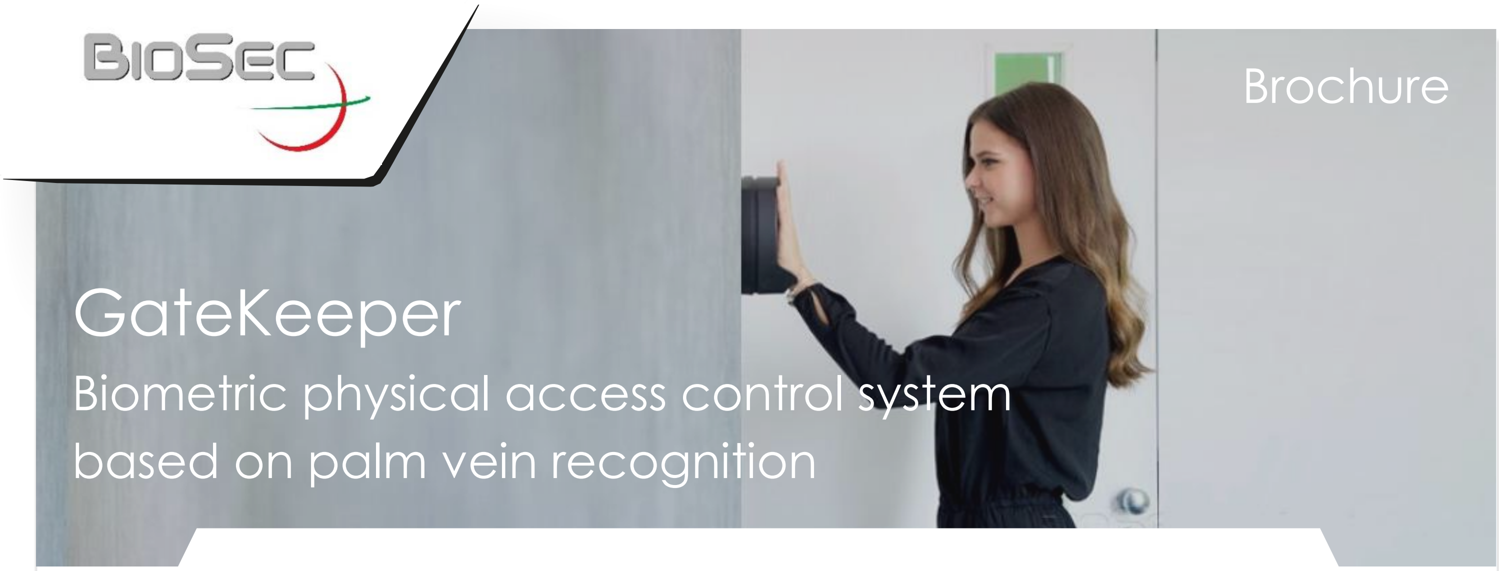
BioSec



Brochure

GateKeeper

Biometric physical access control system based on palm vein recognition

Content

Highest security level

Ease of use

Convenience

www.biosecgroup.com

info@biosecgroup.com

General information

The **GateKeeper** physical access control system is a modular, flexible system, which does not contain any complicated network structure. There are almost no limitations in the number of users, or the size of the system (for detailed information please contact us).

GateKeeper physical access control system has the following benefits:

- Highest security in identification
- The ID cannot be lost, copied or reproduced, since it is an inner biometric ID
- Compatible with most regular and standard systems, easy to integrate
- The person needs to be registered in one system only once in a lifetime
- Large network systems can be also created
- Common Criteria Certificate
- 256-bit encryption, also encrypted data flow
- Active Directory compatible
- High security, FAR 0,00008%, FRR 0,01%
- Can be fully integrated into all Biosec solutions, any 3rd party solutions as well via software, serial or Wiegand interface
- Can be combined optionally with RFID cards (Mifare)

The **GateKeeper** physical access control system is using the LifePass palm vein based biometric identification system for safe and fast security. The complete access control system consists of following elements:

Hardware

- Triple1/Triple1+/ TimeKeeper biometric reader terminal
- PS Guide (registration desk terminal)
- Rector controller (access point control device)
- Server and passive/active network devices
- Optionally the system can be equipped with Mifare RFID readers

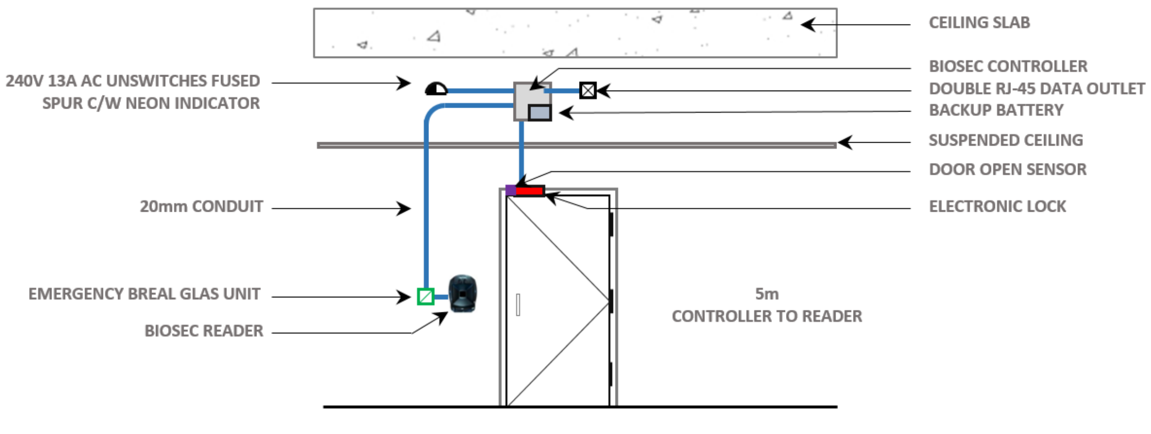
Software

- Client SW (client software for each biometric reader terminal or RFID reader)
- Server software package (central server software for system administration)
- AdminSuite (system/user management, registration graphical user interface)

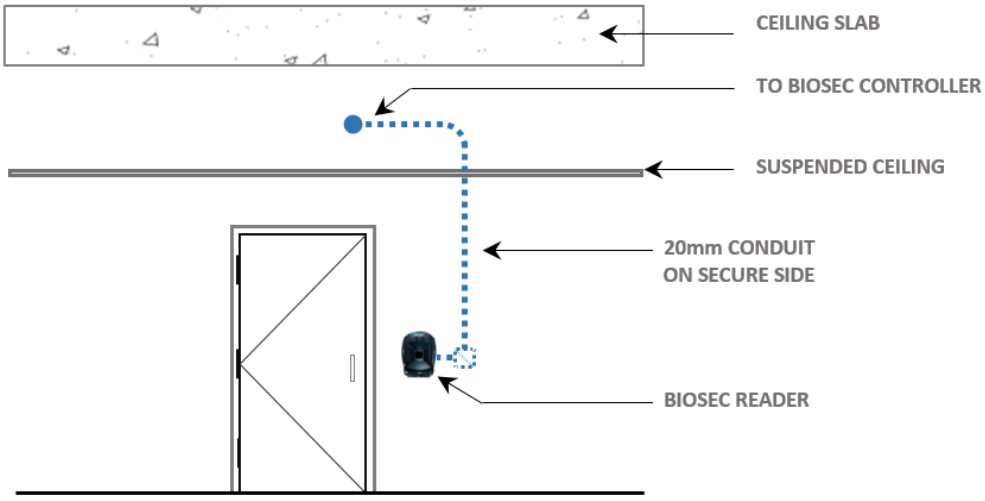
The **Triple 1/Triple1+/TimeKeeper** is the only device installed outside of the unsecured area. It is connected to the local controller, via one USB and one CAT5 cable. The maximum distance between the biometric reader and the controller is 5 meters but can be extended to 25 meters.

The biometric reader does not contain any panels, which would make it possible to manage/sabotage the access point via biometric reader.

DOOR EQUIPMENT LAYOUTS (LOCAL CONTROLLER)



SECURE SIDE



NON-SECURE SIDE

Industry standard components can be connected to the controller as peripheries such as magnetic locks, push-to-release buttons, distress buttons, etc.

Features & Functionality

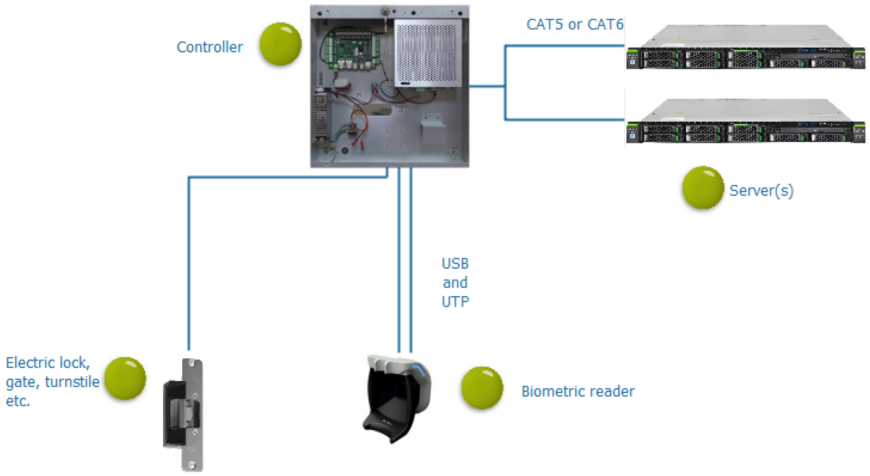
Main features

- Online, offline functioning
- Unlimited number of doors /depends on the license/
- Unlimited number of users /depends on the license/
- 1:1 or 1:n authentication
- Anti-passback
- Sabotage protection, encrypted communication
- ~1 second biometric authentication time

Security features

All components of GateKeeper are protected by latest security mechanisms. GateKeeper uses a three-level encryption (biometric template, communication, database). BioSec software do not use passwords, the software can be accessed only via palm vein recognition. The optional RFID reader used latest Mifare technology (please contact us for further information).

Basic system architecture



Technical Parameters

- Used OP system at controller: Windows 10 IOT 64 bit
- OP system for server: Microsoft Server 2012 or higher
- OP system for AdminSuite: Windows 8 or higher, 64 bit
- Database: MSSQL, PostgreSQL
- Active Directory: complete compatibility
- Stand alone: the system can work also offline
- Necessary hardware: biometric reader, controller, server, PS Guide
- Dedicated router

Possible devices for use

Access control devices for indoor environments

Triple 1 – modular biometric terminal

Triple 1+ - modular biometric terminal with RFID reader

Time and attendance device

TimeKeeper – modular biometric terminal with RFID reader and touchscreen

System components

Triple1 Biometric Terminal

The Triple1 is the biometric reader terminal specialized on 1:n identification. It is connected to the local controller via one USB and one CAT5 wire. The maximum distance between the Triple1 and the controller is 5 meters but can be extended to 25 meters.

The Triple1 has a built-in sabotage protection. In case of an alarm, the terminal will be cut of automatically from the controller and there is no possibility to get into the controller via the terminal after that.

The unique feature of the Triple1 is that it can be installed in three versions: contactless, with finger rest or complete hand rest. The terminal can be surface mounted or sunk into the wall.

Technical specifications of the Triple1

Size of the Triple1:

Contactless version:	120*120*44mm (H*W*D)
Triple1 with finger rest:	134*124*108mm (H*W*D)
Triple1 with hand rest:	162*126*124mm (H*W*D)

Main characteristics:

Material	polycarbonate
Colour	contactless module and hand rest is black, finger rest is light grey but can be modified optionally
IP	Indoor IP 41
Power supply	via CAT5 and USB (max. 0,5 A)

Environment

Temperature	0 - 60 degrees
Density	10-90% relative non-condensing humidity
Sunlight	direct sunlight to be avoided, sun cover can be provided
Light indicator	RGB LED's on both side of the terminal
Audio indicator	internal buzzer
Sabotage protection, in case of signal, the controller cuts of the terminal	

Triple1+ Biometric Terminal with RFID Reader

The Triple1+ is a biometric access control device, which was specially developed for indoor environments. The Triple1+ includes the Triple1 biometric terminal and an RFID reader in one housing. By using palm vein recognition based biometric authentication, the highest security level can be provided, while the RFID reader enables further authentication options based on the client's requests.

Technical specifications of the Triple1+

Biometric terminal of the Triple1+

The Triple1 terminal's features apply to the biometric terminal of the Triple1+.

Technical specifications of the RFID reader:

Operating frequency/ Standards	13.56 MHz. ISO14443 types A & B, ISO18092 (NFC)
Chip compatibility	MIFARE® Classic & Classic EV1, MIFARE Plus®, MIFARE®, DESFire®, MIFARE® DESFire® EV1 & EV2, NFC (HCE)
Functions	PH1: MIFARE® Classic secure sector read only and CSN read only of other chips PC1: pre-configured read only PH5: secure read only (file, sector) and secure protocol (Secure Plus), read/write (SSCP & SSCP2)
Reading distances	Up to 6 cm with a MIFARE® Classic card Up to 4 cm with a MIFARE Plus®/DESFire® EV1 card
Audio indicator	Internal buzzer
Power requirement	Typical 150 mA/12 VDC
Operating temperatures	- 20°C to + 70°C / Humidity: 0 - 95%
Tamper switch	Accelerometer-based tamper detection
Certifications	CE & FCC

TimeKeeper Biometric Time and Attendance Terminal

The TimeKeeper is a biometric time and attendance device for accurate employee attendance tracking. The TimeKeeper includes the Triple1 terminal, an RFID reader and a 5-inch touchscreen for seamless clocking in and out. By using palm vein recognition based biometric authentication, employee monitoring becomes accurate, while identity abuses and buddy punching can be eliminated with the greatest certainty. Combined with an RFID reader, TimeKeeper enables 1:n and 1:1 authentication options based on the client's requests. In addition, the 5-inch touchscreen supports ease of use and convenience.

Technical specifications of the TimeKeeper

Biometric terminal of the TimeKeeper

The Triple1 terminal's features apply to the biometric terminal of the TimeKeeper.

Technical specifications of the RFID reader:

The same features apply to the RFID reader as in case of the Triple1+ terminal's RFID reader.

Technical specifications of the touchscreen:

Power	5V Power via USB Micro
Current	Max 400mA
Display Type	5 inch TFT LCD
Resolution	800x480
Touchscreen	USB capacitive
Touch points	10 points maximum
Interface	HDMI & USB 3.1 Full Speed
Dimensions	133mm x 79mm x 13mm
Weight without package	130g

PS Guide Biometric Registration Device

The PS Guide is a biometric reader terminal, specialized in user enrolment processes. The intuitive design allows users to optimally position their hands for scanning. PS Guide is perfect for high traffic locations, since it has been designed for years of daily contact by hundreds of users and it is easy to install and maintain.

Technical specifications of the PS Guide

Size of the PS Guide:

Width	140 mm
Length	170 mm
Depth	110 mm
Weight	251 g

Main characteristics:

Material	Polycarbonate
Color	Black
IP	Indoor IP 50
Power supply	Via USB
Environment	Indoor
Temperature	-20 - 60 degrees
Density	10-90% relative density
Sunlight	Direct sunlight to be avoided

Rector Controller

The controller unit manages two biometric readers and/or four RFID readers. The controller contains one industrial PC designed for 0-24 operation and one I/O module for management of two access points. The Rector is the link between the biometric reader and the server software installed onto the central server.

The local controllers are communicating with the servers via encrypted and certified TCP/IP protocol and minimum CAT5 network. The system can function in offline modus, when the connection to the server is interrupted for any reason. In this case, the identification process will be taken over by the local micro PC in the controller.

Technical specifications of the Rector

Size of the Rector:

Width	375 mm
Length	385 mm
Depth	110 mm

Main characteristics:

Material	metal
Color	white
Power supply	~230 V/ 50 Hz or ~115V / 60 Hz
Power consumption	12V, 3A (UPS can be provided)
Sensors	sabotage, door opening, fire detection
Number of templates to be stored on controller	up to 5 000 000 for 1:1 verification, 5 000 000 templates for 1:n identification (both can be extended)
I/O module	8 output ports, 2 USB input and output ports, 6 input ports, 6 relays
Offline modus	yes
Online authentication time (1:n or 1:1)	~1 second (in case of 1:n, if the defined server is provided)
Offline verification time	~1 second
Offline identification time	depending on number of users in database
Online/offline verification time for RFID only	~ 1 second with unlimited number of users
Synchronization to server	real time
Number of stored logs	500 000 (default setup, can be increased)

Server Software

Our server software on the server carries out personal identification, contains logs, synchronizes all controllers, manages personal data which server can be redundant.

The redundant server infrastructure is created as master/slave server combination. In case of server failure, the other server takes over the central role of the system automatically.

The system management software, the AdminSuite is connected directly to the server software. The AdminSuite can be installed onto as many workstations as licensed in the system but no sensitive data is stored in the software, direct online connection is needed to the server software.

Technical specifications of the server software

Main characteristics:

Database	MySQL, MsSQL, Oracle or PostgreSQL (client can choose)
Operation system	Microsoft Server 2012 or higher, 64 bit
Server configuration for 1:1 authentication	Up to 1 million users, minimum requirement: Intel E3-1231v3 CPU, 8GB 1600MHz ECC RAM, 250GB SATA HDD free space
Redundancy	Master/slave combination, automatic failover
Hardware key	Yes

General GateKeeper features

General information

Number of doors supported	unlimited
Number of User interfaces	unlimited
Offline mode	yes
Biometric authentication method	palm vein recognition
Primary or secondary RFID	yes
Indoor/outdoor	yes/yes

Remote connection functions

- Remotely lock, unlock single access points or complete zone(s), only if enabled function
- Remotely overrule alarms for a single access point or complete zone(s)
- Remotely acknowledge and clear system alarms
- Remote support for GateKeeper system possible
- Remote soft or hard restart of individual or multiple controllers

Configuration of access point

- Multi user mode (a second person has to approve the authentication of a person on the same or a separate terminal)
- Maintenance mode (turning off sabotage sensors)
- Enabling/disabling access point
- Anti-passback rules
- System diagnosis for every hardware and software element (status)
- Automatic BioSec access point recognition (no need to add new access point and only BioSec controller can get contact to BioSec server)
- Dedicated hardware
- Configuration of Input/Output hardware
- Sabotage protection (disabling access point, where sabotage alarm was raised)
- Configuring fire alarm handling
- Setting up time for electric lock relay
- Configuration of reaction of unauthorized door opening
- Setting response for open left door
- Connecting access points to security zones
- Access point diagnostics
- Real time system diagnosis, where the functioning of all hardware and software components can be seen
- Elevator control

User configuration

- Adding, modify, delete functions
- Enable, disable user
- Biometric enrollment
- Entering PIN code and/or RFID unique card ID/user ID
- Setting user right validity (ss.mm.dd.mm.yyyy) or predefined period of time (24h, until midnight, one week, which can be changed)
- Setting system role (visitor, employee, daily registrator, administrator, integrator etc.)
- Choosing access point rule: deny access in case of successful authentication, allow access or authenticate without opening (security guard checkpoint)
- Setting time period for access point rule (starting, ending time: ss.mm.dd.mm.yyyy)
- Configuring possibility individual access rights for every access point, reducing or increasing user group rights

Managing security zone(s)

- Creating, modifying, deleting security zone
- Adding access points to security zones
- Enabling and disabling security zone by one click

Configuring user groups

- Adding, editing, deleting user groups
- Enable, disable user group
- Choosing access point rule: deny access in case of successful authentication, allow access or authenticate without opening (security guard checkpoint)
- Setting time period for access point rule (starting, ending time: ss.mm.dd.mm.yyyy)
- Configuring individual security zone access rights for user group

Reports

- Ability to Save reports
- Ability to put reports into archive
- Daily reports, Attendance register, Guest lists, List of employees, Event list
- Individual reports can be created
- Scheduled system setup
- Exporting reports/logs in xls or csv format

Access procedure management

- Global / security zone / access point related flow rate
- Supervision of presence of people within security zone
- Percentage of people inside the security zone in relation with maximum capacity or how many should be in the security zone
- Floor based map with real time system management

Additional technical information

3rd Party Systems Integration

GateKeeper can be integrated into any kind of third party solution such as fire alarm, building management system via API. For further information please contact us.

Deployment

GateKeeper is very easy to install to any kind of infrastructure. The topology based on TCP/IP where each access point's controller communicates with server via Ethernet.

The software and hardware environment consists of following components after the proper installation by integrators:

- one server software at least – authentication server
- "n" number of access points equipped with biometric terminals and controllers (optionally with RFID readers)
- minimum one central management workstation (for enrollment, system management)

Necessary system configuration:

- all controllers must be a same subnetwork with the server in case multicasting is not enabled
- the UDP 123 port must be enabled on the network
- the TCP 5555 must be enabled for inbound traffic from the server
- broadcasting/multicasting should be enabled at any network devices
- dedicated router
- Additional ports to be opened: 5554 LifePass, 5432 Database, 11000 UDP, 15001 SCM, 15553 Mulicast, 23500/22325 WIBU, 14476/13579 Deployment

Acceptance test

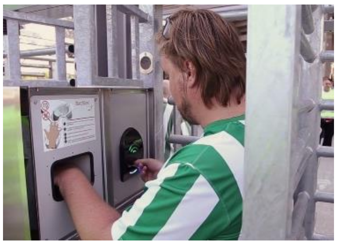
The quality of our product is one of the most important part to us, therefore we developed our own factory acceptance test which we always proceed before sending out any hardware or software.
The milestones of the test procedure are the following:

- Installation of the Controller (Windows OS)
- Regular test of the MicroPC including SSD
- Installation of the dedicated BioSec application components
- Detailed function test for IO module
- Functional test of the controller

More information

Besides GateKeeper, the BioSec product portfolio contains the following solutions:
For further information please visit www.biosecgroup.com

LifePass
Biometric authentication middleware



StadiumGuard
Stadium security- and services solution package

BLogin
Biometric Windows log in system

CityGuard
Integrated access management

RapidGuard
Rapid deployment biometric authentication

Contact:

1119 Budapest, Boglárka Street 32.,
HUNGARY
☎ + 36 1 248 2100
+ 36 1 248 2105
@ info@biosecgroup.com
www.biosecgroup.com

BioSec Group Ltd. is a dedicated developer of innovative security solutions based on palm vein recognition. BioSec is specialized in biometric mass authentication, logical- and physical access control solutions, ensuring highly secure, simple to use and convenient solutions in every fields of life.