

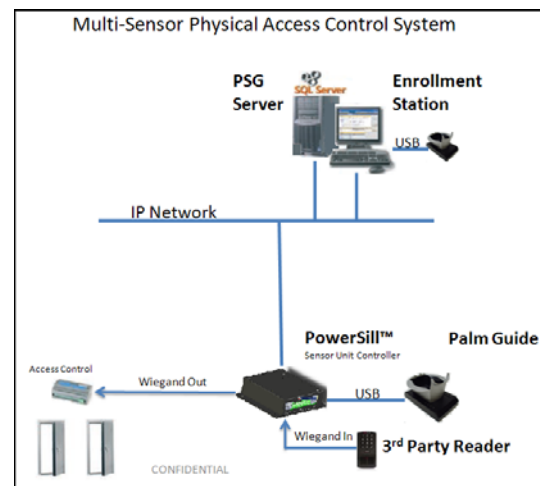
## Multi-Sensor Physical Access Control System (MPACS™)

Physical access control is an important issue in today's security conscious world. An entrance control system must be designed with state of the art security systems. The goal is to bring together modern entrance equipment with advanced electronic and biometric credential based controls, administered by an integrated software application that manages access to a large database of users. A multi-platform system that offers multiple layers of access control options integrated into one unit provides a technical edge in the current competitive security market. A multi-platform access control system needs to support all the standard access control methods and should be able to easily adapt to future security technology.

The **Multi-Sensor Physical Access Control System (MPACS™)** is an elegant solution that operates with any type of security sensor from biometric to electronic access, and can be fitted into any modern automated access control entry point (doors, turnstiles, parking gates, or other barriers). Based on the powerful **PowerSill™ Sensor Unit Controller**, the **MPACS™** system can interface with many different sensor technologies. With its advanced architecture, the **PowerSill™** controls and manages biometric sensors and electronic access devices such as:

- Palm Vein Reader
- Fingerprint Reader
- Face Recognition
- Proximity Sensor
- Smart Card
- ID Card
- Keypad Reader

The biometric and electronic sensors can be attached to the **PowerSill™ Sensor Unit Controller** locally or remote over the IP Network. The **PowerSill™** processes the information from the sensor and responds by issuing commands to an access control unit or relay controller to grant access to authorized persons.



As shown in the block diagram, the **PowerSill™ Sensor Unit Controller** is the heart of the system. An **Enrollment Station** is located at a remote location. A user is enrolled at the systems Enrollment station and the identity information is encrypted and stored in the database along with the user name and ID. A user entering an access point submits his credentials at the biometric or electronic access sensor. The system performs high speed, 1:N matching or 1:1 matching to identity the user. A relay controller is then activated to automatically open the access point. The system performs identification and matching exceptionally well and offers low false accept and false reject rates.



BioGuard Components & Technologies Ltd.

4, HaCharash st.  
Hod-HaSharon  
Israel, 45240

Tel: +972-9-7695200  
Fax: +972-9-7417770  
www.bio-guard.net

Mall: P.O.B. 7341  
Hod-HaSharon Israel, 45240  
Email: info@bio-guard.net

The management features of the **MPACS™** system can be tailored to the specific needs of the business. The database management software varies in complexity based on the levels of security required. The administrator or manager of the security system designates when a person is cleared for access and to which access point. The administrator can enroll and add new users, delete users, and manage the user templates. Different levels of security clearance and privileges can be assigned to each user.

The **PowerSill™** devices are connected to the Local Area Network so that the administrator can view the IP Address, unit ID and status of each device on the network. By connecting to a specific IP Address, the administrator can list all the users on that specific sensor, add or delete users, add privileges to a user, and add a user from the local database to that specific device.

## Summary of Physical Access Control Systems

Physical access control systems include the biometric sensors and the electronic access controls. Standard technology encompasses the electronic key management and can include smart card, proximity sensors, password controls, and access badges. Biometric technology features fingerprint, palm vein, and face recognition.

## Biometric Technologies

**Fingerprint** technology is one of the most secure and foolproof methods for a credential based authentication approach to access control. This simple biometric solution facilitates a dependable access

control system to increase security in both the home and office. Fingerprint technology has been around for a long time and is a sophisticated and verified form of identification. It has been used in criminal investigations for almost a hundred years. In fact, a fingerprint is so unique that it remains unchanged throughout a person's lifetime. It is a human being's built in identity card. Combining fingerprint identification with modern scanning technology, a simple cost effective access control solution is created. A fingerprint scanner captures the unique fingerprint pattern and stores it on a database. The stored fingerprints serve as the basis for various levels of access control software to meet the requirements of a private user or business.

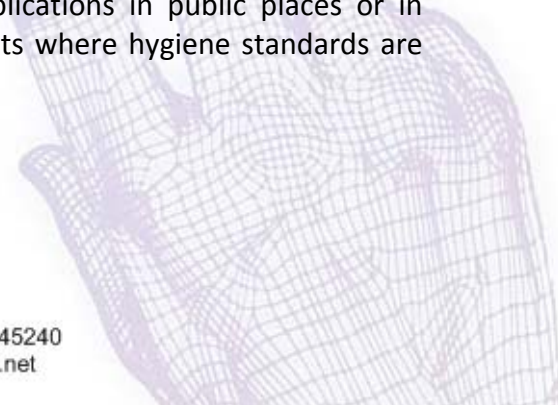
**Palm vein** pattern recognition technology is an advanced biometric authentication system that verifies an individual's identity based on the unique pattern of veins in the palm. Palm vein scanning technology is highly secure, because the veins are deep within the hand, and are arranged in very complicated patterns which are virtually impossible to reproduce. Palm vein terminals utilize "no touch" technology that is not sensitive to skin condition, finger pressure, and dirt, resulting in superior performance levels. Palm vein technology uses the vascular patterns of an individual's palm that contains many differentiating features for personal identification. The contactless identification system is able to capture the palm image regardless of the position and movement of the palm and enables applications in public places or in environments where hygiene standards are required.

## BioGuard Components & Technologies Ltd.

4, HaCharash st.  
Hod-HaSharon  
Israel, 45240

Tel: +972-9-7695200  
Fax: +972-9-7417770  
www.bio-guard.net

Mall: P.O.B. 7341  
Hod-HaSharon Israel, 45240  
Email: info@bio-guard.net



**Face recognition** is a highly complex technology that captures characteristics of a face either from video or image and translates unique characteristics of a face into a set of numbers.

## Electronic Access Control

Many other electronic access control systems can be incorporated into the system including card based, video based, and keypad based. Keypads are the simplest form of electronic access control. Another traditional method of authentication is a card based access control system using proximity cards, smart cards, and smart badges. An example of a card based system is a proximity sensor which detects the presence of nearby objects such as an ID card to trigger a signal which the system can authenticate and react to. All these options can be added to the system to provide users with a higher level of security.

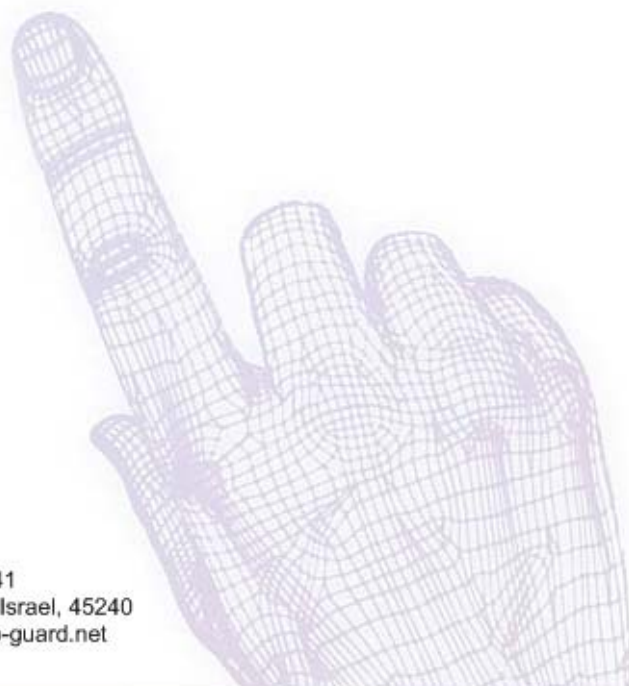
## Summary

A multi-platform access control and management system is needed to meet the demands of today's security threats. The **MPACS™** system is flexible and can interface with a large number of sources

such as biometrics, keypads, proximity sensors, and others, and offers a centralized database management site controller system. The **MPACS™** system contains all the advanced elements for controlling access to your site.

## System Highlights

- Reliable biometric technology
- Enrollment Station
- Power Sill™ Embedded Platform
- Electronic access control
- Multi-level security
- Supports multiple biometric inputs
- Intuitive management application
  - Enroll
  - Delete
  - Identify
- Remote management
- Encrypted Templates



## BioGuard Components & Technologies Ltd.

4, HaCharash st.  
Hod-HaSharon  
Israel, 45240

Tel: +972-9-7695200  
Fax: +972-9-7417770  
www.bio-guard.net

Mall: P.O.B. 7341  
Hod-HaSharon Israel, 45240  
Email: info@bio-guard.net



## Application of MPACS™

### Governmental Application

- Border control
- Visa applications
- Authentication of citizens with a large platform of applications
- Police at Port Authority against watch list
- Time and attendance in different offices and facilities

### Health Care

- Patient identification (patients may arrive unconsciousness), social security, health insurance
- Doctors and staff physical access control for secured area or restricted places.
- Doctors and staff logical access control
- Time and attendance

### Banking

- Access control, logical access, restricted area
- Customer's identification according to regulations
- Time and attendance

### Education

- Access control and logical access, restricted area
- Restricted student and staff areas
- Presence at lessons and laboratory
- Time and attendance for staff

### Large organizations

- Physical access control to restricted areas by authorization, controlled by central data base center, and regulated by levels of security
- Logical access control to restricted areas by authorization, controlled by central data base center, and regulated by levels of security
- Time and attendance by different requirements of biometrics or electronics managed by central database and regulated by levels of security



### BioGuard Components & Technologies Ltd.

4, HaCharash st. | Tel: +972-9-7695200 | Mail: P.O.B. 7341  
Hod-HaSharon | Fax: +972-9-7417770 | Hod-HaSharon Israel, 45240  
Israel, 45240 | www.bio-guard.net | Email: info@bio-guard.net

