



Zertifizierungen Biometrischer System

Stand der Technik in 2020

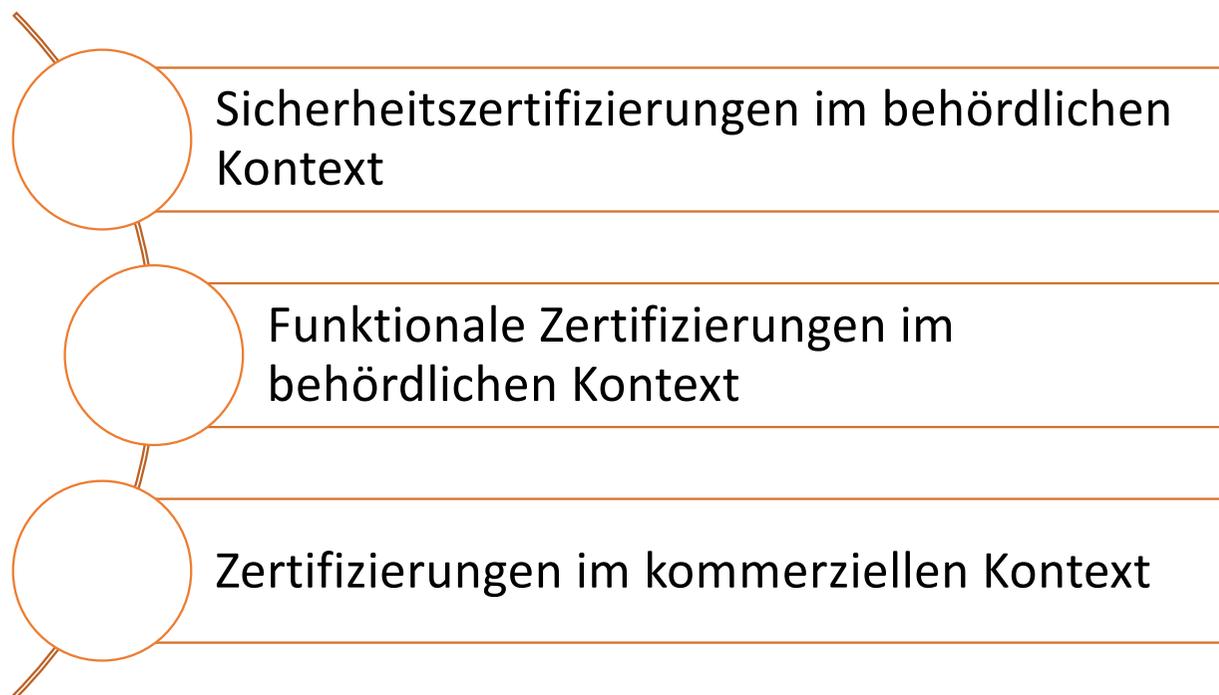


Wer ist die konfidas?

- Arbeitsschwerpunkt: IT-Sicherheit, insbesondere IT-Assurance
- Aktuelle Schwerpunktthemen:
 - Überwindbarkeit biometrischer Systeme
 - Zertifizierung biometrischer Systeme
 - FIDO
 - Technische Sicherheitseinrichtungen
 - Die Zukunft der IT-Sicherheit in Europa



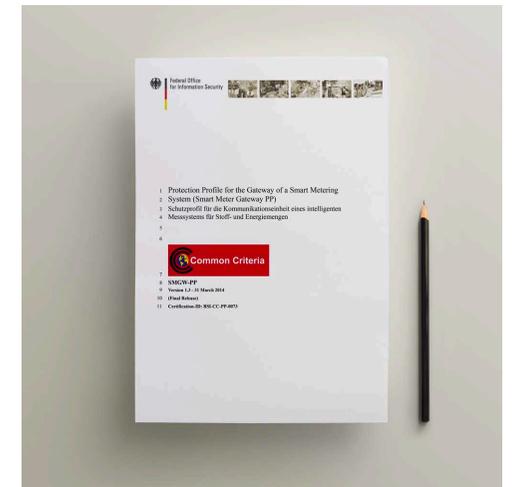
Inhalt





Sicherheitszertifizierungen im behördlichen Kontext

- Der behördliche Einsatz biometrischer Verfahren ist traditionell gut reguliert
- Der aktuelle “Stand der Technik” für Sicherheitszertifizierungen in diesem Bereich sind die Common Criteria (aka ISO/IEC 15408)
- Es existieren verschiedene Schutzprofile zur Definition der Anforderungen an die Vertrauenswürdigkeit und die Funktionalität biometrischer Verfahren





Zertifizierte Produkte¹

- Fingerprint PAD Kit ZF1/F1
- MorphoSmart Optic 301
- ...



1) <https://bit.ly/30tXtTL>



Funktionale Zertifizierungen im behördlichen Kontext

- Während sich die Common Criteria auf die Sicherheitseigenschaften fokussiert, erfordern manche Anwendungen biometrischer Verfahren aber auch die Bereitstellung bestimmter Funktionen oder die Einhaltung bestimmter Standards
- In diesen Fällen kommen (in Deutschland) aktuell z.B. Technische Richtlinien des BSI zum Einsatz
- Technische Richtlinien definieren funktionale Anforderungen, die eingehalten werden müssen und erlauben auch die Zertifizierung
- Darüber hinaus gibt es auch international vergleichbare Richtlinien (z.B. Zertifizierungen gemäß Appendix F des FBI)





Beispiele Technischer Richtlinien

- BSI TR-03104 Produktionsdatenerfassung, -qualitätsprüfung und Übermittlung für hoheitliche Dokumente
- BSI TR-03121 Biometrie in hoheitlichen Anwendungen
- BSI TR-03122 Konformitätspezifikation zur Technischen Richtlinie TR-03121 Biometrie in hoheitlichen Anwendungen
- BSI TR-03123 XML-Datenaustauschformat für hoheitliche Dokumente



Zertifizierte Produkte¹

- HDCryptServer (BSI TR-03132) 
- V-Änderungsterminal (BSI TR-03105) 
- Speed Capture Station (BSI TR-03121) 
- VISOTEC Expert 800 Release (BSI TR-03105) 

¹) <https://bit.ly/2FY8CCJ>

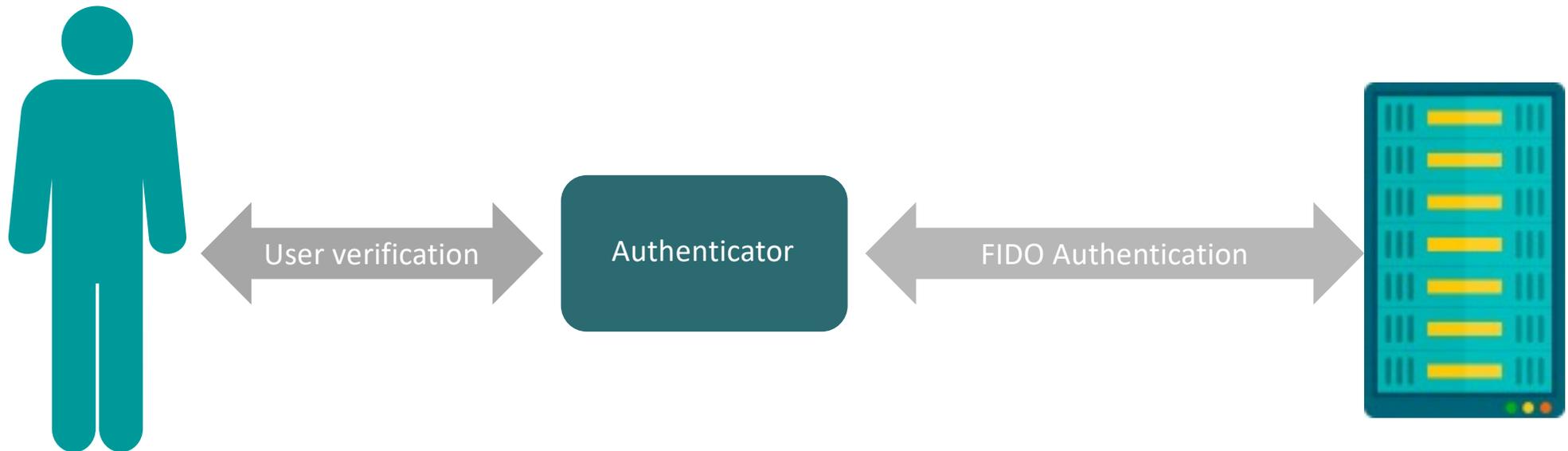


Wer/was ist **fido**[™] ? CERTIFIED

- The FIDO Alliance is working to **change the nature of authentication** with open standards that are **more secure than passwords** and SMS OTPs, simpler for consumers to use, and **easier** for service providers to deploy and manage.
- The FIDO Alliance works to fulfill its mission by:
 - Developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users
 - Operating industry certification programs to help ensure successful worldwide adoption of the specifications
 - Submitting mature technical specification(s) to recognized standards development organization(s) for formal standardization



FIDO: Das grundlegende Prinzip



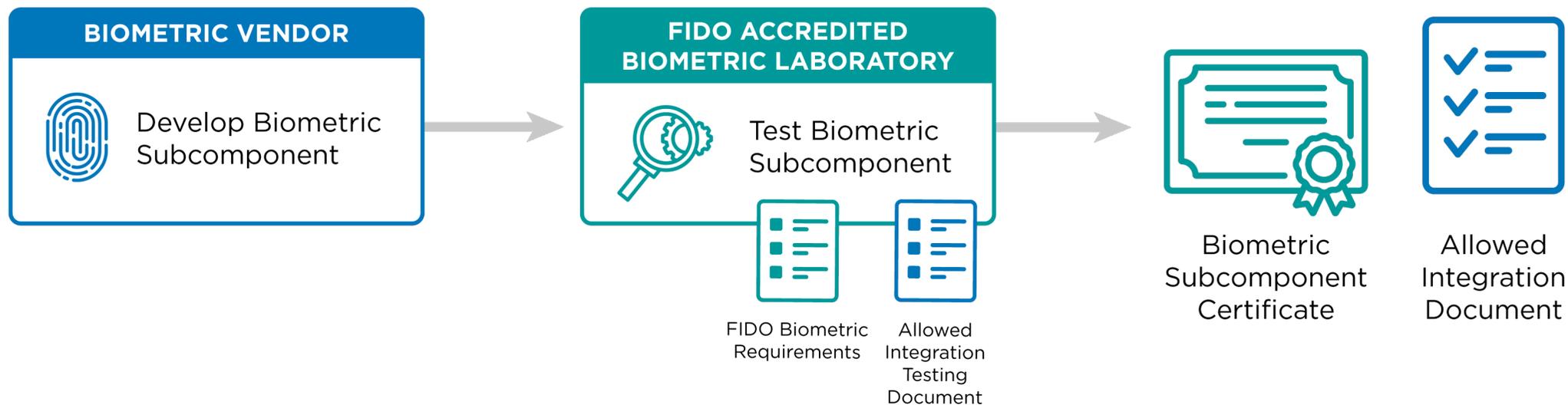


FIDO biometric certification program

- Für einen Authenticator, der mit Level 2+ oder höher zertifiziert werden soll, müssen biometrische Komponenten (sofern der Authenticator sie verwendet) zertifiziert sein
- Die Zertifizierung der biometrischen Komponente erfolgt in einem separaten Prozess, in aller Regel vor der Zertifizierung des Authenticators
- Eine biometrische Komponente kann separat zertifiziert werden und dann in einen (oder mehrere) Authenticator integriert werden
- Das Programm zur Zertifizierung biometrischer Komponenten wird auch von Herstellern genutzt, die keine Pläne zur Integration haben



FIDO BIOMETRIC CERTIFICATION TESTING STEP 1: BIOMETRIC SUBCOMPONENT





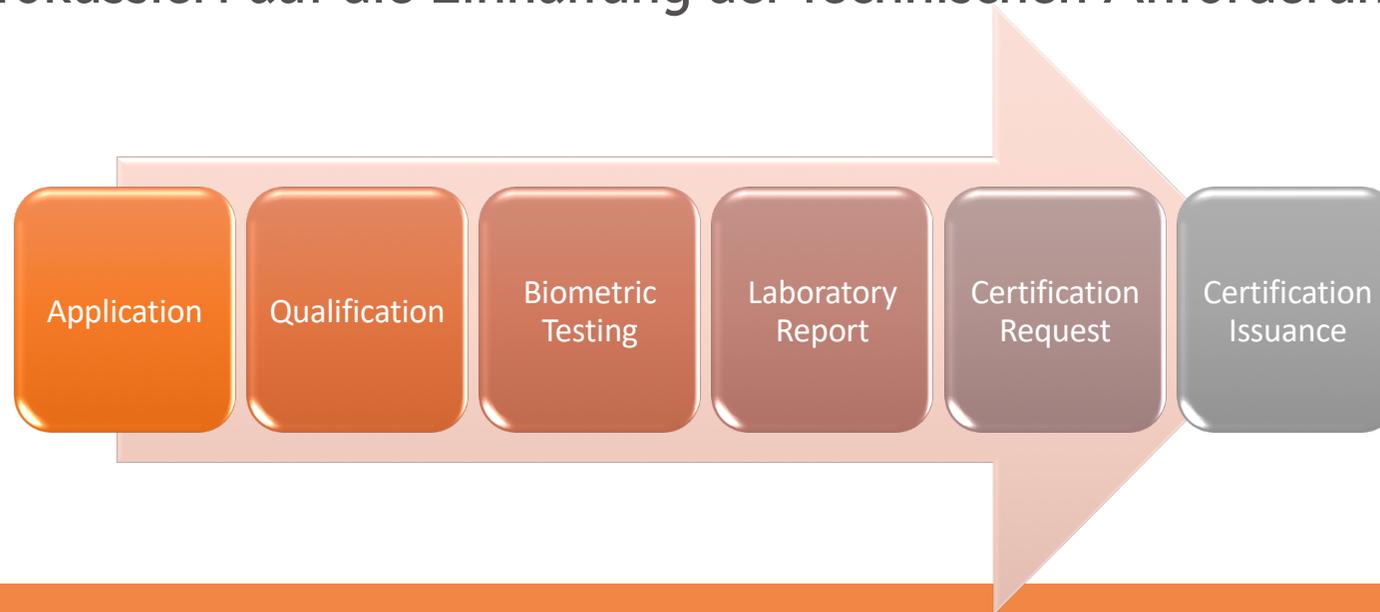
FIDO biometric criteria

- **Anforderungen Performanz**
 - FAR < 1 : 10.000
 - FRR < 3 : 100
 - Performanz getestet durch unabhängiges Labor
 - (Mindest)Größen des Tests durch FIDO Spezifikation vorgegeben
 - Optional kann der Hersteller eine Selbstattestierung zur FAR (zusätzlich) angeben
- **PAD**
 - FIDO definiert drei Klassen von Artefakten (basierend auf dem Aufwand)
 - Aktuell werden Klassen A und B getestet
 - PAD Tests sind verbindlich
 - FIDO Kriterien erlauben Restfehler



Der Zertifizierungsprozess

- Der Zertifizierungsprozess ist recht schlank gehalten und fokussiert auf die Einhaltung der technischen Anforderungen





FIDO certified products¹

- Samsung Galaxy S10
- Samsung Galaxy S10+
- Samsung Galaxy S105G
- Cirrus Logic VeriFi
- [...]
- [...]
- [...]

¹) <https://fidoalliance.org/certification/fido-certified-products/>



Schlussfolgerung und Ausblick

- Der Bedarf an unabhängigen Zertifizierungen biometrischer Verfahren im kommerziellen Umfeld steigt
- Die Verwendung der FIDO Zertifizierung für Applikationen außerhalb des FIDO Ökosystems zeigt den Bedarf für Zertifizierungen im kommerziellen Umfeld
- Die aktuellen Aktivitäten zur Umsetzung des Cyber Security Act in Europa bilden eine gute Grundlage für die Zertifizierung biometrischer Verfahren



Vielen Dank!

- Fragen oder Anmerkungen gerne auch an
- Nils Tekampe
- nt@konfidas.de
- <https://konfidas.de>

