Datenblatt
BioSec GateKeeper

Inhaltsverzeichnis

www.biosecgroup.com
info@biosecgroup.com

I. Überblick

BS GateKeeper ist eine komfortable, biometrie-basierte Lösung zur Überwachung und Steuerung des physischen Zutritts.

BS GateKeeper nutzt die sehr sichere und verbreitete Handvenenerkennung und ermöglicht damit benutzerfreundliches Öffnen von Türen und Drehkreuzen ohne eine aufwändige Verwaltung von Schlüsselkarten oder Schlüsseln.

BS GateKeeper ist ein modulares und flexibles System, das keine komplizierte Netzwerkstruktur voraussetzt. Es skaliert hervorragend, sowohl über die Anzahl der Benutzer als auch und über die Anzahl der Zugangsstellen.

BS GateKeeper kann Ausweise und RFID-Karten durch biometrische Authentifizierung ersetzen. Falls lokale Sicherheitsrichtlinien Ausweise oder RFID-Karten erfordern, können sie dennoch mit BS GateKeeper verwendet werden. Die papierlose Lösung spart Geld während der Betriebszeit und hilft, die Umwelt sauber zu halten.

BS GateKeeper weißt einen hohen Benutzungskomfort auf, so können z.B. Besucher flexible registriert werden. Der Besucherservice kann jede Art von Regeln zuweisen (einschließlich Etagenbeschränkungen für den Aufzug und leicht nachvollziehen, wo sich der Besucher befindet.

BS GateKeeper physische Zutrittskontroll-Lösung hat die folgenden Vorteile:

- Höchste Sicherheit bei der Identifizierung
- Das Identifizierungsmerkmal kann nicht verloren gehen, nicht weitergegeben oder nachgebaut werden, da es ein inneres biometrisches Merkmal ist.
- Höchste Erkennungsgenauigkeit über das ganze Leben: Jede Person muss nur einmal in seinem Leben an einem System registriert werden.
- Hohe Skalierbarkeit: Große Netzwerklösungen können auch aufgebaut werden.
- Zertifizierte Sicherheit nach Common Criteria
- Mehrfache Verschlüsselung für Daten und Datenübertragung (256-bit Verschlüsselung der Daten, 2048-bit Verschlüsselung bei Datenübertragung
- Schnittstelle zu Active Directory
- Hervorragende Erkennung bei höchster Sicherheit, FAR (False Acceptance Rate) 0,00008% bei FRR 0,01%
- Zukunftssicher durch vielseitige Erweiterbarkeit: Großes Spektrum weiterer Biosec Lösungen z.B. für Zeiterfassung oder Zugriffskontrolle,
- Einfache Integration: alle 3rd Party Lösungen können auch mit Hilfe von Software-, seriellen oder Wiegand- Schnittstellen unterstützt werden.
- Kann optional mit RFID (Mifare-Karten) kombiniert werden.

Die **BS GateKeeper** physische Zugangskontroll-Lösung nutzt das innovative BS LifePass handvenen-basierte biometrische Identifizierungssystem für sichere und schnelle Sicherheit. Die komplette Zugangslösung besteht aus den folgenden Elementen:

www.biosecgroup.com
info@biosecgroup.com

Hardware

- Triple 1 biometrisches Leserterminal für den Innenbereich
- BS100 biometrisches Leserterminal für Innen- und Außenbereich
- BS Guide (Registrierungsstation)
- BS CONT GK (Zugangssteuerungsgerät)
- Authentifizierungsserver
- Optional: Die Lösung kann mit Mifare RFID Lesern erweitert werden

Software

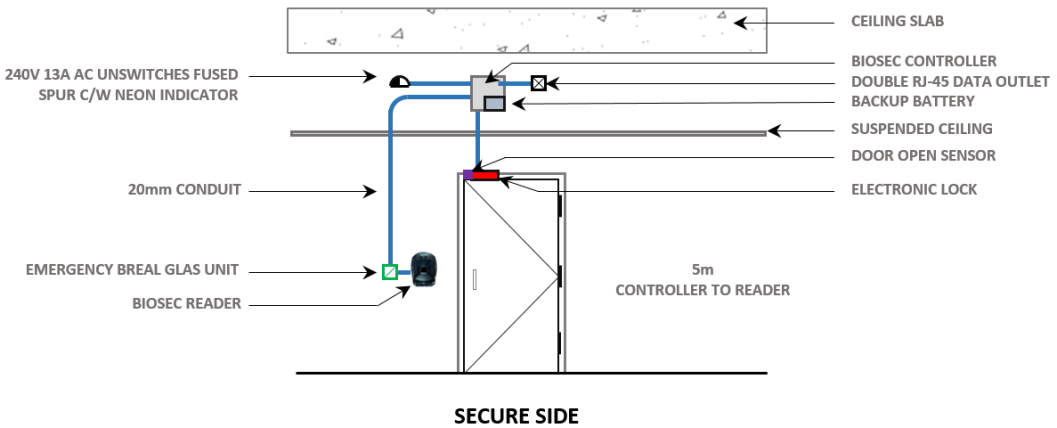
- BS Client (Client Software für jedes Terminal oder RFID Leser)
- IDENGINE (Zentrale Server-Software für die Systemadministration
- AdminSuite (System-/Benutzer-Verwaltung, Benutzeroberfläche für Registrierung)

Das **Triple 1/BS100** Terminal ist das einzige Gerät, das außerhalb des gesicherten Bereichs installiert wird. An diesem erfolgt das Lesen des Handvenenmusters mittels Sensor. Es ist mit dem lokalen Steuerungsgerät, dem BS CONT GK, mit einen USB- und einem CAT5-Kabel verbunden. Der maximale Abstand zwischen Triple 1/BS 100 und dem BS CONT GK Controller beträgt 5 Meter, kann aber über Zusatzkomponenten auf 25 Meter ausgedehnt werden.

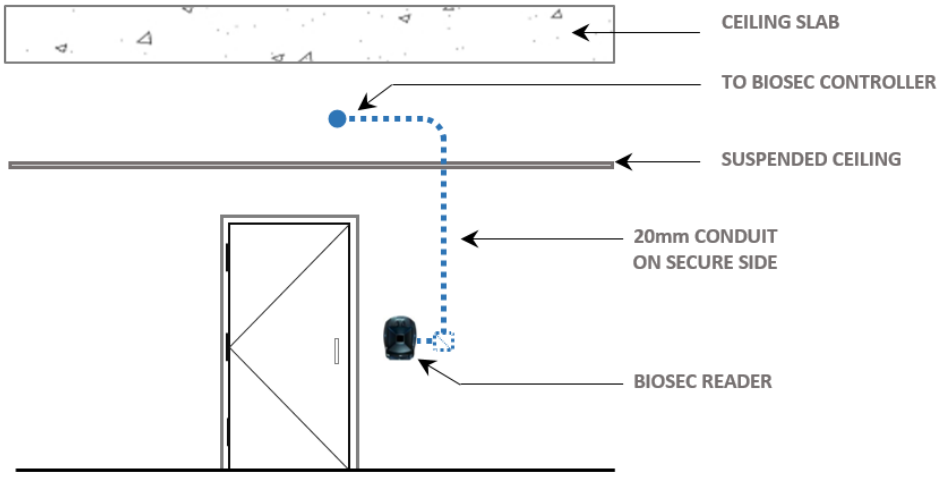
Der biometrische Leser beinhaltet keine Elektronik, die es ermöglichen würde, den Zutrittspunkt mit Hilfe des BS 100 / Triple 1 zu manipulieren.

Das lokale Steuerungsgerät, der BS CONT GK bietet eine Vielzahl von Anschlussmöglichkeiten für Industrie-Standardkomponenten, wie z. B. magnetische Schlösser, Druckknopfentriegelungen Notaus-Taster.
Die beiden folgenden Bild zeigen schematisch die Montage von Terminal und Controller:

DOOR EQUIPMENT LAYOUTS
(LOCAL CONTROLLER)



www.biosecgroup.com
info@biosecgroup.com



II. Gesamtsystem

Haupteigenschaften

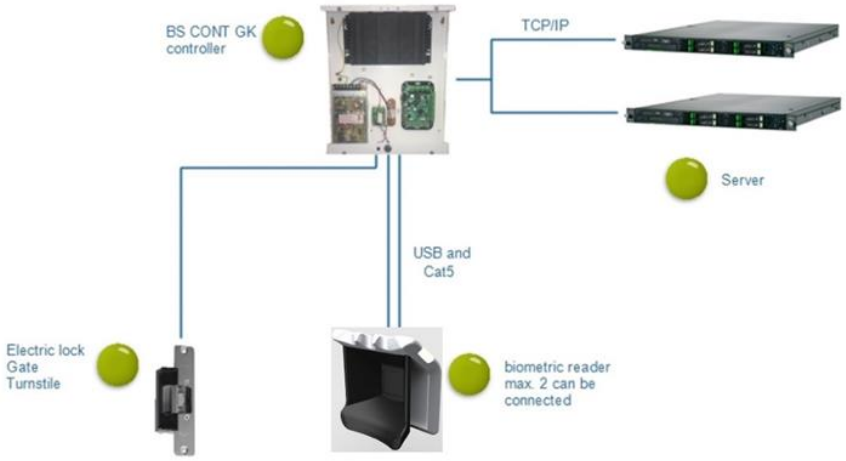
- Online und Offline- Betrieb (Verbindung zwischen Controller und Server ist unterbrochen)
- Unbeschränkte Anzahl von Türen / abhängig von der Lizenz/
- Unbeschränkte Anzahl von Benutzern / abhängig von der Lizenz/
- 1:1 oder 1:n Authentifizierung zur Verifizierung oder Identifizierung des Benutzers
- Schutz vor Doppelbenutzung (Anti-Passback, Anti-Outback)
- Sabotage Schutz, verschlüsselte Kommunikation
- Biometrische Authentifizierung dauert ~1 Sekunde.

Sicherheitseigenschaften

Alle Komponenten der BS GateKeeper-Lösung sind mit den neuesten Sicherheitsmechanismen geschützt. GateKeeper nutzt eine dreistufige Verschlüsselung (Biometrisches Template, Kommunikation, Datenbank). BioSec-Software verzichtet gänzlich auf schwer zu beherrschende Passwörter, es kann ausschließlich durch Handvenenerkennung zugegriffen werden. Der optionale RFID Leser setzt auf die neueste Mifare Technologie auf. (Bitte kontaktieren Sie uns für weitere Informationen).

www.biosecgroup.com
info@biosecgroup.com

Basis System Architektur



Technische Parameter

Benötigte Hardware:	BS 100/Triple1, BS CONT GK, Server, BS Guide
Betriebssystem für den Controller:	Windows 8.1 embedded 64 bit
Betriebssystem für Server:	Microsoft Server 2008 oder neuer, 64 bit
Betriebssystem für Adminsuite:	Windows 7 oder neuer, 64 bit
Datenbank:	MySQL, MSSQL, Oracle, PostgreSQL

III. System Komponenten

Triple1 Biometrisches Terminal

Das Triple1 ist das biometrische Leserterminal, das für die 1:n Identifizierung geeignet ist. Es ist mit dem lokalen Controller (BS CONT GK) mit einem USB- und einem CAT5-Kabel verbunden. Der maximale Abstand zwischen Triple 1und dem BS CONT GK Controller beträgt 5 Meter, kann aber durch zusätzliche Komponenten auf 25 Meter ausgedehnt werden.

Das Triple1 hat einen eingebauten Sabotage-Schutz. Im Falle eines Alarms wird das Terminal automatisch vom Controller getrennt, und damit gibt es keine Möglichkeit über das Terminal in den Controller einzudringen.

Die einzigartige Eigenschaft des Triple1 ist, dass man es in drei Varianten installieren kann: vollständig berührungslos, mit einer Fingerauflage oder mit einer kompletten Handauflage. Das Terminal kann Auf- oder Unterputz montiert werden.

www.biosecgroup.com
info@biosecgroup.com

Technische Spezifikation des Triple1

Größe des Triple 1:

Berührungslose Variante:	120*120* 44mm (H*B*T)
Triple1 mit Fingerauflage:	134*124*108mm (H*B*T)
Triple1 mit Handauflage:	162*126*124mm (H*B*T)

Haupteigenschaften:

Material	Polycarbonat
Farbe	Basismodul und Handauflage: schwarz Fingerauflage: weiß, kann optional in anderer Farbe geliefert werden
IP Schutzklasse	Indoor IP 41
Energieversorgung	über CAT5 und USB (max. 2 A) vom Controller aus
Lichtsignalisierung	RGB LED's auf beiden Seiten des Terminals
Audiosignalisierung	Buzzer
Zertifizierungen	CE & FCC
Sabotage Schutz	im Falles eines Alarms wird der Controller vom Terminal getrennt

Umgebungseigenschaften

Temperatur	0 - 60 °C
Luftfeuchtigkeit	10-90% relative nicht kondensierende Feuchtigkeit
Sonnenlicht	Direkte Sonnenbestrahlung soll vermieden werden, Sonnenabdeckung kann geliefert werden

BS100 Biometrisches Terminal

Das BS100 ist das biometrische Leserterminal, das für die 1:n Identifizierung geeignet ist. Es ist mit dem lokalen Controller (BS CONT GK) mit einem USB- und einem CAT5-Kabel verbunden. Der maximale Abstand zwischen Triple 1und dem BS CONT GK Controller beträgt 5 Meter, kann aber durch zusätzliche Komponenten auf 25 Meter ausgedehnt werden. BS100 ist sowohl für den Innen- als auch Außenbereich geeignet.

Das BS100 hat einen eingebauten Sabotage-Schutz. Im Falle eines Alarms wird das Terminal automatisch vom Controller getrennt und damit gibt es keine Möglichkeit über das Terminal in den Controller einzudringen.

Größe:

Breite	120 mm
Länge	189 mm
Tiefe	120 mm (ohne Wandmontage-Kit)

www.biosecgroup.com
info@biosecgroup.com

Haupteigenschaften:

Material	Polycarbonat
Farbe	Schwarz
IP Schutzklasse	Innenbereich IP 50, Außenbereich IP 65 (auf Anfrage).
Energieversorgung	über CAT5 und USB
Umgebung	Innenbereich oder Außenbereich
Temperatur	-20 - 60 °C
Luftfeuchtigkeit	10-90% relative nicht kondensierende Feuchtigkeit
Sonnenlicht	Direkte Sonnenbestrahlung soll vermieden werden, Sonnenabdeckung kann geliefert werden
Lichtsignalisierung	4 LEDs auf beiden Seiten des Terminals (blau, orange, rot, grün)
Audiosignalisierung	Buzzer
Heizung	Integrierte Heizung
Zertifizierungen	CE & FCC

Optionales Zubehör:

- Zubehör für eine Montage in Schräglage an einer senkrechten Wand
- Externer RFID Leser für eine 1:1 Identifizierung kombiniert mit der biometrischen Erfassung
- Sabotage Schutz: im Falles eines Alarms wird der Controller vom Terminal getrennt
- Sonnenabdeckung

RFID Leser für Triple 1 (optional)

Der RFID Leser Architect® One vereint ultra-kompaktes Design mit einer sicheren Benutzer-Identifizierung. Der Leser nutzt die neueste MIFARE® kontaktlose Chip Technologie (MIFARE Ultralight® & Ultralight® C, MIFARE® Classic & Classic EV1, MIFARE Plus®, DESFire® EV1 & EV2, NFC (HCE), ®) mit neuen Datensicherheitsmechanismen, die empfohlene und öffentlich anerkannte Verschlüsselungsalgorithmen verwenden. Dies erlaubt die sichere EAL5+ Datenspeicherung (ARC1S Version). Der Manipulationschutz schützt sensitive Daten und bietet die Möglichkeit die Authentifizierungsschlüssel zu löschen (zum Patent angemeldet).

Technische Spezifikation des RFID Lesers:

Betriebsfrequenz/ Standards	13.56 MHz, ISO14443 Type A & B, ISO18092 (NFC)
Unterstützte Chips	MIFARE Ultralight® & MIFARE Ultralight® C, MIFARE® Classic & Classic EV1, MIFARE Plus®, MIFARE®, DESFire®, MIFARE® DESFire® EV1 & EV2, NFC (HCE),
Lesereichweite	Bis zu 6 cm bei einer MIFARE® Classic Karte Bis zu 4 cm bei einer MIFARE Plus®/DESFire® EV1 karte
Schnittstellen	ISO2 Protokol (Data Clock), Wiegand (Verschlüsselter Mode S31), RS485 (Verschlüsselter Mode S33)

www.biosecgroup.com
info@biosecgroup.com

Anschlüsse	2 Versionen: A – 3 m festes Kabel B – 3 m steckbares Kabel
Lichtsignalisierung	2 RGB LEDs - 360 Farben
Audiosignalisierung	Interner Lautsprecher
Leistungsaufnahme	Typisch 120 mA/12 V Gleichspannung
Spannungs-versorgung	10 V bis 15V Gleichspannung
Material	ABS-PC UL94-V0 (Schwarz)
Abmessung (h x l x b)	110 x 42 x 22 mm
Betriebstemperatur	- 20°C bis + 70°C / Rel. Luftfeuchtigkeit: 0 - 95%
Manipulations-erkennung	Beschleunigungs-basierte Manipulationserkennung mit Löschen des Schlüssels
Schutzklasse	IP65 (mit Ausnahme der Anschlüsse) / verstärkte Vandalismus resistente Stoßfestigkeit IK10
Zertifizierungen	CE & FCC

BS CONT GK lokaler Controller

Der Controller steuert maximal zwei biometrische Leser und/oder vier RFID Leser. Der Controller beinhaltet einen Industrie-PC konzipiert für 24 Stunden Betrieb und ein I/O Modul für die Steuerung von zwei Zutrittspunkten. Der BS CONT GK ist die Verbindungsstation zwischen dem BS 100/Triple 1 und der IDENGINE Software, die auf dem zentralen Server installiert ist.

Die lokalen Controller kommunizieren mit den Servern über eine verschlüsselte TCP/IP Verbindung (zertifikatsbasierte Verschlüsselung). Es wird mindestens ein CAT5 Kabel benötigt. Die Zutrittskontrolle funktioniert auch im Offline-Modus, d.h. wenn die Verbindung zum Server aus irgendwelchen Gründen unterbrochen ist. In diesem Fall wird der Identifizierungsprozess vom lokalen Controller übernommen.

Technische Spezifikation des BS CONT GK

Größe:

Breite	320 mm
Länge	380 mm
Höhe	71 mm

Haupteigenschaften:

Material	Metall
Farbe	Weiß
Spannungsversorgung	~230 V/ 50 Hz oder ~115V / 60 Hz
Leistungsaufnahme	12V, 3A

www.biosecgroup.com
info@biosecgroup.com

Sabotage Schutz	ja
Anzahl der Templates, die auf dem Controller gespeichert werden	Bis zu 5.000.000 für 1:1 Verifizierung, 5.000.000 Templates für 1:n Identifizierung (beides kann erweitert werden)
I/O Module	6 Ausgänge, 2 USB Eingänge und Ausgänge, 12 Eingänge
Offline Modus	ja
Dauer für Online Authentifizierung (1:n oder 1:1)	~1 Sekunde (für den Fall 1:n, falls der definierte Server zur Verfügung steht)
Dauer für Online Verifizierung	~1 Sekunde
Dauer für Online Identifizierung	Hängt von der Anzahl der Benutzer in der Datenbank ab
Dauer für Online/Offline Verifizierung nur mir RFID karte	~ 1 Sekunde bei einer unbegrenzten Anzahl von Nutzern
Synchronisierung zum Server	Echtzeit
Anzahl von Log-Einträgen, die im Offline Modus gespeichert werden können	500 000
Statusmeldung des Türsensors	Ja
Ladefunktion für Batterie zur Überbrückung von Stromausfall	Ja (Batterie optional)

IDENGINE, die BioSec Server-Software

Die Identifizierungs-Software IDENGINE läuft auf einem Authentifizierungsserver und führt die Identifizierung von Personen durch, enthält Logs, synchronisiert alle Controller, verwaltet persönliche Daten.

Der Authentifizierungsserver kann redundant ausgeführt werden. Die redundante Serverinfrastruktur wird als Master/Slave-Server-Kombination erstellt. Bei dem Ausfall eines Master-Servers übernimmt dann der Slave automatisch die Rolle des Masters.

Technische Spezifikation der Software IDENGINE

Haupteigenschaften:

Datenbank	MySQL, MS SQL, Oracle oder PostgreSQL (Kunde kann wählen)
Betriebssystem	Lauffähig unter Microsoft Server 2008 oder höher, 64 bit
Server Konfiguration für 1:1 Authentifizierung	Bis zu 1 Million Nutzer, Minimal-Anforderungen: Intel E3-1231v3 CPU, 8GB 1600MHz ECC RAM, 250GB SATA HDD
Redundanz	Master/Slave Kombination, automatisches Failover

www.biosecgroup.com
info@biosecgroup.com

AdminSuite

Die Registrierung der Benutzer und die Aufnahme der Handvenen (Enrollment) erfolgt auf einem oder mehreren Management/Registrierungs-PCs mit einem installiertem BS Guide Leser. Auf dem PC läuft die Systemverwaltungssoftware AdminSuite. Diese ist direkt mit dem Authentifizierungsserver gekoppelt. Die erfassten Templates der Handvenen werden ausschließlich auf dem Authentifizierungsserver gespeichert und nicht auf dem Registrierungs-PC. Deshalb wird eine direkte Online-Verbindung zu der Server-Software IDENGINE benötigt.
Die AdminSuite kann auf so vielen Arbeitsstationen installiert werden, wie lizenziert sind.

Anforderungen an den PC

PC-Ausstattung	Aktueller PC mit mind. 4 GB Arbeitsspeicher, ansonsten keine besonderen Anforderungen
USB 2.0	Freie USB-Schnittstelle zum Anschluss des BS Guide
Betriebssystem	Microsoft Windows 7 oder neuer, 64 bit

www.biosecgroup.com
info@biosecgroup.com

IV. Allgemeine Eigenschaften

Allgemeine Informationen

Anzahl der unterstützen Türen	unbegrenzt
Anzahl der Registrierungsstellen (Adminsuite)	unbegrenzt
Offline Modus	Ja (Zutrittskontrolle auch möglich, wenn Verbindung zum Server unterbrochen)
Biometrische Authentifizierungs Methode	Handvenen-Erkennung
Zusätzliche RFID Karte	Ja (Karte vor oder nach Handvenen-Erkennung möglich)
Innenbereich / Außenbereich	Ja / Ja

Remote Verbindungsfunktionen

- Schließen und Öffnen einzelner Zutrittspunkte oder kompletter Zone(n) aus der Ferne, falls diese Funktion eingeschaltet ist
- Verwerfen von Alarmen für einzelne Zutrittspunkte oder komplette Zone(n) aus der Ferne
- Bestätigen und Löschen von Systemalarmen von der Ferne
- Support für GateKeeper Lösung aus der Ferne ist möglich
- Soft- oder Hard-Neustart einzelner oder mehrerer Controller aus der Ferne

Konfiguration der Zutrittspunkte

- Multi-User-Modus (eine zweite Person muss die Authentifizierung einer Person am selben oder einem separaten Terminal genehmigen)
- Wartungsmodus (Sabotage-Sensoren ausschalten)
- Aktivieren / Deaktivieren der Zutrittspunkte
- Anti Passback Regeln
- Systemdiagnose für jedes Hardware- und Softwareelement (Status)
- Automatische Erkennung des BioSec-Zutrittspunkts (es muss kein neuer Zutrittspunkt hinzugefügt werden, und nur der BioSec-Controller kann Kontakt zum BioSec-Server aufnehmen)
- Dedizierte Hardware
- Konfiguration der Hardware für Input/Output
- Sabotage Schutz (Deaktivieren der Zutrittspunkte, an denen ein Sabotage-Alarm aufgetreten ist)
- Konfiguration des Verhaltens bei Feueralarm.
- Einstellen der Zeiten für die Relais der elektrischen Schlösser
- Konfiguration der Reaktion auf unautorisiertes Öffnen der Türen
- Einstellen der Reaktion auf offen gelassene Türen
- Zusammenschließen von Zutrittspunkten zu Sicherheitszonen

www.biosecgroup.com
info@biosecgroup.com

- Diagnose der Zutrittspunkte
- Systemdiagnose in Echtzeit, bei der das Funktionieren aller Hardware- und Software-Komponenten angezeigt wird.
- Aufzugssteuerung

Benutzer Konfiguration

- Hinzufügen, Ändern und Löschen von Nutzern
- Aktivieren, Deaktivieren von Nutzern
- Biometrische Registrierung
- Eingabe PIN Code und/oder RFID ID Karte /Nutzer ID
- Einstellen der Gültigkeit für Nutzerrechte (ss.mm.dd.mm.yyyy) oder für einen vordefinierten Zeitraum (24h, heute bis Mitternacht, eine Woche). Die Zeiträume können auch geändert werden.
- Auswahl der Rolle im System (Besucher, Angestellter, Administrator, Super Administrator etc.)
- Auswahl von Regeln für den Zutrittspunkt: Zutritt bei erfolgreicher Authentifizierung verweigern, Zutritt erlauben oder Authentifizierung ohne zu öffnen (Kontrollpunkt für Sicherheitspersonal)
- Einstellen des Zeitraumes für Regeln des Zutrittspunktes mit Start- und Ende-Zeit (ss.mm.dd.mm.yyyy)
- Konfiguration der Möglichkeit individueller Zugriffsrechte für jeden Zutrittspunkt, Reduzieren oder Erweitern von Rechten für Nutzergruppen.

Verwalten von Sicherheitszone(n)

- Erstellen, Ändern und Löschen von Sicherheitszonen
- Hinzufügen von Zutrittspunkten zu Sicherheitszonen
- Aktivieren und Deaktivieren von Sicherheitszonen mit einem Klick

Konfiguration von Nutzergruppen

- Hinzufügen, Ändern und Löschen von Nutzergruppen
- Aktivieren und Deaktivieren von Nutzergruppen
- Auswahl von Regeln für den Zutrittspunkt: Zutritt bei erfolgreicher Authentifizierung verweigern, Zutritt erlauben oder Authentifizierung ohne zu öffnen (Kontrollpunkt für Sicherheitspersonal)
- Einstellen des Zeitraumes für Regeln des Zutrittspunktes mit Start- und Ende-Zeit (ss.mm.dd.mm.yyyy)
- Konfiguration von individuellen Sicherheitszonen-Rechten für Nutzergruppen

Berichte

- Möglichkeit zum Speichern / Laden von Berichten
- Möglichkeit, Berichte ins Archiv zu stellen
- Tägliche Berichte, Anwesenheitsliste, Gästelisten, Liste der Mitarbeiter, Ereignisliste
- Individuelle Berichte können erstellt werden
- Geplantes System Setup
- Exportieren der Berichte / Log-Dateien in xls- oder csv-Format

www.biosecgroup.com
info@biosecgroup.com

Verwalten des Zutritt-Prozesses

- Globale / Sicherheitszone / auf Zutrittspunkt bezogene Zutrittsrate
- Überwachung der Anwesenheit von Personen innerhalb der Sicherheitszone
- Prozentsatz der Personen innerhalb der Sicherheitszone bezogen auf die maximal zulässige bzw. die geplante Personenanzahl
- Etagenpläne in Echtzeit

Zusätzliche Eigenschaften

- Ereignis- oder zustandsbezogene Benachrichtigung
- Nationale Kalender
- Blacklist (Verbotsliste)
- Einfache Besucherverwaltung
- Lokalisierung von Personen
- Im-Büro-Liste
- Verwalten von Eintrittskarten
- Öffnen und Schließen von Zutrittsstellen und Zonen für den Notfall aus der Ferne
- Warnung bei einer Zutrittsrate außerhalb der Toleranz
- Alarmbehandlung bei Sabotage / Brand / Evakuierung (um Fehlalarme zu behandeln)

www.biosecgroup.com
info@biosecgroup.com

V. Weitere technische Information

3rd Party System-Integration
BS GateKeeper kann in jede Art von Drittanbieterlösung wie Feueralarm-, Gebäude-Managementsystem integriert werden.

Installation
BS GateKeeper ist ein hoch performantes, benutzerfreundliches System. Es kann sehr einfach installiert und in bestehende Infrastrukturen integriert werden. Sowohl Installation als auch Integration sollten nur durch qualifiziertes Fachpersonal durchgeführt werden.

Die Topologie basiert auf TCP/IP, wobei der Controller jedes Zutrittspunkts über Ethernet mit dem Server kommuniziert.

Die Software- und Hardware-Umgebung besteht aus folgenden Komponenten:
- mindestens einem IDENGINE-Authentifizierungsserver
- "n" Zutrittspunkten ausgestattet mit BS 100/Triple 1 Terminals und BS CONT GK Controllern (optional mit RFID Lesern)
- mindestens einer zentralen Management-Workstation mit BS Guide (für Registrierung, Systemmanagement)

Netzwerkkonfiguration
Folgende Anforderungen werden an das Netzwerk gestellt:

Ein getrenntes Netzwerk ist zwingend erforderlich.
- Sämtliche Controller, die Management-Workstation und der Server müssen sich im gleichen Netzwerk befinden
- Der UDP-Port 123 muss im Netzwerk aktiviert sein
- Der TCP-Port 5555 muss für eingehenden Datenverkehr vom Server aktiviert sein
- Broadcasting sollte auf allen Netzwerkgeräten aktiviert sein (UDP 11000)

Weitere Anforderungen
Für die unterbrechungsfreie Stromversorgung ist zu sorgen. Der Controller kann optional mit einer Pufferbatterie mit 7Ah optional ausgestattet werden.