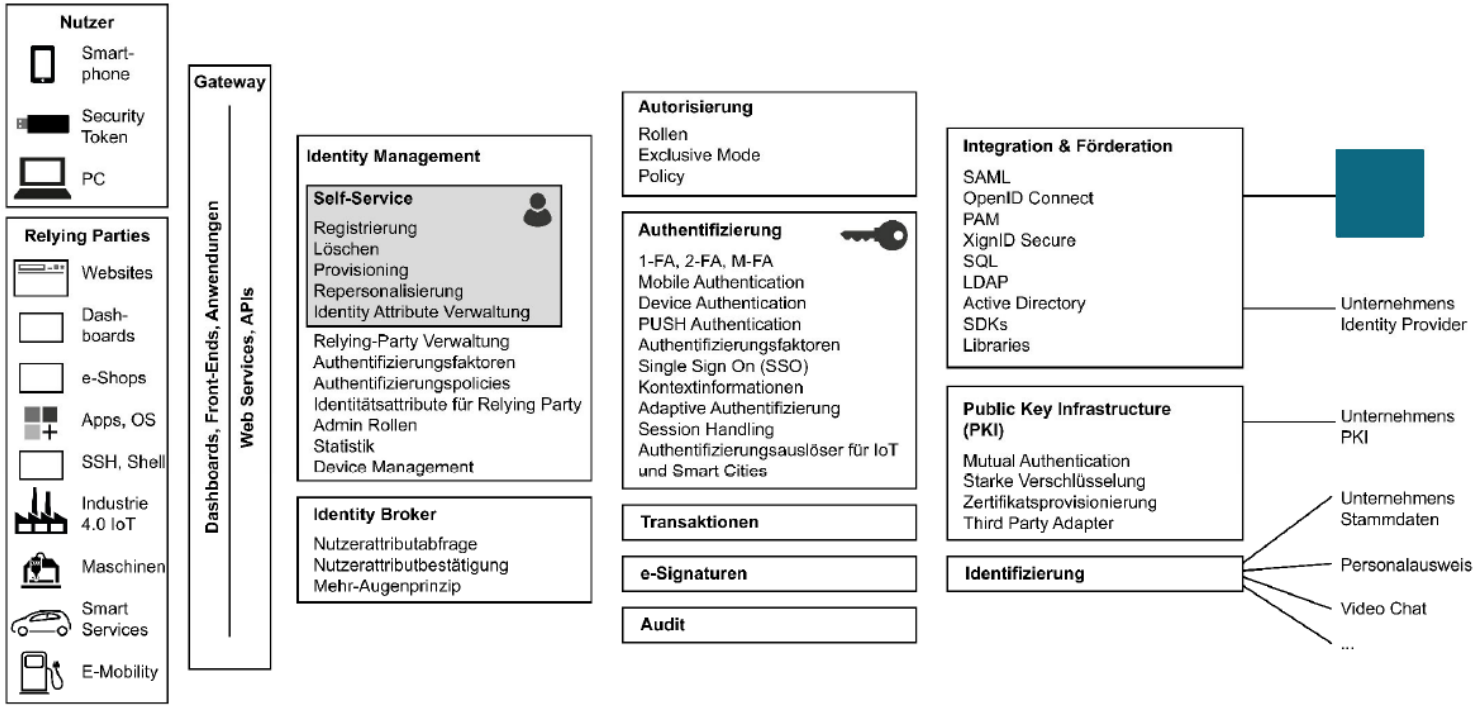
Biometrische Verfahren

Moderne Authentifizierungssysteme

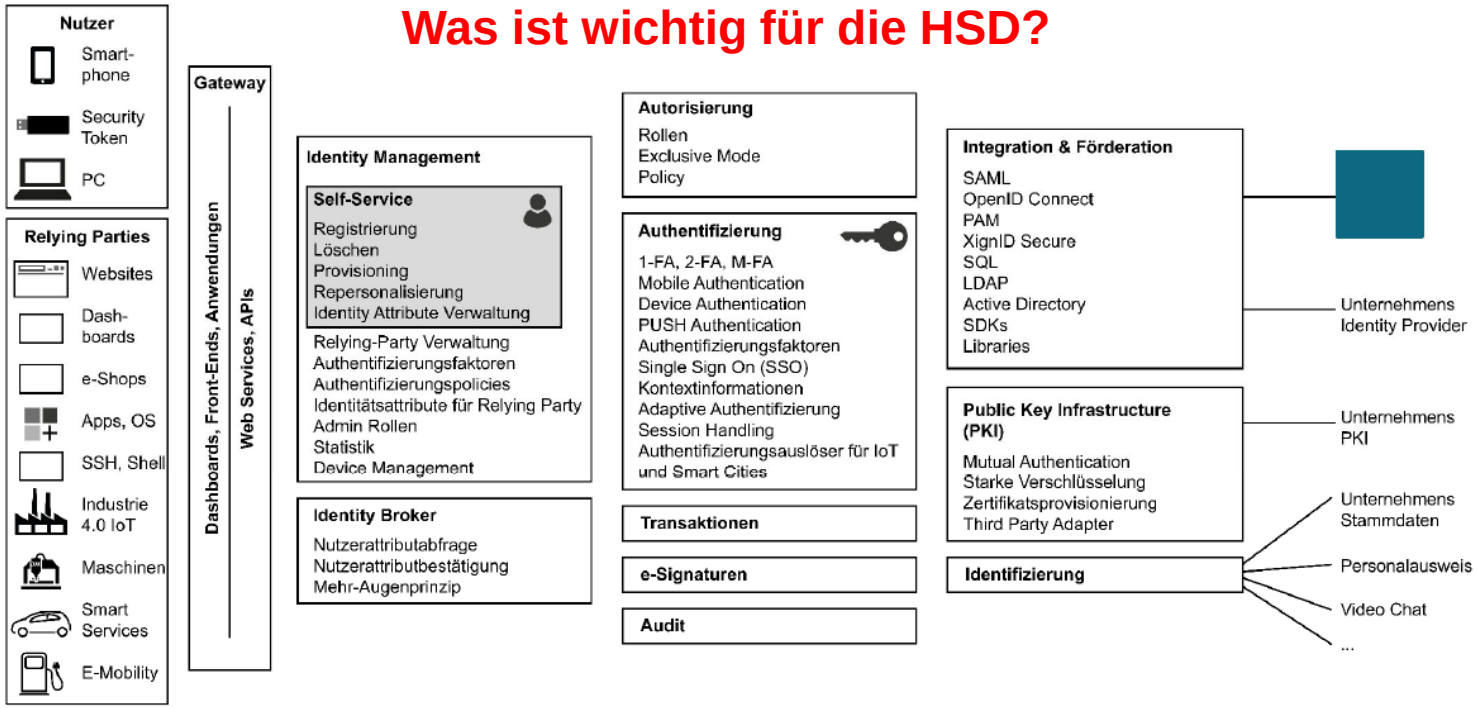
Schnittstellen zu sehr vielen Systemen Denkbar



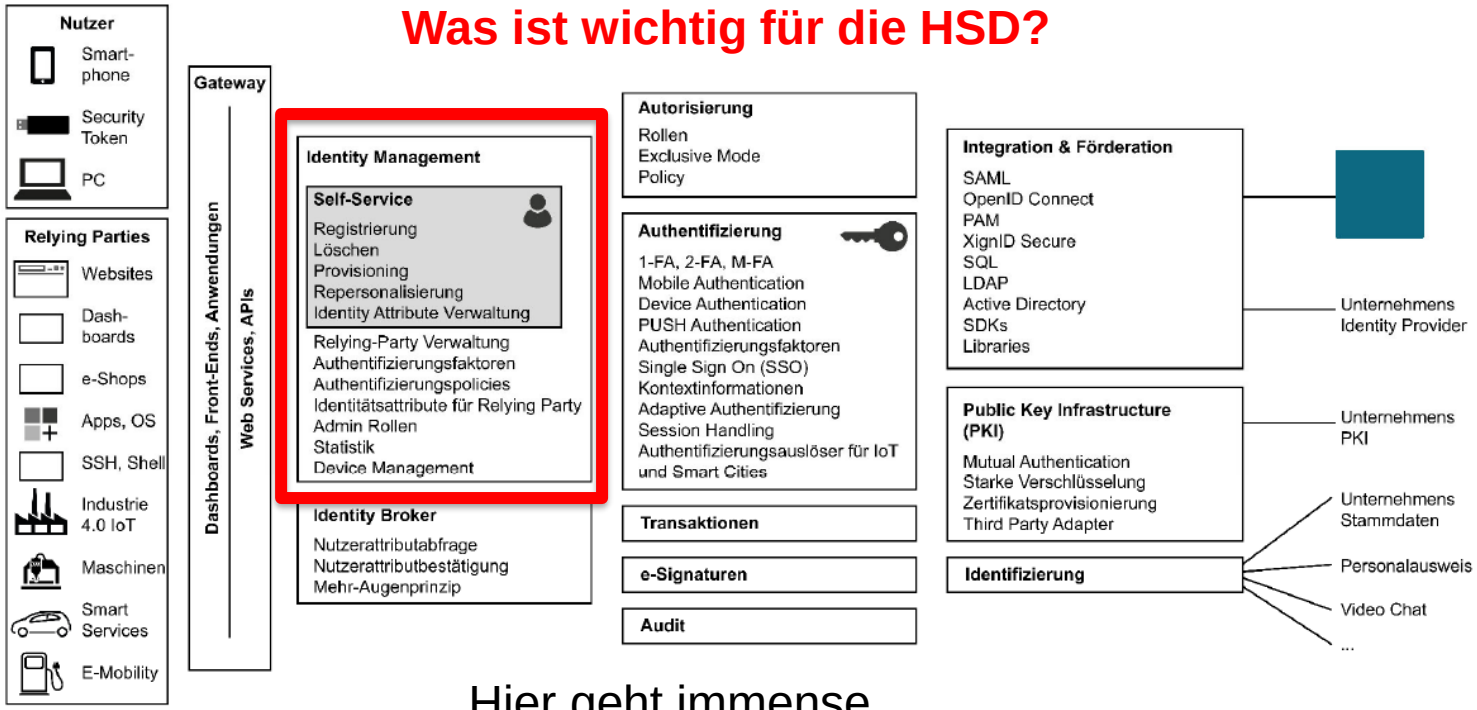
Moderne Authentifizierungssysteme



Moderne Authentifizierungssysteme



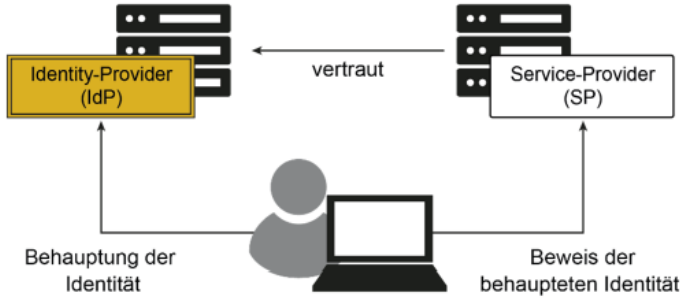
Moderne Authentifizierungssysteme



Hier geht immense Programmierarbeit rein.

Moderne Authentifizierungssysteme

Was ist wichtig für die HSD?



Muss für jeden Service der HSD ausgeführt werden.

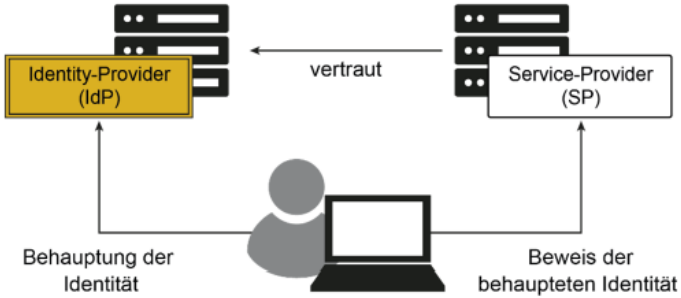
Digitaler Arbeitsplatz | E-Mail | HSD Account | Microsoft 365 & Teams | Online Speicher | Software | Telefonie | WLAN | Anwendungsentwicklung

Consulting | Cumulus | Drucken & Scannen | Equipmentverleih | Zertifikatsmanagement | Infoscreens | LAN | Medientechnik | Notebookwagen | Radiatus

Security | Videospinne | Servicequalität | eLP | Externe Services | Moodle | Panopto

Moderne Authentifizierungssysteme

Standard im Internet?



Stellt die Weiche