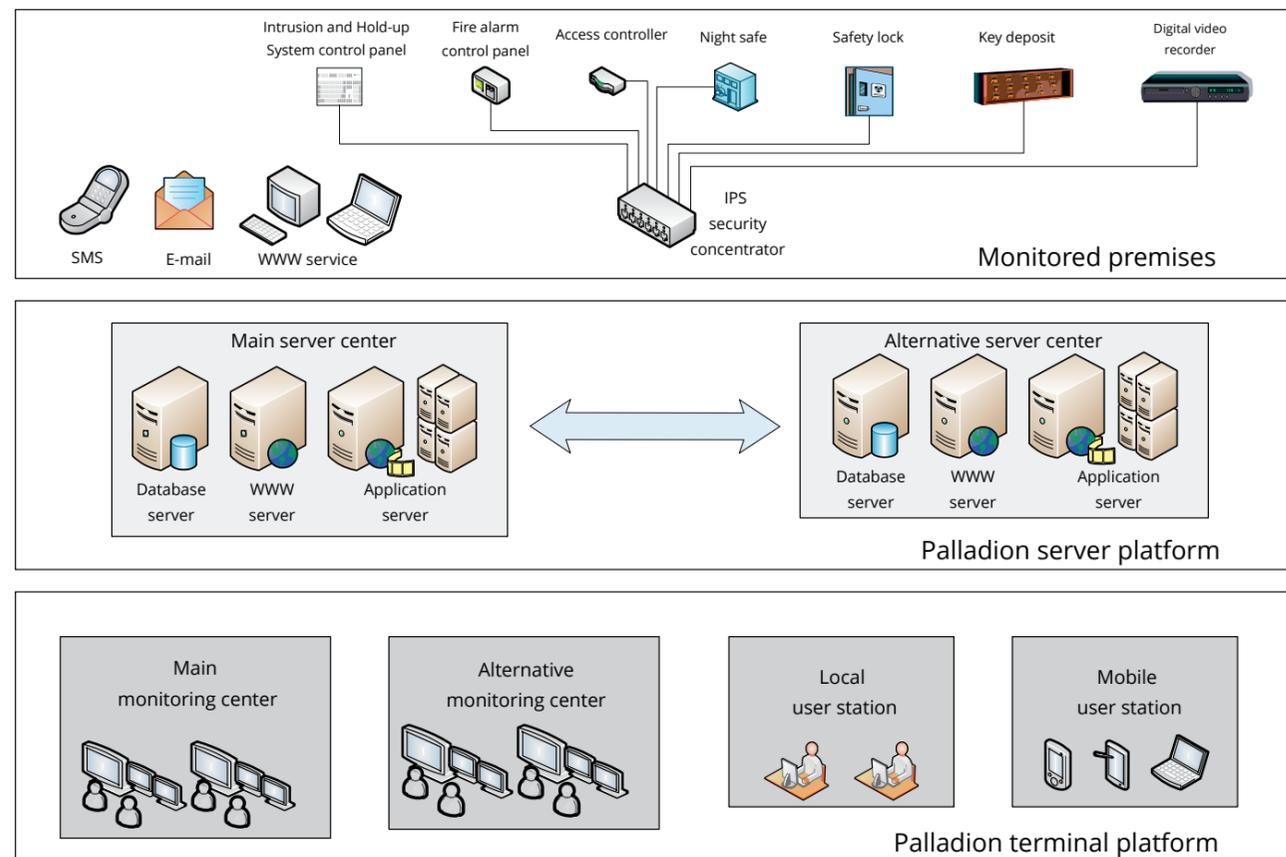


## Central Security Management System PALLADION



### Characteristics of the PALLADION Central Security Management System

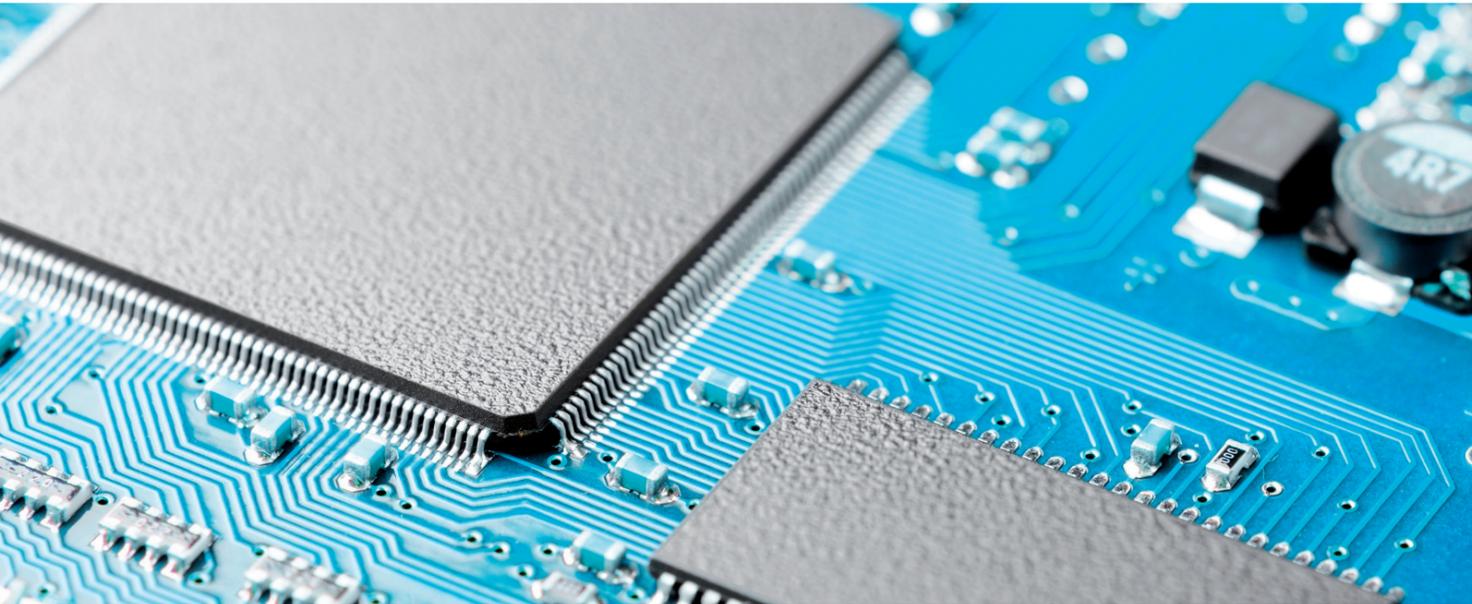
Server operating system .....	MS Windows Server 2008/2012
Terminal operating system .....	MS Windows 7 PRO, 8 PRO, XP Pro
Database .....	MS SQL Server 2008/2012
Software .....	PALLADION Server PALLADION Administration Terminal PALLADION Alarm Terminal
User interface .....	Configurable layout of the graphical user interface Single-monitor and multi-monitor mode of operation Multi-layer presentation of security zone states Graphical presentation of the event list, including the state of event handling Presentation of current states of security zones and devices
Supervisory functions .....	Graphical presentation of alarm events and technical events Automatic diagnostics of main elements of the system Remote management and configuration of devices Logging of operator actions
Access control subsystem .....	Max. 5,000 controlled passes Max. 1,000 users Centralised management of permissions Integration with Active Directory
Reports .....	Acc. to the Customer's requirements

# Central Security Management System PALLADION



STEKOP SA • 02-127 Warsaw • ul. Moldawska 9  
 Head Office: Poland • 16-070 Choroszcz • kol. Porosly 52  
 office phone: +48 85 748 90 15 • fax: +48 85 748 90 38  
 www.stekopsa.pl • e-mail: stekop@stekopsa.pl





**The Palladion Central Security Management System** is an innovative platform in the field of security technology, intended for building and centrally managing security systems in distributed facilities on a global scale, such as corporations, bank networks, retail store networks, offices and military facilities.

The Palladion system utilises the existing LAN/WAN and GSM/GPRS network structures to provide full integration of field security systems, such as intrusion and hold-up systems, access control systems, fire alarm systems, and building automation, using the IPS concentrator. Other types of systems operated by the Customer can also be integrated and supervised. This way, a platform is created that enables centralised collection and analysis of facility security information in real time, as well as support in decision making, depending on the type of threats detected. In addition, the Palladion system allows each connected device to be managed centrally, e.g. to have configured operating parameters, have modified access permissions, have software updated, etc. Data collected from the entire system are utilised to create various reports used by specialised departments of a given organisation. Report templates are adapted to the procedures functioning in the organisation.

Due to the low consumption of the LAN/WAN communication link bandwidth by the Palladion system during its operation, it can operate within the Customer's existing corporate network without a noticeable impact on network performance. Therefore there is no need for building and maintaining a dedicated monitoring network. This greatly limits the costs related to system operation. The security of operation, provided by the encryption mechanisms of transmitted data, multi-path communication channels, and server redundancy, is an unquestionable advantage of the PALLADION system.

The PALLADION system has obtained the Certificate of Qualification that confirms meeting the highest parameters specified in the PN-EN standard: 50136-1-1 and 2-1 – Alarm systems. Alarm transmission systems and equipment.

#### **System elements**

- System servers;
- Specialised system terminals: alarm, administration, technical, access control;
- IPS security concentrator.

#### **Basic features of the Palladion Central Security Management System**

##### **• Monitoring and management of intrusion and hold-up systems**

- Integration of I&HAS control panels from various manufacturers in the system.
- Visualisation of alarm system states.
- Centralised configuration and management of I&HAS control panels.
- Providing cooperation of the I&HAS control panels with the access control system, the CCTV system, and the fire protection system.

- Remote management of security zones (dependent or independent disabling/enabling).
- Monitoring the performance of duties of security contractors based on reports generated (interventions, convoys, cash processing).

##### **• Monitoring and management of fire alarm systems**

- Visualisation of fire alarm system states.
- Capability of verifying a 1st degree alarm, using technical resources of the system (e.g. CCTV).
- Centralised configuration and management of fire alarm control panel.
- Providing cooperation of the fire protection system with the access control system and the CCTV system.

##### **• Management and monitoring of access control systems**

- Global integration of the existing local access control systems.
- Operation in the global network mode or the stand-alone mode, with switching between modes of operation depending on the network availability.
- Distribution of access permissions and rules for users.
- Creation and management of user groups at the central level and the regional level.
- Effective mechanism for granting and migrating permissions depending on the role assigned to a user in the access control system.
- Verification and reporting of events from local access control systems.
- Integration with the existing IT security and user permission management systems (Active Directory, SAP/HR, etc.).
- Integration of custom equipment, such as locks with user's weight identification, palm geometry readers, key depositories, safes, cassettes with electronic code locks, etc.
- Cooperation with time and attendance systems.

##### **• CCTV system support**

- Cooperation with local CCTV recorders from various manufacturers.
- Automatic and manual monitoring of operational status of local DVR recorders.
- Automatic and semi-automatic verification of camera settings.
- Automation of the CCTV recording retrieval process.
- Providing cooperation with integrated security subsystems: e.g. links to alarm events, verification of fire alarms, support for the verification of intrusion and hold-up system users as well as access control system users, etc.
- Workstation types:
  - central monitoring;
  - local monitoring;
  - WWW service.