



Biometrische Erkennungsverfahren

Anforderungen und Prüfmethoden

ENTWURF

Vorgesehen als Ausgabe VdS 3112 : 2010-07 (01)

Dieser Richtlinienentwurf ist mit der Fachöffentlichkeit abgestimmt und kann ab sofort als Grundlage für Prüfungen und Zertifizierungen verwendet werden. Bis zum endgültigen Erscheinen der Richtlinien kann noch mit Änderungen gerechnet werden.

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174

D-50735 Köln

Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

Copyright by VdS Schadenverhütung GmbH. Alle Rechte vorbehalten.

VdS-Richtlinien für Sicherheitstechnik

Biometrische Erkennungsverfahren

Anforderungen und Prüfmethoden

ENTWURF

Vorgesehen als Ausgabe VdS 3112 : 2010-07 (01)

Dieser Richtlinienentwurf ist mit der Fachöffentlichkeit abgestimmt und kann ab sofort als Grundlage für Prüfungen und Zertifizierungen verwendet werden. Bis zum endgültigen Erscheinen der Richtlinien kann noch mit Änderungen gerechnet werden.

Inhalt

1	Allgemeines	4
1.1	Geltungsbereich.....	4
1.2	Gültigkeit.....	4
2	Normative Verweisungen	4
3	Begriffe, Definitionen und Abkürzungen	5
3.1	Abkürzungen.....	6
4	Einführung	6
4.1	Allgemeines	6
4.2	Biometrische Prozesse	6
4.3	Kennzahlen	8
5	Anforderungen	9
5.1	Schutz gegen Umwelteinflüsse	9
5.2	Funktionssicherheit.....	9
5.3	Bedienungssicherheit	9
5.4	Sabotagesicherheit.....	10
5.5	Dokumentation.....	11
6	Prüfmethoden	11
6.1	Schutz gegen Umwelteinflüsse	11
6.2	Funktionssicherheit.....	12
6.3	Bedienungssicherheit	12
6.4	Sabotagesicherheit.....	13
6.5	Dokumentation.....	13

1 Allgemeines

1.1 Geltungsbereich

Diese Richtlinien für Sicherungstechnik, Biometrische Erkennungsverfahren, Anforderungen und Prüfmethode n gelten für Produkte der Einbruchmeldetechnik, Zutrittskontrolltechnik und elektronische Schlösser, die mit biometrischen Merkmalen arbeiten und enthalten Festlegungen zur Beurteilung und Prüfung von biometrischen Merkmalen. Weitere Anwendungsgebiete sind grundsätzlich nicht ausgeschlossen und werden von diesen Richtlinien ebenfalls abgedeckt, falls biometrische Merkmale zur Anwendung kommen.

Die in den Richtlinien für die entsprechenden Produkte festgelegten Anforderungen (beispielsweise hinsichtlich der unterscheidbaren Codes) werden durch diese Richtlinien umgesetzt und durch adäquate Prüfmethode n ergänzt.

Diese Richtlinien gelten in Verbindung mit den Richtlinien für Einbruchmeldeanlagen, Allgemeine Anforderungen und Prüfmethode n, [VdS 2227](#) und den Richtlinien für Gefahrenmeldeanlagen, Schutz gegen Umwelteinflüsse, Anforderungen und Prüfmethode n, [VdS 2110](#). Für softwaregesteuerte Anlageteile gelten zusätzlich die Richtlinien für Brandschutz- und Sicherungstechnik, Software, Anforderungen und Prüfmethode n, [VdS 2203](#).

1.2 Gültigkeit

Diese Richtlinien für Sicherungstechnik, Biometrische Erkennungsverfahren, Anforderungen und Prüfmethode n sind ab dem 01.07.2009 gültig.

2 Normative Verweisungen

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils letzte Fassung.

[VdS 2110](#) Richtlinien für Gefahrenmeldeanlagen, Schutz gegen Umwelteinflüsse, Anforderungen und Prüfmethode n

[DIN EN 50130-4](#) Alarmanlagen, Teil 4: Elektromagnetische Verträglichkeit – Produktfamiliennorm

[DIN EN 50130-5](#) Alarmanlagen, Teil 5: Methoden für Umweltprüfungen

[EN 60950-1](#) Einrichtungen der Informationstechnik -Sicherheit – Teil 1: Allgemeine Anforderungen

[ISO/IEC 19795-1](#) Information technology – Biometric performance testing and reporting – Part 1: Principles and framework

[ISO/IEC 19795-2](#) Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies and for technology and scenario evaluation

[VdS 2227](#) Richtlinien für Gefahrenmeldeanlagen; Allgemeine Anforderungen und Prüfmethode n für Gefahrenmeldeanlagen Version 2

[VdS 2119](#) Richtlinien für Einbruchmeldetechnik; Schalteinrichtungen, Anforderungen

[VdS 2358](#) Richtlinien für Zutrittskontrollanlagen, Anforderungen

VdS 2359 Richtlinien für Zutrittskontrollanlagen, Prüfmethode

VdS 2396 Richtlinien für mechanische Sicherungseinrichtungen, Hochsicherheitsschlösser für Wertbehältnisse, Anforderungen und Prüfmethode.

3 Begriffe, Definitionen und Abkürzungen

Die allgemeinen Begriffe sind in den Richtlinien für Einbruchmeldeanlagen, Allgemeine Anforderungen und Prüfmethode; **VdS 2227** zusammengefasst. Zusätzlich gelten die folgenden Begriffe:

Biometrische Merkmale

Die aus den biologischen oder verhaltensabhängigen Eigenschaften einer Person erfassten charakteristischen Informationen.

Falschakzeptanzrate (FAR)

Die FAR ist die Häufigkeit, mit der **nichtberechtigte** Personen als berechtigt **akzeptiert** werden. Sie wird wie folgt berechnet:

$$\text{FAR} = \frac{\text{Zahl der erfolgreichen unberechtigten Verifizierungen}}{\text{Gesamtzahl der unberechtigten Verifizierungsversuche}}$$

Hinweis: FAR wird im 1:1-Vergleich ermittelt

Falschrückweisungsrate (FRR)

Die FRR ist die Häufigkeit, mit der **berechtigte** Personen unberechtigterweise **zurückgewiesen** werden. Sie wird wie folgt berechnet:

$$\text{FRR} = \frac{\text{Zahl zurückgewiesene Verifizierungsvers. berechtigter Personen}}{\text{Gesamtzahl aller Verifizierungsversuche berechtigter Personen}}$$

Hinweis: FRR wird im 1:1-Vergleich ermittelt

Enrolment (Einlernen)

Erfassung von biometrischen Merkmalen einer Person und anschließende Verarbeitung und Speicherung des Templates als Referenzmuster dieser Person.

Identifikationsmodus

Betriebsart, in der ein Live-Template mit allen gespeicherten Referenz-Templates verglichen wird (1:n-Vergleich).

Live-Template

Template, das während eines Erkennungsvorganges gebildet wird.

Referenz-Template

Template, das während eines Enrolment erzeugt wurde und zum Vergleich beim Erkennungsvorgang herangezogen wird.

Sample

Die von einem Sensor erzeugten Informationen (Rohdaten) körperspezifischer Merkmale.

Template

Datensatz, der aus den extrahierten biometrischen Merkmalen einer Person mittels eines Algorithmus gebildet wird. Templates sind demnach abhängig vom erzeugenden Algorithmus.

Verifikationsmodus

Betriebsart, in der ein Live-Template mit einem bestimmten Referenz-Template verglichen wird (1:1-Vergleich).

3.1 Abkürzungen

In den Richtlinien werden folgende Abkürzungen verwendet

FAR	Falschakzeptanzrate
FRR	Falschrückweisungsrate
IMT	Identifikationsmerkmalsträger

4 Einführung

4.1 Allgemeines

Charakteristische biologische oder verhaltensabhängige Eigenschaften einer Person können zur Feststellung der Identität verwendet werden. Diese erfolgt bei biometrischen Erkennungsverfahren in einer weitgehend automatisierten Form durch Erfassung, Verarbeitung und Auswertung der gewonnenen personenbezogenen Daten, die sich in verschiedene Prozesse unterteilen lässt.

4.2 Biometrische Prozesse

4.2.1 Enrolment

Um eine Person anhand ihrer biometrischen Merkmale erkennen zu können, müssen diese zunächst erfasst, verarbeitet und als Referenzmuster gespeichert werden.

Das aus dem biometrischen Merkmal gebildete Referenztemplate wird in einer Datenbank hinterlegt.



Bild 1: Ablauf eines Enrolment

4.2.2 Identifikation/Verifikation

In gleicher Weise wie beim Enrolment werden die biometrischen Merkmale erfasst und verarbeitet, sodass ein Lifetemplate gebildet wird, das mit einem biometrischen Referenztemplate aus der biometrischen Enrolment-Datenbank verglichen wird. Da es keine vollkommene Übereinstimmung des Lifetemplates mit dem Referenztemplate gibt, wird beim Vergleich der beiden Templates ein Ähnlichkeitswert ermittelt.

Bei der Verifikation wird das Lifetemplate nur mit einem Referenzmuster aus der Enrolmentdatenbank verglichen, die die angegebene Identität repräsentiert. Übersteigt der gemessene Ähnlichkeitswert den Schwellwert so war die Verifikation erfolgreich.

Bei der Identifikation werden alle in der Enrolmentdatenbank hinterlegten Referenzmuster mit dem Lifetemplate verglichen. Es wird die Identität herangezogen, bei der der Vergleich die größte Ähnlichkeit erbracht hat und den Schwellwert überschritten hat.

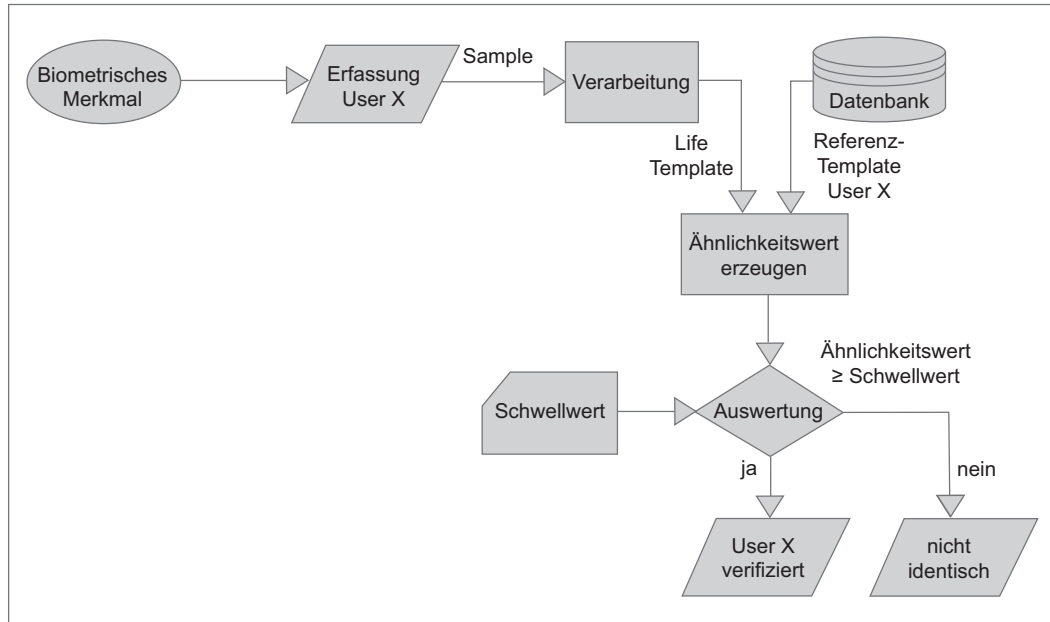


Bild 2: Ablauf einer Verifikation

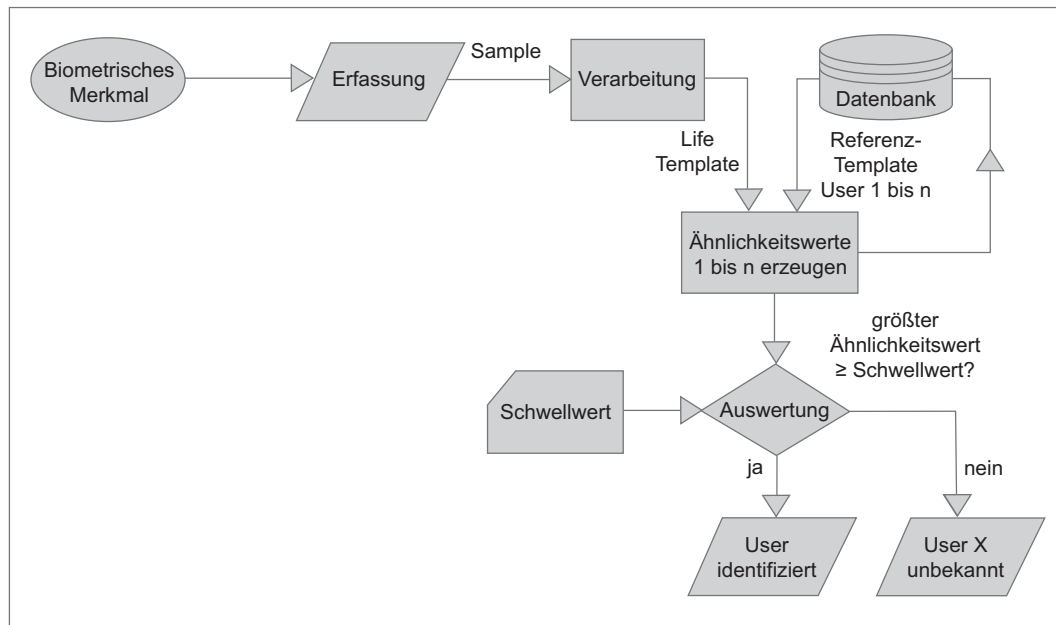


Bild 3: Ablauf einer Identifikation

4.3 Kennzahlen

Die Anforderungen an biometrische Identifikationsmerkmale sind in Analogie zu anderen Identifikationsmerkmalen aufgebaut.

Um biometrische Merkmale mit den anderen Identifikationsmerkmalen (geistig und materiell) vergleichen zu können, kann die Anzahl der unterscheidbaren Codes herangezogen werden.

Hinweis: Die Arbeitspunkteinstellung in einer installierten Anlage darf nicht zu Lasten einer höheren FAR veränderbar sein (siehe Kapitel Bedienungssicherheit).

4.3.1 Falschakzeptanzrate

Als Maßzahl bei biometrischen Anwendungen steht die Falschakzeptanzrate nach folgender Definition zur Verfügung

$$\text{FAR} = \frac{\text{Zahl der erfolgreichen unberechtigten Verifizierungen}}{\text{Gesamtzahl der unberechtigten Verifizierungsversuche}}$$

Dabei wird die FAR in der Form ermittelt, dass sich die Anzahl der Versuche auf 1:1-Vergleiche (Verifikationen) bezieht. Sie stellt die Wahrscheinlichkeit dar, dass eine unberechtigte Person erfolgreich gegenüber einem Referenztemplete verifiziert wird. Somit ist der Reziprokwert der FAR die Anzahl der unterscheidbaren Kombinationen.

Beispiel: Eine FAR von 10^{-4} würde 10^4 unterscheidbare Codes bedeuten.

Bei einem 1:n-Vergleich, wie er bei der Identifikation der Fall ist, steigt die Wahrscheinlichkeit einer Falschakzeptanz gegenüber der FAR für Verifizierung an

Wenn FAR_V die Wahrscheinlichkeit für eine Falschakzeptanz im Verifikationsmodus ist, so ist die Wahrscheinlichkeit für das Nichtauftreten einer Falschakzeptanz bei einem Vergleichsmuster gleich $1 - \text{FAR}_V$.

Bei einem Vergleich mit N Mustern (Anzahl der in einer Datenbank hinterlegten Referenztemplates) ist die Wahrscheinlichkeit für das Nichtauftreten einer Falschakzeptanz

$$(1 - \text{FAR}_V)^N$$

Die Gegenwahrscheinlichkeit, dass mindestens eine Falschakzeptanz im Identifikationsmodus auftritt, beträgt dann

$$\text{FAR}_I = 1 - (1 - \text{FAR}_V)^N$$

Hieraus geht unmittelbar hervor, dass Geräte mit Identifikationsmodus nach der resultierenden FAR_I bewertet werden müssen, welche mit steigender Anzahl der hinterlegten Referenztemplates ansteigt.

4.3.2 Falschrückweisungsrate

Die Falschrückweisungsrate steht in unmittelbarem Zusammenhang mit der Bedienbarkeit. Sie ist wie folgt definiert:

$$\text{FRR} = \frac{\text{Zahl zurückgewiesene Verifizierungsvers. berechtigter Personen}}{\text{Gesamtzahl aller Verifizierungsversuche berechtigter Personen}}$$

Dabei wird die FRR in der Form ermittelt, dass sich die Anzahl der Versuche auf 1:1-Vergleiche (Verifikationen) bezieht.

Die Falschrückweisungsrate hängt mit der Falschakzeptanzrate zusammen. Je niedriger die FAR ist, desto höher ist die FRR und umgekehrt.

5 Anforderungen

Im Geltungsbereich dieser Richtlinien werden biometrische Erkennungsverfahren als Bestandteil von Produkten der Einbruchmeldetechnik, Zutrittskontrolltechnik und elektronischen Schlössern betrachtet. Die für diese Produkte geltenden gerätespezifischen Anforderungen sind somit implizit auch für die Komponenten zur biometrischen Erkennung relevant. Zusätzliche oder abweichende Anforderungen im Zusammenhang mit den spezifischen Eigenschaften von biometrischen Erkennungsverfahren werden in den folgenden Absätzen beschrieben.

5.1 Schutz gegen Umwelteinflüsse

Es gelten die zum Schutz gegen Umwelteinflüsse des jeweiligen Gerätes gestellten Anforderungen in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen).

5.2 Funktionssicherheit

Es gelten die zur Funktionssicherheit des jeweiligen Gerätes gestellten Anforderungen in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen).

Das Gerät muss mit einer Arbeitspunkteinstellung (Kombination FAR/FRR) betrieben werden, so dass die in den gerätespezifischen Richtlinien geforderte Mindestanzahl der Kombinationen (z. B. nach Tabelle „Mögliche Kombinationen von IM“ in [VdS 2119](#)) erfüllt ist.

Besondere Anforderungen an die Dokumentation mit Bezug auf die speziellen Eigenschaften biometrischer Erkennungsverfahren sind zu berücksichtigen.

Beispiel: Die Dokumentation muss Angaben zu den Arbeitspunkteinstellungen enthalten.

Hinweis: Die FAR wird gemäß Abschnitt 4.3.1 ermittelt.

5.3 Bedienungssicherheit

Es gelten die zur Bedienungssicherheit des jeweiligen Gerätes gestellten Anforderungen in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen).

Darüber hinaus gelten folgende spezifischen Anforderungen:

5.3.1 Arbeitspunkteinstellung

Durch geeignete Maßnahmen ist sicherzustellen, dass der Arbeitspunkt von unberechtigten Personen nicht geändert werden kann (Beispiel: Bei Einbruchmeldeanlagen ist in Zugangsebene 1 und 2 eine Änderung des Arbeitspunktes nicht zulässig)

5.3.2 Speicherung der Arbeitspunkteinstellung

Ist im Betrieb eine Arbeitspunkteinstellung möglich, muss eine Änderung der Einstellung gespeichert werden. Folgende Daten müssen gespeichert werden: Neuer eingestellter Wert, Datum, Uhrzeit, Berechtigter. Die Dauer der Speicherung oder die Anzahl der zu speichernden Änderungen richtet sich nach den Angaben in den produktspezifischen Richtlinien.

5.3.3 Automatische Arbeitspunkteinstellung

Eine automatische (adaptive) Anpassung der Arbeitspunkteinstellung (z. B. zum Ausgleich schlechterer Samples aufgrund eines verschmutzten Sensors) ist nicht zulässig.

5.3.4 Maximale Falschrückweisungsrate (FRR)

Mit der Verwendung von biometrischen Erkennungsverfahren geht die Wahrscheinlichkeit einher, dass die Identifizierung von berechtigten Personen trotz richtiger Anwendung des Erkennungsverfahrens misslingt. Die mit der gewählten Arbeitspunkteinstellung verbundene FRR darf den Wert von 10 % nicht überschreiten.

5.3.5 Enrolment mit Rechtevergabe

Wenn das Enrolment mit Rechtevergabe verbunden ist, müssen die gerätespezifischen Anforderungen erfüllt werden. (Beispiel: Enrolment in einer Schalteinrichtung ist direkt mit der Schaltberechtigung verknüpft. Daraus folgt Enrolment nur in Zugangsebene 3 und 4 zulässig.)

5.4 Sabotagesicherheit

5.4.1 Sabotageschutz

Es gelten die zum Sabotageschutz des jeweiligen Gerätes gestellten Anforderungen in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen).

5.4.2 Kompromittierung von biometrischen Merkmalen

5.4.2.1 Nachbildung von biometrischen Merkmalen

Die erfolgreiche Nutzung von Nachbildungen von biologischen Eigenschaften oder deren charakteristischen biometrischen Merkmalen muss in Abhängigkeit vom entsprechenden Profil gemäß der nachfolgenden Tabelle verhindert werden.

Profil	Täterprofil	Möglichkeit zur Nachbildung von biometrischen Merkmalen
Profil 1	Laie	Reaktivierung von Latenzbildern
Profil 2	Semi-Profi	Nachbildung mit einfachen Mitteln z. B. Vorhalten von Abbildungen
Profil 3	Fachmann	Überwindung mit bearbeiteten Nachbildungen

Profil 1:

Das biometrische Erkennungsverfahren muss mindestens so ausgeführt sein, dass ein Überwinden mit einfachen Mitteln durch Personen ohne fachliche Kompetenz (Laien) nicht möglich ist.

Profil 2:

Das biometrische Erkennungsverfahren muss mindestens so ausgeführt sein, dass ein Überwinden mit erhöhtem Aufwand (Kosten und Zeit) durch Personen mit bedingter fachlicher Kompetenz („Semi-Profi“) nicht möglich ist.

Profil 3:

Das biometrische Erkennungsverfahren muss mindestens so ausgeführt sein, dass ein Überwinden mit nur mit hohem Aufwand (Kosten und Zeit) durch Personen mit fachlicher Kompetenz und Systemkenntnissen (Fachmann) möglich ist.

Hinweis: Das anzuwendende Profil ergibt aus den spezifischen Geräte-Richtlinien, wobei Profil 1 für die unterste Klasse und Profil 3 für die höchste Klasse gilt.

5.4.3 Speicherung von Templates

Templates müssen verschlüsselt gespeichert werden oder nur über Zugriffsschlüssel auslesbar sein, wenn der Speicher zugänglich ist (z. B. der Speicher befindet sich außerhalb des Sicherheitsbereiches). Alternativ muss der Speicherinhalt bei unbefugtem Zugriff gelöscht werden.

5.5 Dokumentation

Es gelten die zur Dokumentation des jeweiligen Gerätes gestellten Anforderungen in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen).

6 Prüfmethode

6.1 Schutz gegen Umwelteinflüsse

Die zum Schutz gegen Umwelteinflüsse des jeweiligen Gerätes gestellten Anforderungen in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen) werden im Rahmen der Geräteprüfungen abgeprüft. Die entsprechenden Prüfmethode sind den Richtlinien für Gefahrenmeldeanlagen, Schutz gegen Umwelteinflüsse, Anforderungen und Prüfmethode [VdS 2110](#) beschrieben.

6.2 Funktionssicherheit

Es wird geprüft, ob die Anforderungen an die Funktionssicherheit, wie sie in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen) festgelegt sind, erfüllt sind.

Mit geeigneten Mitteln ist nachzuweisen, dass die geforderten FAR-Werte mit angegebenen Arbeitspunkteinstellungen erreicht werden. Eine standardisierte und reproduzierbare Prüfung ist, soweit als möglich, anzuwenden.

Darüber hinaus wird geprüft, ob in der Dokumentation vollständig, konsistent und nachvollziehbar die speziellen technischen Eigenschaften von biometrischen Erkennungsverfahren berücksichtigt sind. Es muss mindestens eine Beschreibung der Arbeitspunkteinstellung (Kombination FAR/FRR) für die richtlinienkonforme Anwendung vorhanden sein.

6.3 Bedienungssicherheit

Es wird geprüft, ob die Anforderungen an die Bedienungssicherheit, wie sie in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen) festgelegt sind, erfüllt sind.

6.3.1 Arbeitspunkteinstellung

Darüber hinaus wird geprüft, ob die Arbeitspunkteinstellung durch unbefugte Personen (z. B. in der Zugangsebene 1 oder 2) möglich ist. Die Prüfung ist nicht bestanden, wenn dies möglich ist. Arbeitspunkteinstellung

6.3.2 Speicherung der Arbeitspunkteinstellung

Es wird weiterhin geprüft, ob für den Fall, dass eine Arbeitspunkteinstellung möglich ist, eine Speicherung jeder Einflussnahme auf den Arbeitspunkt mit mindestens folgenden Angaben vorgenommen wird: Neuer eingestellter Wert, Datum, Uhrzeit, Berechtigter.

Die Dauer der Speicherung oder die Anzahl der zu speichernden Änderungen richtet sich nach den Angaben in den produktspezifischen Richtlinien und wird ebenfalls nachvollzogen und auf Einhaltung der Anforderungen überprüft

6.3.3 Automatische Arbeitspunkteinstellung

Es wird geprüft, ob eine automatische (adaptive) Anpassung der Arbeitspunkteinstellung (z. B. zum Ausgleich schlechterer Samples aufgrund eines verschmutzten Sensors) möglich ist. Ist dies der Fall ist diese Prüfung nicht bestanden.

6.3.4 Maximale Falschrückweisungsrate (FRR)

Bei gemäß diesen Richtlinien gewählter Arbeitspunkteinstellung, wird mittels empirischer Versuche oder einem standardisierten und reproduzierbaren Verfahrens überprüft, ob die FRR einen Wert von 10% nicht überschreitet.

Eine Falschrückweisung wird als solche gezählt, wenn drei Versuche in Folge mit dem gleichen biometrischen Merkmal abgewiesen werden.

6.3.5 Enrolment mit Rechtevergabe

Es wird überprüft, ob die den gerätespezifischen Richtlinien entsprechenden Anforderungen zur Rechtevergabe in Verbindung mit dem Enrolment erfüllt sind. (Beispiel: Enrolment in einer Schalteinrichtung ist direkt mit der Schaltberechtigung verknüpft. Demnach darf das Enrolment nur in Zugangsebene 3 und 4 möglich sein.)

6.4 Sabotagesicherheit

6.4.1 Sabotageschutz

Es wird geprüft, ob die Anforderungen an den Sabotageschutz, wie sie in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen) festgelegt sind, erfüllt sind.

6.4.2 Kompromittierung von biometrischer Merkmalen

Es wird geprüft, ob das Gerät Angriffen, die den Täterprofilen 1 bis 3 gemäß Abschnitt 5.4.2.1 entsprechen, widersteht

6.4.2.1 Speicherung von Templates

Es wird geprüft, ob die Templates verschlüsselt gespeichert werden oder nur über Zugriffsschlüssel auslesbar sind, wenn der Speicher zugänglich ist bzw. ob alternativ der Speicherinhalt bei unbefugtem Zugriff gelöscht wird.

6.5 Dokumentation

Es ist zu prüfen, ob die geforderte Dokumentation entsprechend den Anforderungen, wie sie in den jeweiligen gerätespezifischen Richtlinien (beispielsweise in den Richtlinien [VdS 2119](#) für Schalteinrichtungen zum Einsatz in Einbruchmeldeanlagen) vollständig, konsistent und nachvollziehbar verfügbar ist.

