

BIOSCRYPT® V-STATION™

(bioscrypt® on board — Fingerabdruckerkennung)



Die V-Station™ integriert bioscrypt™'s bewährte Fingerabdrucktechnologie in ein komplettes Zutrittskontrollterminal und zeichnet sich u.a. durch Ethernetanschluss, ein zweizeiliges Display plus farbige LED's zur Benutzerführung und eine numerische Tastatur aus. Das Gerät kann als Stand-Alone oder mit PC-Anbindung eingesetzt werden und unterstützt in den verschiedenen Modellvarianten Identifikation, Verifikation und die Speicherung von Templates auf Mifare-Karten.

- > **EINFACHE PLUG & PLAY INSTALLATION**
- > **UNTERSTÜTZUNG VON STANDARD UND BENUTZERDEFINIERTEN WIEGAND-FORMATEN, RS 232, RS 485 UND ETHERNET-KOMMUNIKATION**
- > **TTL, ZWEIMAL LINE-IN, ZWEIMAL LINE-OUT, FREI PARAMETRIERBAR**
- > **TRANSACTION LOG FÜR 8.192 EINTRÄGE**
- > **VOLLE KOMPATIBILITÄT MIT LESERN DER VERI-SERIES**
- > **INTEGRIERTES LCD DISPLAY MIT 4X20 ZEICHEN UND NUMERISCHE TASTATUR MIT FUNKTIONSTASTEN**
- > **DEFINITION VON GRUPPEN FÜR ZEITLICH BESCHRÄNKTEN ZUTRITT**
- > **INBETRIEBNAHME UND ADMINISTRATION VOLLSTÄNDIG AM GERÄT ODER ÜBER VERIADMIN SOFTWARE**



BIOSCRYPT® V-STATION™

(bioscrypt® on board — Fingerabdruckererkennung)

> Spezifikationen

- > Abmessungen (LxBxT): 143x168x67mm
- > Kommunikation: RS 232, RS 485, Ethernet, Wiegand IN/OUT, TTL: 2x Line-In, 2x Line-Out
- > Spannungsversorgung:
 - > 12...24 V DC
 - > max. 1,5A bei 12 V DC

> Standardmodell

- > Anlernzeit < 5 sek.
- > Verifikationszeit < 1 sek.
- > EER: 0,1%
- > Maximale Anzahl der Templates: 3.000
- > Größe eines Templates: < 350byte

> Identifikations Modell

- > Anlernzeit < 5 sek.
- > Identifikationszeit < 2 sek.
- > FAR: 0,2%
- > FRR: 1,0%
- > Maximale Anzahl der Templates: 200
- > Größe eines Templates: < 2.500byte

> MIFARE® Modell

- > Anlernzeit < 5 sek.
- > Verifikationszeit < 1 sek.
- > EER: 0,1%
- > Maximale Anzahl der Templates: unbegrenzt
- > Größe eines Templates: < 350byte
- > Unterstützung von Mifare-/Multiapplikationskarten
- > Unterstützung der Mifare-Schlüsselstruktur einschließlich Hash-Funktion für Schlüssel

> Lieferumfang:

- > V-Station
- > PC-Verbindungskabel (RS-232)
- > VeriAdmin 5.0 Installations-CD
- > Installations-/Benutzerhandbuch auf CD
- > Wandmontagehalterung inkl. Zubehör
- > Anschlusskabel
- > Spezial-Innensechskantschlüssel

> erforderliches Zubehör

- > Netzteil*/Spannungsversorgung

> optionales Zubehör

- > PC (ab Pentium, Windows 98, ME, NT4, 2K, XP)
- > RS-232/RS-485-Konverter*
- > Türöffner etc.

*dieses Zubehör ist über bioscrypt® verfügbar

Biometrie Know-How

> Ability To Acquire (ATA)

ist die Anzahl der Personen aus 100 Personen, deren Fingerabdruck grundsätzlich erfasst werden kann. Moderne Sensoren wie der E-Field Sensor ermöglichen eine ATA von mehr als 99%.

> E-Field Sensor

Diese Generation neuester Sensoren arbeitet mit einem elektrischen Feld, das zwischen den lebenden Hautschichten des Fingers und dem Sensor aufgebaut wird. Es wird also nicht die Hautoberfläche erfasst, die häufig durch Trockenheit, Feuchtigkeit, Abrieb oder Verschmutzung beeinträchtigt ist, sondern die tieferliegende Lederhaut, dort, wo die Fingerlinien entstehen. Gleichzeitig wird die Sicherheit erhöht, da die Sensoren nicht mit einfachen Imitaten oder durch die Reaktivierung latenter Fingerabdrücke auf dem Sensor manipuliert werden können.

> Fehlerquoten

- > **FAR** (False Acceptance Rate) ist die Wahrscheinlichkeit, dass der Finger einer nicht berechtigten Person fälschlicherweise als berechtigt erkannt wird.
- > **FRR** (False Rejection Rate) ist die Wahrscheinlichkeit, dass der Finger einer berechtigten Person fälschlicherweise als unberechtigt zurückgewiesen wird.
- > Beide Größen sind abhängig vom gewählten Sicherheitslevel. Je höher das Sicherheitslevel (und damit der Grad der erforderlichen Übereinstimmung) gewählt wird, desto niedriger wird die FAR, gleichzeitig steigt aber auch die FRR.
- > **EER** (Equal Error Rate) ist die durchschnittliche Fehlerquote. Es gilt $EER = FAR = FRR$

> Identifikation (Vergleich 1:n)

Bei der Identifikation wird der Fingerabdruck gegen eine komplette Datenbank verglichen, um festzustellen, wer die Person ist, d.h. die Person wird identifiziert.

> Mustervergleich vs. Minutienvergleich

Beim Mustervergleich wird das komplette Muster des Fingerabdrucks in einem mehrstufigen Prozess zum Vergleich herangezogen. Im Gegensatz hierzu vergleichen minutienbasierte Systeme lediglich einzelne Punkte des Fingerabdrucks bezüglich Ihrer Lage und Orientierung.

> Template

Das Template beinhaltet die unverwechselbaren Merkmale des Fingerabdrucks, zumeist in verschlüsselter Form. Es ist keinesfalls ein komplettes Abbild des Fingers; ein Rückschluss von den Merkmalen auf das Abbild des Fingers ist ebenso nicht möglich.

> Verifikation (Vergleich 1:1)

Bei der Verifikation wird der Fingerabdruck gegen einen, z.B. durch die Benutzernummer der Person, vorgegebenen Fingerabdruck verglichen, um festzustellen, ob die Person tatsächlich die Person ist, die sie zu sein vorgibt.

> Wiegand

Das Wiegand-Protokoll wird im Bereich Zeiterfassung, Zutrittskontrolle etc. für den Datenaustausch zwischen verschiedenen Gerätetypen- und -herstellern genutzt.