Amt für Justizvollzug Graubünden
Uffizi per l'execuziun giudiziala dal Grischun
Ufficio per l'esecuzione giudiziaria dei Grigioni

Amt für Justizvollzug Graubünden
Rechtsdienst
Grabenstrasse 15
CH-7001 Chur

[redacted]
www.ajv.gr.ch

Amt für Justizvollzug Graubünden, Grabenstrasse 15, 7001 Chur

Departement für Justiz, Sicherheit und Gesundheit
[redacted]
Hofgraben 5
7000 Chur

DEPARTEMENT FÜR JUSTIZ, SICHERHEIT UND GESUNDHEIT DES KANTONS GRAUBÜNDEN

14. NOV. 2025

Post:	Geschäft:
an;	
o zur Kenntnis	o zur Erledigung
o zu den Akten	o zur Stellungnahme
o zur Besprechung	o Frist:
Datum:	

Chur, 13. November 2025

Beschwerde [redacted] betreffend biometrische Erfassung

Sehr geehrt[redacted]

Mit Schreiben vom 10. November 2025 bitten Sie uns, im Zusammenhang mit o.g. Beschwerde einige Fragen zu beantworten.

Es ist anzumerken, dass in der Justizvollzugsanstalt (JVA) Cazis Tignez zwei verschiedene Biometriesysteme im Einsatz sind – einerseits der Zutritt für Mitarbeitende mit Fingerprint und andererseits der Zutritt für Besuchende mit dem Iris-Scan. Die nachfolgenden Antworten auf Ihre Fragen beziehen sich ausschliesslich auf das Fingerprint-System für Besuchende:

1. *Erfolgt jeweils eine «one to one» Verifizierung oder ein Abgleich 1:N?*
   Zur Besucher-Erkennung werden Iris-Scanner eingesetzt. Die sog. TBS-Leser laufen im Identifikationsmodus, d.h. der Besucher lässt sein Gesicht fotografieren und der TBS-Leser erkennt die Person anhand der Iris. Dabei werden beide erfassten Iris zu Templates verarbeitet. Diese werden mit der gesamten in der JVA Cazis Tignez gespeicherten Datenbank an Templates abgeglichen (1:N). Der Benutzer wird erkannt, wenn eines der beiden Templates in vordefiniertem Ausmass mit einem Referenztemplate übereinstimmt. Beim Referenz-Template handelt es sich um den Iris-Scan, welcher bei Ersteintritt in die Anstalt erfasst wurde. Bezüglich Sicherheit (falsche Akzeptanz) bestehen keine Bedenken – der eingesetzte Leser kann 50'000 Iris-Paare unterscheiden, derzeit sind in der JVA Cazis Tignez noch weniger als 5'000 Besucher biometrisch erfasst.

2. *Ist die Bestimmbarkeit der betreffenden Person möglich oder erfolgt – wie oben umschrieben – die Verifizierung nur durch zwei Vergleichsbilder?*
   Anhand des Templates kann der TBS-Leser die Person identifizieren, falls sie vorgängig bei der JVA Cazis Tignez biometrisch erfasst wurde. Das TBS System kennt keine Bilder – bei der Erfassung werden die aufgenommenen Fotos zwar angezeigt, gespeichert werden aber nur verschlüsselte Templates. Weitere Informationen können Sie den Beilagen entnehmen.

3. *Werden Profile erstellt?*
   Nicht im Sinne von Personalprofilen, sondern nur biometrische Templates. Personenprofile im Sinne von Rasse, Geschlecht etc. kennt TBS nicht. Wer wann in der Anstalt ein und ausgeht, kann allerdings manuell nachvollzogen werden.

4. *Welche technischen Massnahmen gewährleisten die Zweckbindung (Art. 23b JVG und Art. 37 VEV) der biometrischen Erfassung?*
   Zur Gewährleistung der Zweckbindung werden die biometrischen Daten in einem getrennten System gespeichert, der Zugriff ist nur autorisiertem Personal vorbehalten, und eine Verknüpfung mit anderen Datenbanken ist technisch ausgeschlossen.

5. *Welche Vorkehrungen wurden getroffen, um die erhobenen biometrischen Daten gemäss Art. 37 Abs. 4 VEV zu schützen?*
   Sämtliche biometrischen Daten sind gehasht und somit irreversibel (das Originalbild kann nicht hergestellt werden). Die Templates werden doppelt verschlüsselt. Der Biometrie-Server steht in einem Raum, der vor physischem Zugriff durch Unbefugte geschützt ist.

Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung.

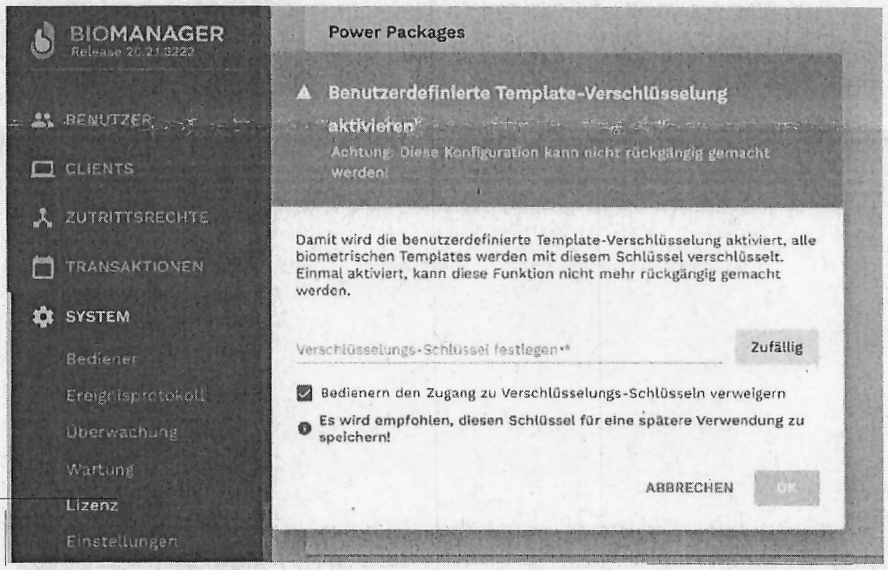
Freundliche Grüsse
Amt für Justizvollzug Graubünden

[redacted]

Beilage:
- TBS – Touchless Biometric Systems
- TBS Information – Umgang mit Biometrie-Daten (Fingerprint Mitarbeitende)

Touchless Biometric Systems

Technologie - White Paper:
Biometrie-System & Aspekte der Datensicherheit



HINWEIS: Die aktuelle Version dieses Dokumentes ist immer verfügbar unter:
https://cloud1.tbs-biometrics.com/index.php/s/AV3as4wQlP9mKJ0

Release	Autor	Bemerkung
11.09.2024	TM/AG	Erste deutsche Fassung
17.01.2025	TM/AG	TwoFish Schlüssellänge ergänzt

Einleitung

Zutrittskontroll- und Zeiterfassungssysteme basieren häufig auf Token (Schlüssel oder Karte, "etwas, das ich habe") oder Wissen (PIN, "etwas, das ich kenne"). Diese "schwachen" Authentifizierungsmethoden genügen den hohen Sicherheitsanforderungen nicht, da sie leicht an Unbefugte weitergegeben oder verloren gehen, gestohlen oder kopiert werden können.

Die Verwendung biometrischer Merkmale erhöht die Authentifizierungssicherheit, da die Identität des Benutzers durch die Messung eines physischen Körpermerkmals, "etwas, das ich bin", unbestreitbar nachgewiesen wird, da dieses nicht weitergegeben werden kann.

Der effektive Einsatz eines biometrischen Systems hängt von verschiedenen Aspekten ab, und der biometrische Sensor ist nur ein Teil einer vernetzten Sicherheitskette. TBS versteht diese systemischen Anforderungen und bietet Lösungen an, die sich nicht nur auf Sensoren beschränken, sondern sämtliche Herausforderungen der Daten- und Systemsicherheit im Zusammenhang mit Biometrie lösen.

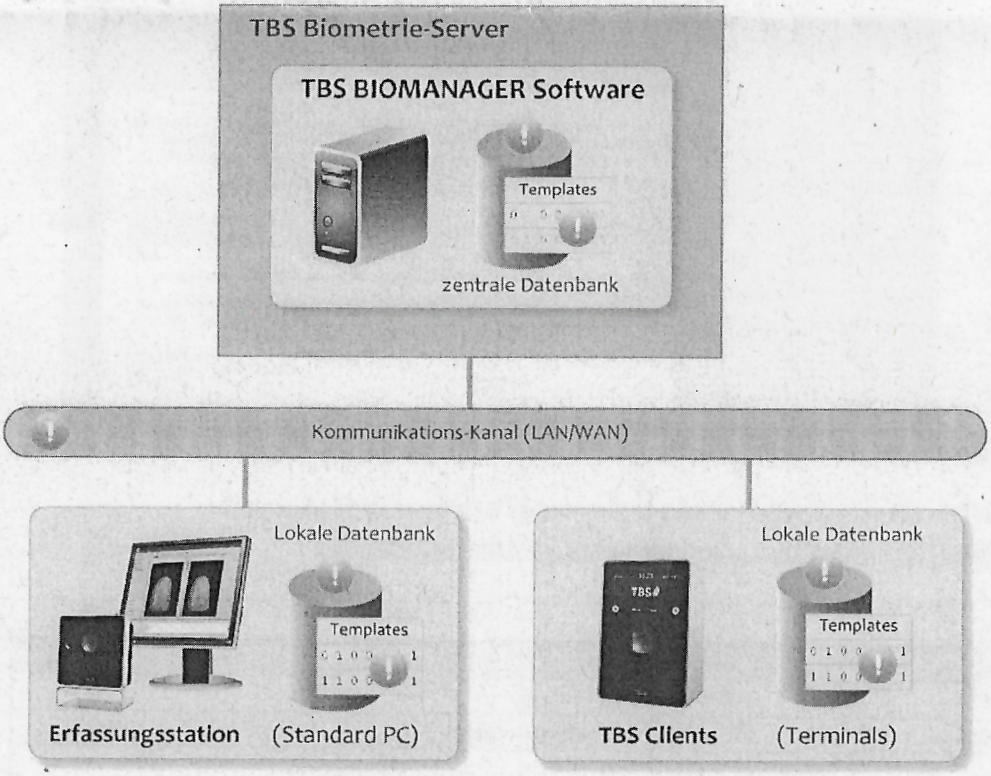
Im Zusammenhang mit biometrischen Lösungen stehen zwei Sicherheitsbedenken im Vordergrund:

(1) Fälschung der biometrischen Identität

Dies kann zwar nicht vollständig verhindert werden, aber die Aufgabe eines Anbieters biometrischer Systeme besteht darin, den Aufwand zu erhöhen, den ein potenzieller Eindringling betreiben muss, um das System zu überwinden.

(2) Unbefugter Zugriff auf biometrische Daten

Unternehmen sind oft erfahren im Umgang mit vertraulichen Daten, aber biometrische Daten fügen eine neue Dimension hinzu. Die biometrische Identifizierung beinhaltet die Offenlegung besonders schützenswerter personenbezogener Daten, so dass der Schutz der Privatsphäre der Benutzer und die Wahrung der Datenintegrität von höchster Bedeutung sind.



Bedrohungen für eine biometrische Client-Server Installation

Dieses Whitepaper befasst sich mit Massnahmen zur Verbesserung der Datensicherheit und -integrität auf allen Ebenen der TBS-Infrastruktur. Die grössten Herausforderungen bestehen darin, wie sensible personenbezogene Daten in einer vernetzten Umgebung gesichert werden können und wie man potenzielle Eindringlinge daran hindert, das System zu kompromittieren.

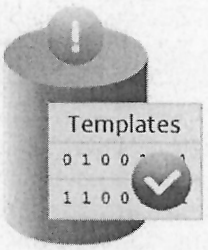
Sichere Datenspeicherung auf den Geräten

Bei der biometrischen Erfassung werden Benutzerdaten und Biometriedaten einer Person erstellt und in der zentralen TBS-Datenbank gespeichert. Sowohl die Daten selbst als auch der Speichervorgang müssen sorgfältig behandelt werden, um Identitätsdiebstahl zu vermeiden.

Um ein Client-Server-System gegen Angriffe zu schützen, müssen beide Seiten durch kryptografische Methoden gesichert werden. Obwohl man davon ausgeht, dass die meisten Angriffe auf der Client-Seite stattfinden (falls diese in einer unsicheren Zone installiert sind), müssen die Server-Daten ebenfalls sicher gespeichert werden.

Die TBS-Lösung (Terminals in Kombination mit der BIOMANAGER-Software) basiert auf Software-Komponenten, die eine starke zweistufige Datenverschlüsselung implementieren:

(1) Verschlüsselung des biometrischen Templates



Obwohl das Bild des biometrischen Merkmals (Finger, Hand, Iris oder Gesicht) bei der biometrischen Erfassung angezeigt wird, werden diese "nativen" Daten weder gespeichert noch weitergegeben. Stattdessen wandelt der biometrische Algorithmus direkt im TBS-Leser das Bild in eine mathematische Beschreibung um, die als "biometrisches Template" bezeichnet wird. Diese Templates sind eindeutige Identifikatoren einer Person, die als binärer Code von bis zu 5 kB Grösse gespeichert werden. Es ist unmöglich, anhand dieses Templates das Originalbild wieder herzustellen.

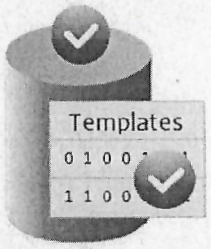
Aus der Sicherheitsbetrachtung sind diese Templates der sensibelste Teil einer biometrischen Anlage und erfordern daher besondere Aufmerksamkeit.

Alle von TBS erstellten biometrischen Templates werden durch einen Verschlüsselungsalgorithmus geschützt. Es handelt sich um eine symmetrische Blockchiffre, die mit variabler Schlüssellänge arbeitet. TBS verwendet Schlüssel mit einer Länge von mindestens 64 Bit. TBS-Leser mit der älteren Firmware Version 2.xx verwenden einen in der Firmware codierten *BlowFish*-Schlüssel.

Mit BIOMANAGER ENTERPRISE hat TBS die neue Funktion 'Custom Template Encryption' eingeführt. Sie ermöglicht die freie Konfiguration des Verschlüsselungs-Schlüssels auf Basis von *TwoFish (256 bit)*, wodurch alle biometrischen Daten mit diesem installationsspezifischen Schlüssel verschlüsselt werden. Die in dieser Installation erfassten Templates können nur von TBS-Terminals entschlüsselt werden, die mit diesem Server verbunden sind. Damit erhält der TBS-Systembetreiber die volle Gewissheit, dass die Biometrie-Daten für immer exklusiv an den eigenen Biometrie-Server gebunden bleiben.

(2) Verschlüsselung der Datenbank auf den TBS Terminals

Für die dauerhafte Datenspeicherung implementieren die TBS-Client-Software und -Firmware eine Schnittstelle zu einer lokalen Datenbank (auf SQL-Basis). Die Daten in dieser Datenbank werden automatisch auf Speicherebene verschlüsselt, d.h. in der SQL-Datenbank-Engine selbst.



Zu diesem Zweck leitet die Datenbank-Engine alle Daten beim Lese-/Schreibzugriff durch ihre integrierte Verschlüsselung. Dieser Mechanismus wird als "transparente Verschlüsselung" bezeichnet und hat den Haupteffekt zu verhindern, dass unverschlüsselte Daten gespeichert werden.

Die Datenbank-Engine verwendet einen Advanced Encryption Standard (AES)-Algorithmus mit einer Schlüssellänge von 256 Bit zur Verschlüsselung der Daten. AES ist ebenfalls eine Blockchiffre und wurde von der US-Regierung als Verschlüsselungsstandard akzeptiert.

Der Datenbankschlüssel wird von einem komplexen Passwort abgeleitet, das automatisch im TBS-Client generiert wird. Dieses Passwort basiert auf einem UID-Hardwareblock, der eine eindeutige ID liefert, was die gespeicherten Daten auf jedem Gerät einzigartig macht.

Zusammengefasst bedeutet dies: Auch wenn der Datenbankinhalt auf allen TBS-Clients in derselben biometrischen Installation identisch ist, sind es die verschlüsselten Daten nicht.

Jeder TBS-Leser verfügt über eine eigene, einzigartige Version der Datenbank, die sicherstellt, dass (verschlüsselte) Daten, die von einem Gerät gestohlen wurden, nicht zur Kompromittierung eines anderen Geräts verwendet werden können.

Sichere Datenspeicherung auf dem Server

Die Templates in der zentralen Server-Datenbank werden mit dem benutzerdefinierten Verschlüsselungsschlüssel verschlüsselt, oder mit dem Standard-BlowFish-Schlüssel, falls der TBS-Server noch auf einer älteren WebEdition-Version läuft.

Die Datenbank auf dem Server selbst ist nicht verschlüsselt, denn:

- Der Server muss als sichere Umgebung in einer professionellen IT-Umgebung betrachtet werden
- SQL Server ist in verschiedenen Versionen verfügbar und bietet verschiedene Möglichkeiten zur Verschlüsselung von Daten.
- TBS überlässt die Wahl den Partnern und Kunden, um ihre spezifische Anwendung zu definieren.
- Zur Sicherheit auf dem Server gehören auch Backup-Routinen und der anschliessende Schutz dieser Backup-Daten.

Sicherer Datenaustausch

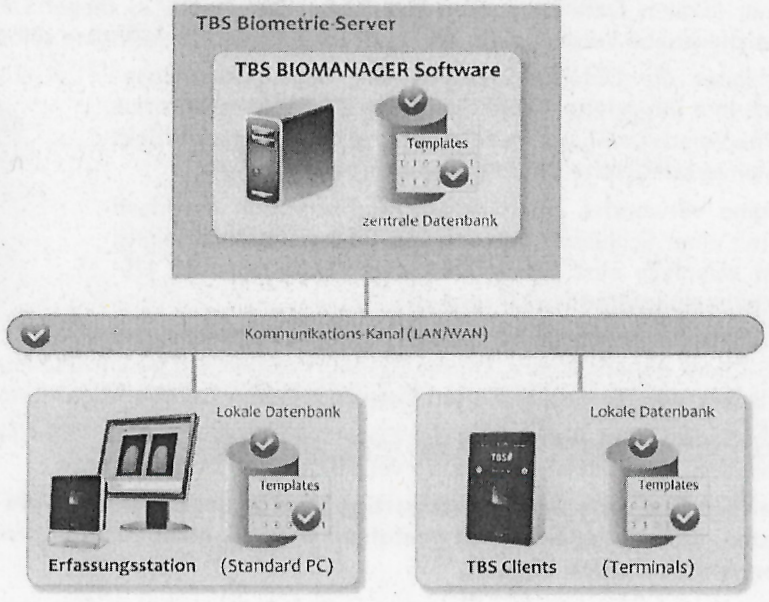
Während der Schutz sensibler Benutzerdaten ein Schlüsselelement für die Sicherheit biometrischer Systeme darstellt, ist der Schutz der Datenkommunikation zwischen Clients und Server ein weiteres. Das Verhindern von Abhören, Manipulation und Datenfälschung sind wichtige Anforderungen in einem vernetzten System.

Die TBS-Kommunikationsinfrastruktur basiert standardmässig auf HTTPS, d.h. die TBS-Clients und der TBS-Server kommunizieren in einem gesicherten, für andere Netzwerkteilnehmer nicht sichtbaren Kanal. Mit TBS BIOMANAGER ENTERPRISES R20.x wurde die Aktivierung der SSL-Kanalverschlüsselung durch selbstsignierte Zertifikate vereinfacht. Standorte, die eine höhere Sicherheit benötigen, können bestehende Zertifikate importieren, die von einer anderen Zertifizierungsstelle als TBS signiert wurden (öffentliche oder nicht-öffentliche CA).

Um erweiterte Sicherheitsanforderungen auch in Installationen mit der älteren 'WebEdition' Serverversion zu erfüllen, kann auch dort die SSL-Verschlüsselung für den Kommunikationskanal aktiviert werden. TBS bietet dafür eine detaillierte Anleitung, einschliesslich der Installation der erforderlichen Zertifizierungsstelle und der Erstellung eines eigenen, von TBS signierten Server-Zertifikats.

Um den Kanal vollständig abzusichern, erzwingen die TBS-Clients ab Firmware 3.xx eine HTTPS-Kommunikation. HTTPS kann auch in älteren Firmware-Versionen aktiviert werden (ab Firmware 2.06.10, veröffentlicht im Januar 2021).

Zusammengefasst schützen die genannten Massnahmen den TBS-Systembetreiber vor den typischen Sicherheitsbedrohungen auf Server-, Client- und Kanalseite:



Zusätzliche Sicherheits-Massnahmen

Nebst den beschriebenen Mechanismen implementieren TBS-Lösungen weitere Hardware- und Softwarefunktionen, um die Sicherheit des Biometrie-Systems zu erhöhen. Dazu gehören zum Beispiel:

- Erkennung und Meldung von Angriffen (z.B. Einbruchserkennung mit Sabotagekontakt)
- sichere Kommunikation mit externen Modulen (z.B. sichere Relaisfunktion über Controller)
- intelligente Verfahren zur Validierung der TBS-Clients
- Lebenderkennung zur Vermeidung von Präsentationsattacken (auf ausgewählten Modellen)

TBS ist sich bewusst, dass ein biometrisches System nur ein Teil des gesamten Sicherheitskonzepts einer Zutrittskontrolle ist. Bitte kontaktieren Sie uns, gerne sind wir bereit, unser Wissen mit Ihren Anforderungen abzugleichen, um die optimale Lösung für Ihre Anwendung zu finden.

Portfolio an TBS Biometrie-Lesern

Das beschriebene Sicherheitskonzept und die Funktionen gelten für alle TBS-Leser, da sie dieselbe Serversoftware und eine einheitliche Firmware-Architektur verwenden.

Das aktuelle Portfolio der TBS Biometrie-Leser umfasst diese Geräte:

- 3D FLY
- 3D AIR (frühere Bezeichnung: 3D TERMINAL)
- 3D LIGHT (2D EYE)
- 3D FLASH+
- 2D IRON (2D+ TERMINAL)
- 2D SENSE (2D TERMINAL)
- 2D TIME
- 2D MOVE (2D PORTABLE)
- 2D STATION
- 2D MINI
- TBS CONTROLLER SMART+

Die 2D ENROLL und 3D ENROLL Erfassungsstationen sind reine USB Sensoren ohne interne Datenbank.

Amt für Justizvollzug Graubünden
Uffizi per l'execuziun giudiziala dal Grischun
Ufficio per l'esecuzione giudiziaria dei Grigioni

Amt für Justizvollzug Graubünden
Rechtsdienst
Grabenstrasse 15
CH-7001 Chur

[redacted]
www.ajv.gr.ch

DEPARTEMENT FÜR JUSTIZ, SICHERHEIT UND GESUNDHEIT DES KANTONS GRAUBÜNDEN

19. NOV. 2025

Post:	Geschäft:
an:	
o zur Kenntnis	o zur Erledigung
o zu den Akten	o zur Stellungnahme
o zur Besprechung	o Frist:
Datum:	

Amt für Justizvollzug Graubünden, Grabenstrasse 15, 7001 Chur

Departement für Justiz, Sicherheit und Gesundheit
[redacted]
Hofgraben 5
7000 Chur

Chur, 18. November 2025

Beschwerde [redacted] betreffend biometrische Erfassung

Sehr geehrt[redacted]

Mit Schreiben vom 13. November 2025 beantworteten wir Ihnen im Zusammenhang mit o.g. Beschwerde einige Fragen. Dabei erwähnten wir in den Vorbemerkungen, dass sich die Antworten ausschliesslich auf das «Fingerprint-System» für Besuchende beziehen würden. Dies ist nicht korrekt. Die Antworten auf die von Ihnen mit Schreiben vom 10. November 2025 aufgeworfenen Fragen beziehen sich auf das «**Iris-Scan-System**».

Bitte entschuldigen Sie die Umstände. Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse
Amt für Justizvollzug Graubünden

[redacted]