

Anforderungen an eine biometrische Authentisierung nach BSI TR-03166

Dr. Stephan Bergmann, Referent

Omnisecure, Berlin, 22.05.2023



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Das Beispiel Smartphone.
Zentrales Element für ...



Das Beispiel Smartphone. Zentrales Element für ...



Smarthome



Identitätsnachweis



Soziale Netzwerke



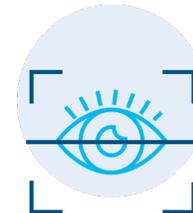
Gesundheitswesen



Kommunikation



Finanzwesen

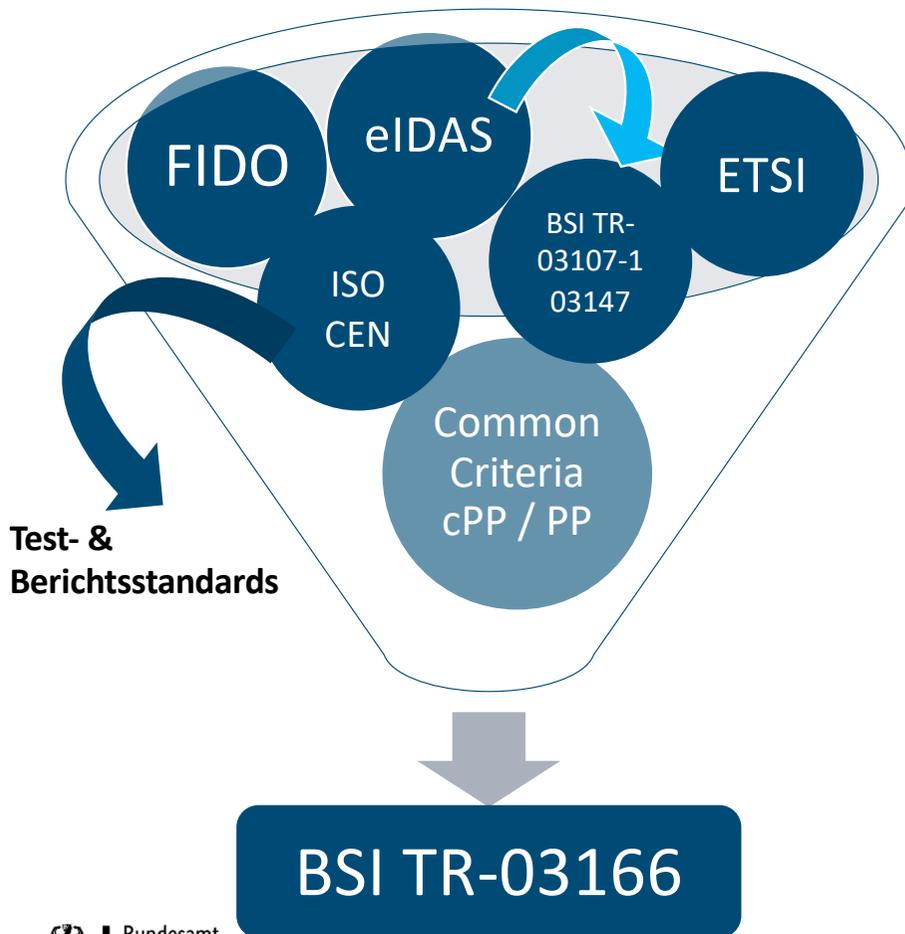


Nationale Anforderungen an biometrische Verifikations- und Authentisierungssysteme sind wichtig, weil...

- übergeordnete europäische Regularien zumeist generisch und unspezifisch sind.
 - VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS)
 - BSI TR-03107-1 & BSI TR-03147
- privatwirtschaftlich definierte Standards mehr auf Nutzerfreundlichkeit, als auf Sicherheit ausgelegt sind.
 - z.B. FIDO Biometrische Anforderungen , ETSI TS-103 732 V1.1.1, ETSI TS 119 461 V1.1.1
- etablierte Testmethodologien nach Common Criteria sind aufwändig und mit Nutzungszeiträumen von Verbraucherendgeräten schwer vereinbar.

... sie füllen den Anwendungsraum zwischen nationalen / europäischen Gesetzesgrundlagen und zum Teil stark industrietriebenen Normen.

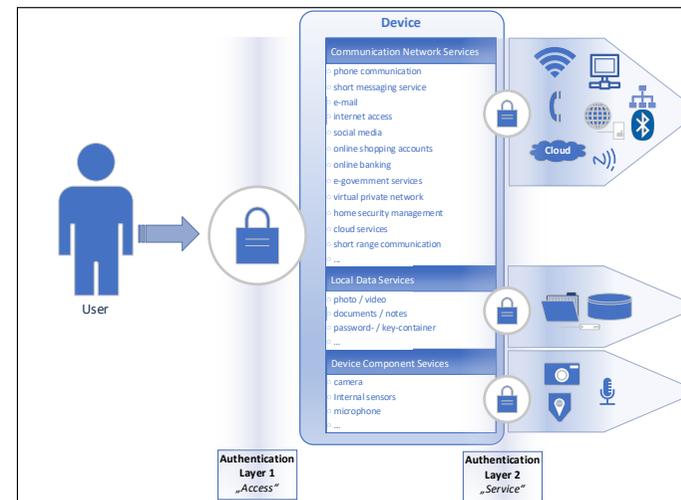
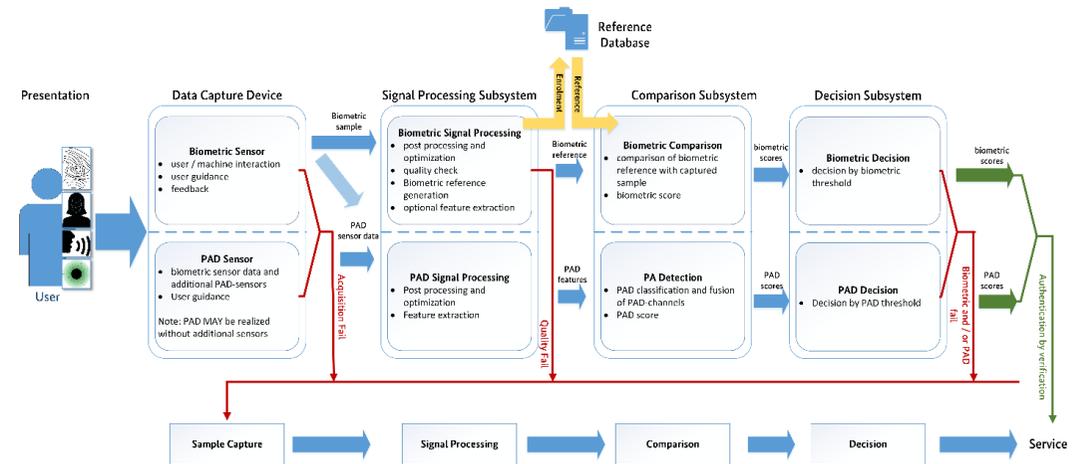
Verfügbare Biometriestandards sind nur begrenzt nutzbar.



Standard	Level	Performanz Falschakzeptanzrate (FAR)	Präsentationsangriffs-erkennung (PAD)
FIDO Biometric Requirements 3.0			<p>Ungeeignet für Anwendung mit besonders schützenswerten Daten, z.B. medizinische Daten.</p> <p>“Unsupervised Szenarien” erfordern ausreichende PAD!</p>
ETSI TS 103 732 V1.1.1 “Consumer Mobile Device Protection Profile”			
NIAP PP Mobile Device Fundamentals Version 3.3			
eIDAS / BSI TR-03107-1			Common Criteria Evaluation, aktuell wenig geeignet. Offene Fragen: z.B. Re-Zertifizierung nach Updates

Das macht das BSI in der BSI TR-03166 anders als andere Standards.

- Das BSI versucht ein Gesamtüberblick mobiler biometrischer Systeme und möglicher Angriffsvektoren zu geben.
- Usability und Anwendungsbeispiele werden im geringen Maße angesprochen.
- Es werden Möglichkeiten zur verbesserten Authentisierung mittels Biometrie aufgezeigt, die hardwareunabhängig umgesetzt werden können.
- Bestrebungen Sicherheitsevaluation und –abschätzungen greifbarer zu machen. Zwischenwege aus einfacher Prüfung und Inspektion / Schwachstellenuntersuchung



Kernanforderungen der BSI TR-03166

	BSI TR-03107-1		BSI TR-03166	
	Performanz (FAR)	Resistenz gegen Angriffspotential	Performanz (FAR)	Resistenz gegen Angriffspotential (Ausschließlich Presentation Attack Detection)
Normal	1 : 3.333 – 1 : 33.333	enhanced-basic	≤ 1 : 10.000	Basic → BSI definierte Liste
Substantiell	1 : 33.333 – 1 : 333.333	moderate	≤ 1 : 33.333	Enhanced-Basic → BSI definierte Liste + Evaluator erstellt weitere relevante Angriffsinstrumente
Hoch	≤ 1 : 333.333	high	≤ 1 : 333.333	Moderate → BSI definierte Liste + Evaluator erstellt weitere relevante Angriffsinstrumente

Reduktion der zu erbringenden Performanz durch multi-modale und –instantielle Ansätze



Zusätzliche organisatorische Maßnahmen:

- Re-Authentisierungsintervalle

Weitere implementierbare Maßnahmen:

- Unterschiedliche biometrische Charakteristiken für unterschiedliche Applikationen

Ausnutzung technischer Möglichkeiten und organisatorischer Maßnahmen

Verwendung unterschiedlicher biometrischer Modalitäten

Verwendung unterschiedlicher biometrischer Instanzen für verschiedene Applikationen

Wiederholte Präsentation eines biometrischen Merkmals

Anpassbare Sensitivität des Vergleichsalgorithmuses

Unterschiedliche Modalitäten erfordern unterschiedliche Angriffsinstrumente

Mehr biometrische Informationen notwendig

Mehrmalige Angriffserkennung & zusätzlich Merkmale

Detailliertere / hochwertigere Angriffsinstrumente notwendig

Verwendung unterschiedlicher Finger



Herausforderungen bei der Evaluation biometrischer Systeme



Biometrische Performanz

Große Anzahl an Testpersonen erforderlich.
→ Rule of 3 / 30

Kleiner, aber feiner Unterschied
Falschakzeptanzrate und
Falschvergleichsrate



Präsentationsangriffserkennung

Angemessene Prüfmetriken und Angriffsinstrumente für Anwendungsszenarien

Datenquelle für Angriffsinstrumente?

Ab wann ist ein System angemessen sicher?

Biometrie ist nicht deterministisch. Eine Evaluation hat Performanz, wie auch Angriffserkennung zu umfassen.

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Stephan Bergmann
Referent

stephan.bergmann@bsi.bund.de

Tel. +49 (0) 228 9582 6838

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Deutschland
Digital•Sicher•BSI•

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Tätigkeiten des BSI im Bereich Evaluation biometrischer Systeme und was hat das mit Fernidentifikation zu tun?

Mittwoch 24.05 10:20 - 11:00 Forum 16-B
Geprüfte Biometrie- praktische Einblicke in das Biometrie-Evaluations-Zentrum (BEZ)

Mittwoch 24.05 14:15 - 15:15 Forum 19-A
Fernidentifikation im Jahr 2023

