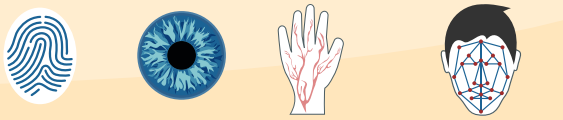
Erfolgreiche Authentifikation

Biometrie: Nahezu jede Eigenschaft einer Person kann als biometrisches Merkmal verwendet werden, sofern sie die folgende Anforderungen erfüllt:

- Jede Person besitzt diese Merkmale
- Das Merkmal ist für jede Person unterschiedlich
- Das Merkmal bleibt nahezu unverändert
- Das Merkmal kann von Sensoren erfasst werden

Es wird zwischen aktiven und passiven Merkmalen unterschieden. Passive Merkmale erfordern keine eigene Aktion. Für aktive Merkmale werden jedoch Muster aus dem aktiven Verhalten des Nutzers abgeleitet.

Physische Merkmale (Passiv):



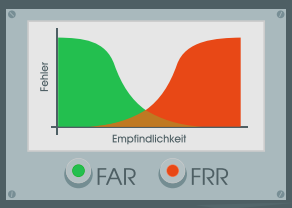
Fingerabdruck | Irismuster | Handvenen | Gesichtserkennung

Verhaltensmerkmale (Aktiv):

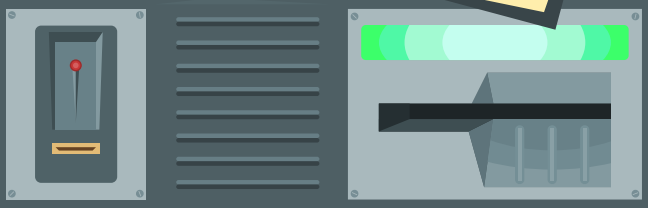
Unterschrift | Stimme | Bewegung | Tastenanschlag

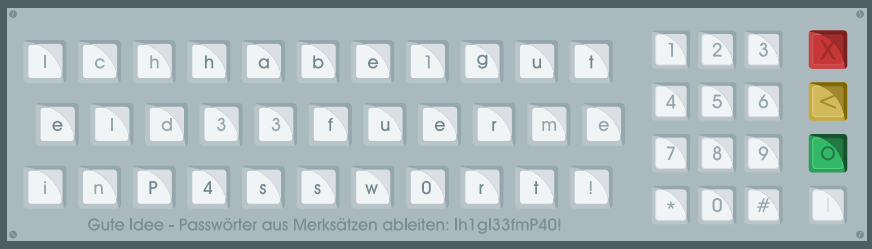
Anmelden über:

Passwort & PIN + + − − − −	• Einfache Integration • Intuitive Nutzung	• Benutzerunfreundlich • Viele bekannte Angriffe • Unsicherheitsfaktor Mensch • Begrenzt anwendbar
Biometrie + + + − − −	• Personenerkennung • Robust gegen Angriffe • Einfache Verwendung	• Kopierbar • Kostenintensiv • Zusätzliche Hardware
Starke Authentifikation + + + + − −	• Robust gegen Angriffe • Keine Geheimnisübermittlung • Zweiter Faktor • Vielfalt	• Infrastruktur notwendig • Teilweise extra Hardware



Biometrie: Leistungsfähigkeit hängt stark von der Falschrückweisungsrate (FRR) und Falschakzeptanzrate (FAR) ab. Je kleiner die Überschneidung, desto besser die Leistung des Systems und desto geringer die Gesamtfehlerrate.





Passwort: Passwörter werden heute in IT- und Internetdiensten benutzt. Sie sind jedoch anfällig für viele bekannte Angriffe und dadurch nicht ideal. Um ein Mindestmaß an Sicherheit zu gewährleisten, ist die Einhaltung der Passwort-Regeln daher Pflicht.

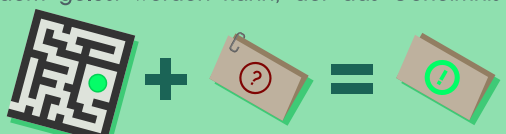
PIN: PINs verhalten sich fast genau wie Passwörter, nur dass diese bei der Eingabe auf Zahlen beschränkt sind. Daher ist hier besondere Sorgfalt geboten. Da PINs in der Regel nur 4 Zeichen lang sind, gibt es genau 10.000 Kombinationsmöglichkeiten, die sehr schnell zu erraten sind.

Passwort Regeln:

- Mindestens 12 Zeichen
- Groß- und Kleinschreibung
- Sonderzeichen und Zahlen
- Jeder Dienst ein eigenes Passwort
- Maximal 30 Tage Gültigkeit
- Sinnfreie Zeichenkette

Einmal Passwort: Ein im Vorfeld verteiltes Passwort (z.B. TAN) wird einmalig zu einem bestimmten Zweck benutzt. Danach verliert es seine Gültigkeit. Alternativ kann ein Passwort auch durch ein vorher definiertes Verfahren generiert werden.

Starke Authentifikation: Als Grundlage für starke Authentifikation dient das Challenge Response Verfahren. Zwei Parteien besitzen dabei ein gemeinsames Geheimnis, dass zur Authentifizierung genutzt, aber nicht übertragen wird. Eine Challenge lässt sich dabei als kryptographisches Rätsel beschreiben, das nur von jemandem gelöst werden kann, der das Geheimnis kennt.



Zwei-Faktor-Authentifizierung: Kommt zusätzlich zum Challenge Response Verfahren ein zweiter Faktor hinzu, spricht man von Zwei-Faktor-Authentifizierung. Ein zweiter Faktor kann beispielsweise der Besitz eines Zusatzgerätes, ein biometrisches Merkmal oder ein Passwort sein. Werden mehrere solcher Faktoren genutzt, spricht man von einer Multi-Faktor-Authentifizierung.

XignQR: Modernes Kombinationsverfahren mit dem eigenen Smartphone. Es arbeitet komplett passwortlos und basiert auf modernster Kryptographie. XignQR erlaubt dabei eine einfache Verwendung bei starker Authentifizierung.

https://www.xignsys.com/

Authentifikationsverfahren

Institut für Internet-Sicherheit - if(is)

https://www.internet-sicherheit.de

Stand: März 2017
Bereich: Anwendersicherheit
Autor(en): Bothe, David
bothe@internet-sicherheit.de
Wacowski, Sebastian
wacowski@internet-sicherheit.de