



KADRIS 4

Solutions by ČETRTRA POT

Enterprise Identity & Access Control Platform

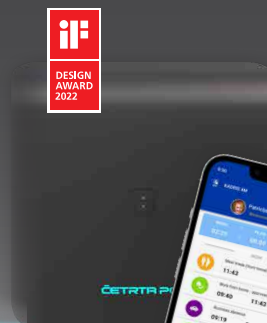
One Platform. One Manufacturer. One Accountability.

Enterprise Hardware ■ Software ■ ID Media ■ Mobile Access

TX-600 Time and Attendance Terminal



CMX3 readers



CMX5 readers



NEW!
X-line
hardware
range

KADRIS 4 ID cards



KADRIS 4 Mobile app



Developed & Manufactured in Slovenia
One trusted European manufacturer.



ISO 27001
Information security by design.



ISO 22301
Ensuring business continuity and organisational resilience.



NIS2 Compliant
Designed to support evolving NIS2 requirements.



EN 60839-11-1
Certified Security Grades 2-4.



Quantum-Ready
Advanced NXP-based cryptography for future-ready credentials.

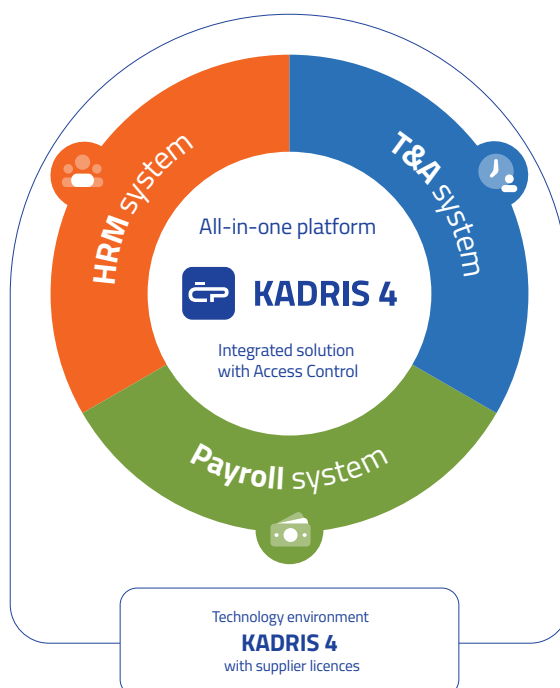


01 Why partners choose KADRIS 4?

KADRIS 4 combines Access Control, Time & Attendance, Identity & Workforce Management and Payroll within a single enterprise platform. Hardware, firmware and software are developed by company ČETRТА POT in Slovenia, giving our partners direct access to the engineering expertise and lifecycle support behind the solution.

The platform supports projects ranging from standard commercial installations to complex enterprise and critical infrastructure environments with flexible deployment, integration and authentication options.

For our partners, this means one technology portfolio, direct manufacturer support and the ability to address projects from Access Control to broader Workforce management requirements.



Key differentiators:

- **European development & manufacturing**
Hardware, firmware and software developed in Slovenia.
- **Integrated hardware & software**
Readers, controllers, terminals, mobile credentials and software designed as components of the same platform.
- **Enterprise Security**
EN 60839-11-1 (Security Grades 2-4), ISO 27001, ISO 22301, NIS2 Compliant architecture and advanced NXP-based cryptography.
- **Flexible identification**
Smart cards and mobile credentials, including offline mobile access.
- **Flexible Deployment**
On-premises, cloud, SaaS and ACaaS deployment models.
- **Long-term compatibility**
Scalable architecture, backwards compatibility and integration with ERP, fire alarm and other enterprise systems.

Why European technology matters?



Designed. Developed. Manufactured. Supported. All in Slovenia.

Photo source: Arhiv ARMAT d. o. o.

35+
YEARS OF EXPERIENCE

TRUSTED BY
950+
CLIENTS



Healthcare



Banking



Manufacturing



Energy



Government



Critical
Infrastructure

For partners and their customers, the origin of security technology is becoming increasingly important. European development and manufacturing provide greater transparency over where technology is developed, how cybersecurity is managed and who is responsible for its long-term development and support.

This is particularly relevant as organisations place greater emphasis on digital sovereignty, NIS2 requirements, supply-chain security and the long-term availability of critical technologies. For enterprise and critical infrastructure projects, choosing a European manufacturer can therefore be an important part of both technology and risk management.

With KADRIS 4 developed and manufactured in Slovenia, our partners work directly with a European technology manufacturer and have access to local engineering expertise, technical support and long-term product development within the EU.

02 Security & Compliance

As a critical part of an organisation's security infrastructure, Access Control in enterprise and critical infrastructure environments requires more than reliable identification and door control.

Security must be addressed throughout the entire system - from credentials and encrypted communication between devices to system architecture, information security and operational continuity. At the same time, organisations need to consider cybersecurity requirements, regulatory obligations and the ability of their security systems to remain available and supported over the long term.

KADRIS 4 combines certified Access Control with secure identification technologies and cybersecurity-focused architecture.



Developed & Manufactured in Slovenia
One trusted European manufacturer.



ISO 27001
Information security by design.



ISO 22301
Ensuring business continuity and organisational resilience.



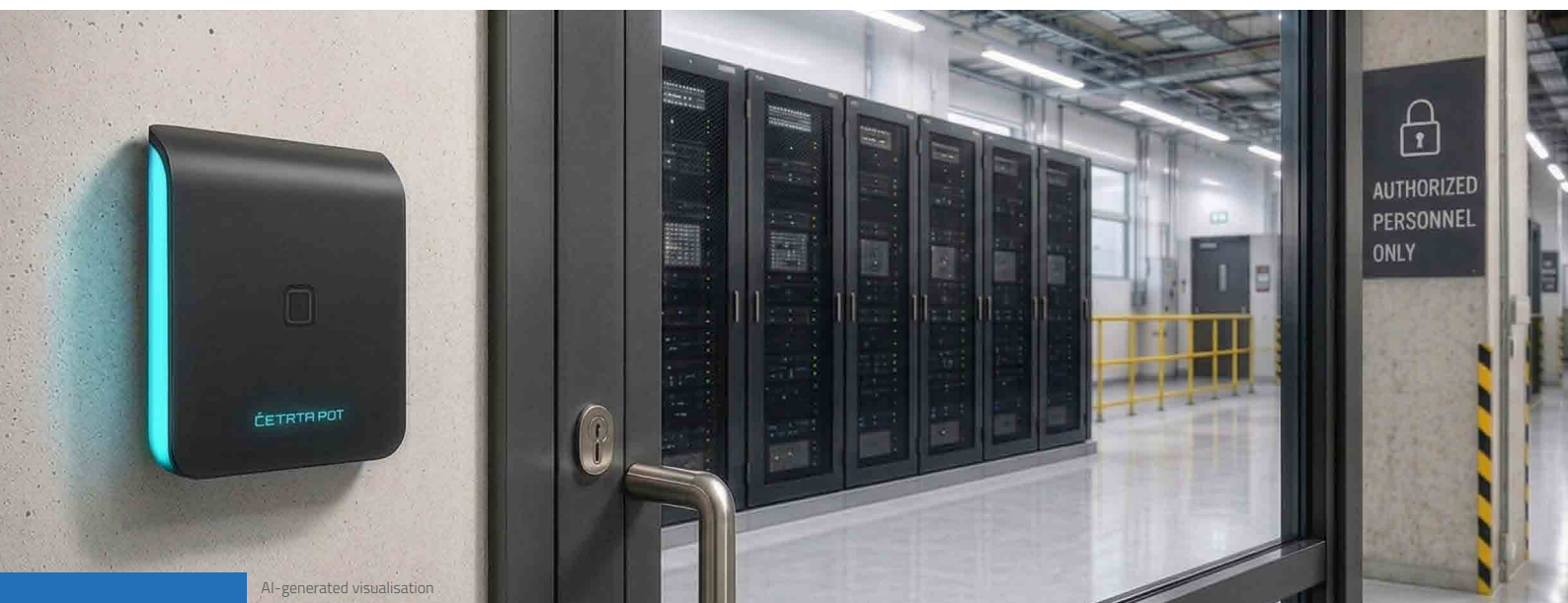
NIS2 Compliant
Designed to support evolving NIS2 requirements.



EN 60839-11-1
Certified Security Grades 2-4.



Quantum-Ready
Advanced NXP-based cryptography for future-ready credentials.

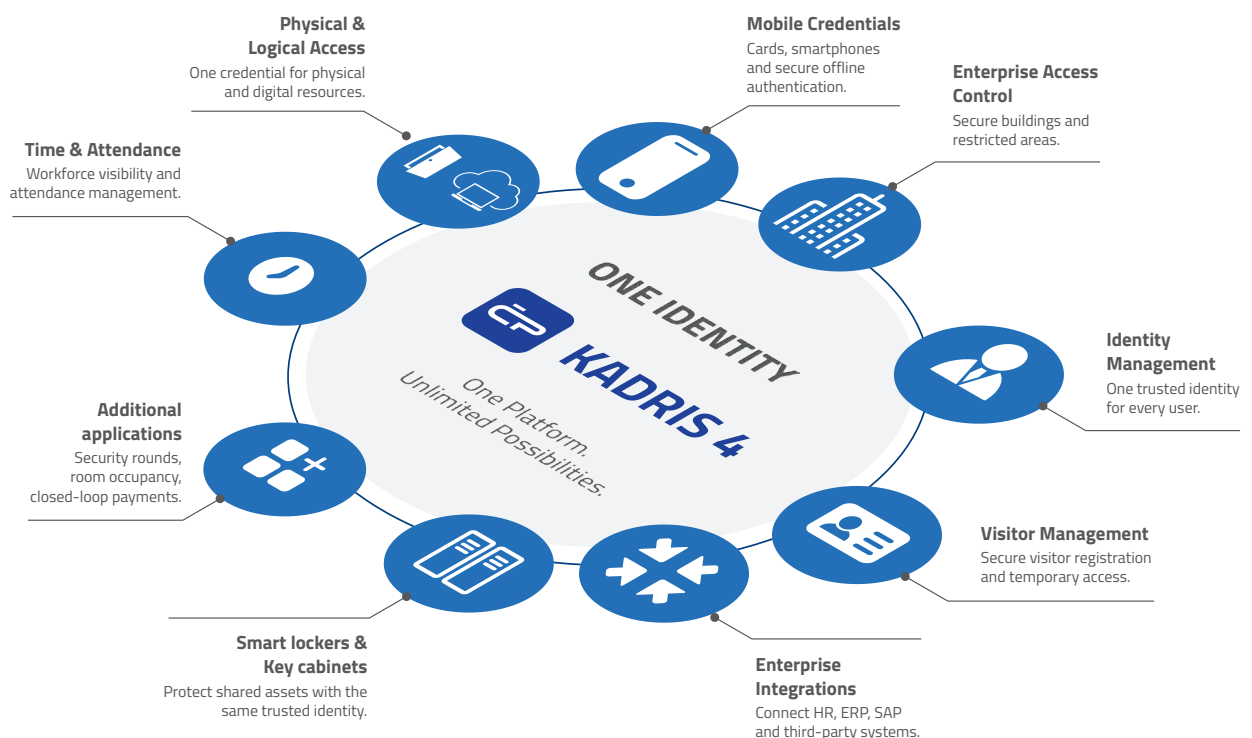


One platform. One identity.

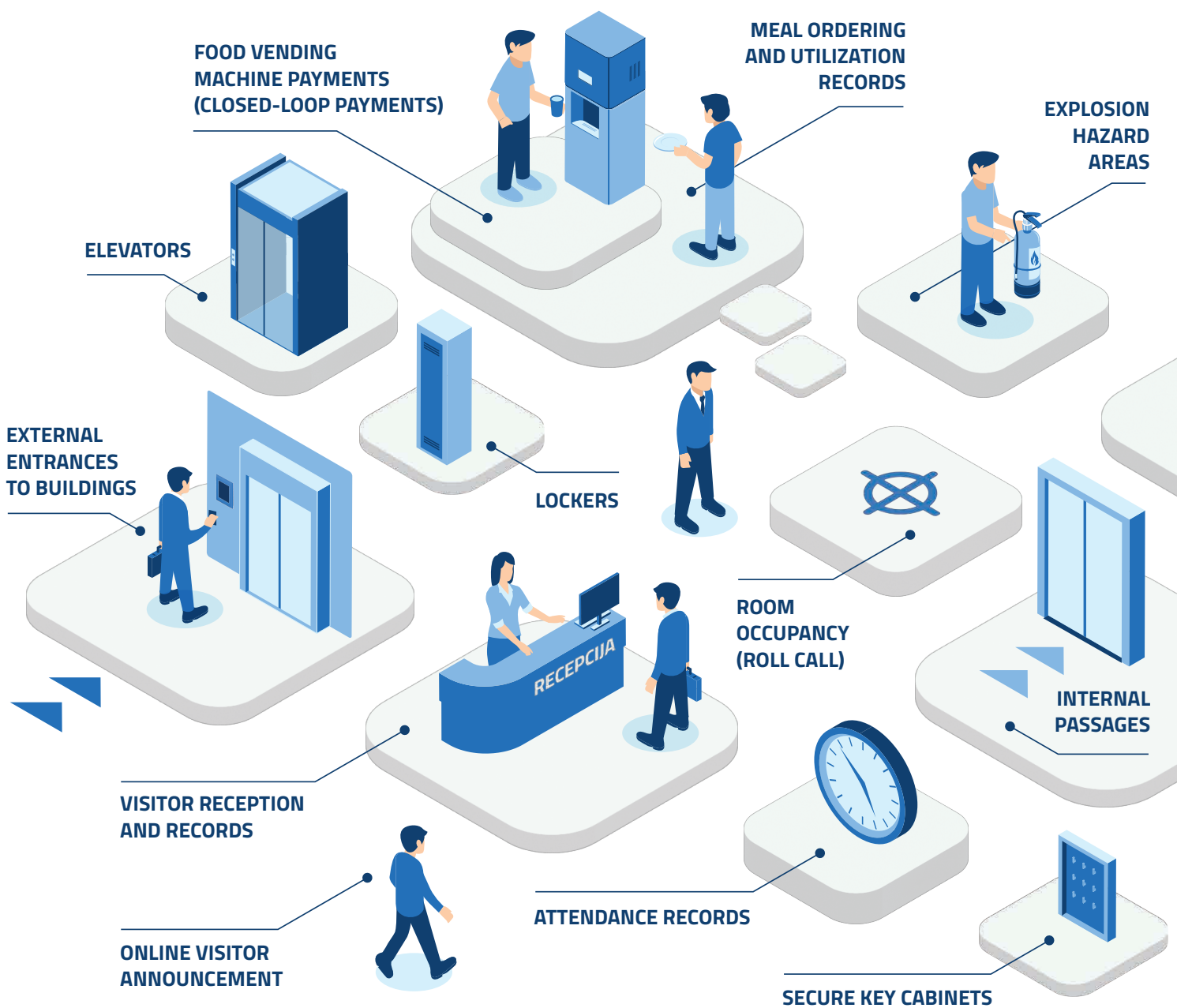
KADRIS 4 extends Access Control beyond securing entrances and restricted areas. The system can also support visitor management, security rounds, employee lockers and key cabinets, room occupancy, Time & Attendance and other processes where secure identification is required.

The same physical or mobile credential can be used across different KADRIS 4 functionalities, while user data and access rights are managed centrally. KADRIS 4 can also connect with HR, ERP and other security and enterprise systems.

What can partners manage with KADRIS 4?



03 Platform applications



KADRIS 4 Enterprise Identity & Access Control offers a range of functions for the client to choose from according to their needs and requirements. The system is built in a modular way and can be extended and scaled up at any time to keep up with your company's development. The figure below shows the different areas of Access Control application, with Time and Attendance functions also shown, as both areas are comprised in KADRIS 4.



FIELDS OF APPLICATION

- External entrances to areas (sliding doors, barrier gates, areas with anti-passback)
- Entrances to premises (building entrances, intercom line)
- Internal entrances (offices, passageways, elevators)
- Emergency exits (emergency exits and fire escapes, connection to fire alarm system)
- Spaces of special significance (vaults, laboratories, explosion hazard areas)
- Cabinets (lockers, secure key cabinets, safes)
- Use of devices and machines (printers, production machines)

04 Platform capabilities

KADRIS 4 Enterprise Identity & Access Control offers a range of functionalities that are available to users by means of a single identification medium, thus simplifying their use. The system is also easy to use for security staff, as it provides control over who, when and where can enter, while keeping a record of user accesses and access attempts.

The system is modular, which means that the client can choose which processes will be supported by the information system. The system can be expanded at any time, both in terms of functionality and the number of rooms it covers. The system is also scalable in terms of the number of users – the client can easily assign and revoke employee ID media. For larger companies, it is useful to issue the ID media in-house, whereas ID media personalization (printing of personalized information on the ID card) is also supported in KADRIS 4.



Control of access to areas and premises

Access Control not only replaces the keys for the main entrance to the premises, but also allows the entire company to be monitored through a single system, controlling access to all areas of the premises – from the reception area to important and high-security areas. As an integral part of the KADRIS 4 platform, Access Control provides comprehensive control of access to business premises using a single or a combination of several different identification media. Access Control restricts and controls access to premises and areas, controlling who, when and where can enter. A record of all accesses and attempts to gain access is also maintained.



Room occupancy

The list of people present is updated as users register at Access Control readers or Time and Attendance terminals. For the room occupancy functionality to operate, a room or zone must be defined and entry and exit readers must be assigned. As a user presents their credentials at a specific entry reader, the user is included in the attendance list, and when presenting at the exit reader, they will be deemed to have left the premises. Users are required to register their entries and exits diligently to ensure correct attendance records. The functionality may be used to ensure occupational health and safety, and for evacuation purposes. When only required to provide information about who is present at work, while information on the exact room is not relevant, the Time and Attendance part of KADRIS 4 is sufficient.





Time and Attendance

Time & Attendance is one of the core capabilities of the KADRIS 4 Enterprise Identity & Access Control Platform. Fully integrated with Access Control, it enables organisations to manage employee identities, attendance records and access rights from a single platform. Users authenticate with the same trusted credential across both functionalities, while employee data and access permissions are managed centrally. This eliminates duplicate administration, simplifies daily operations and reduces the risk of errors. Depending on the deployment scenario, Time & Attendance terminals can also be used to control access to secured areas.



Online visitor announcement, reception and records

Admission of visitors to premises is part of a comprehensive security system that includes advance notice of visits, reception and registration of guests. KADRIS 4 provides Online Visitor Announcement and Visitor Reception (Reception Desk) modules, which complement the Access Control system. The modules support reception desk activities and analysis of the data on visits, visitors and reception desk staff. Employees can announce their visitors and book meeting rooms. The system provides an overview of the announced visits and assigns the visitor a temporary ID card to open appropriate doors. The receptionist has an overview of the visitors currently present and all visits are recorded in the database. It is also possible to create reports on visits and visitors in accordance with GDPR guidelines. The functionality is of particular value in cases of evacuation.



Guard tour monitoring with the KADRIS 4 Security app

The majority of security risks and unnecessary costs related to business premises arise due to forgetting to turn off the lights and leaving the windows open. These and any burglary risks can be eliminated by the security service performing regular patrols. The solution for tracking and monitoring security guard patrols is ensured by the guard tour system. Guards record their tour at control points using their mobile phone or a registration terminal, thus enabling the monitoring of their tour by the surveillance team.



Wardrobe locker security

Wardrobe locker access control using ID cards is a very simple solution for employees. The operator can monitor the information about which lockers are occupied, trigger an alarm in case of burglary, and create reports on locker events and status. At the same time, the organization can cut locker maintenance costs.



Key cabinet security

Key locker is a convenient key storage solution that provides simple access control to keys using an ID card. The solution can be used in environments where electronic locking access control is not absolutely necessary or economically feasible.



Logical Access Control

Logical access control means controlling access to information systems and computers using a smart ID medium and a personal password. The advanced KADRIS 4 ID card version – K4IDX, based on MIFARE DUOX® technology, enables this with a single medium: employees use the same card to enter the building and to log into the information system. To implement logical access control, appropriate ID media, readers, software and Public Key Infrastructure (PKI) are required. The optimum solution is a combination of a physical ID medium, a unified media database and a Single Sign-On (SSO) system. Users must handle their ID card with care, as they cannot use their computer without it. When leaving the office, they are forced to take it with them, and consequently the computer automatically locks. Any sharing of cards and passwords is thus inherently prevented.

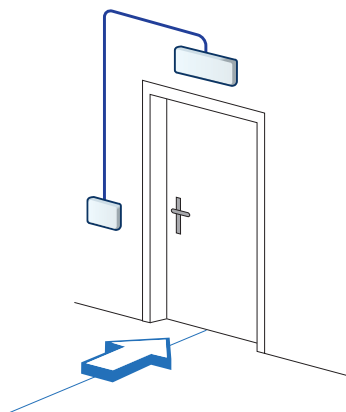
05 Access Control layouts

An Enterprise Identity & Access Control platform combines hardware components such as control units, readers, locks and other point-of-entry restriction devices (e.g. turnstile, barrier gate), power supply components and software that links the operation of the components. The software allows the management of user access rights, implements the functionalities offered by the system, and processes events in the system and records them accordingly in the database. The identification media used by users to communicate with the system are also considered part of the system. Time and Attendance terminals may be part of Access Control, however, their primary role is to record working time and, only in rare cases, to control access.

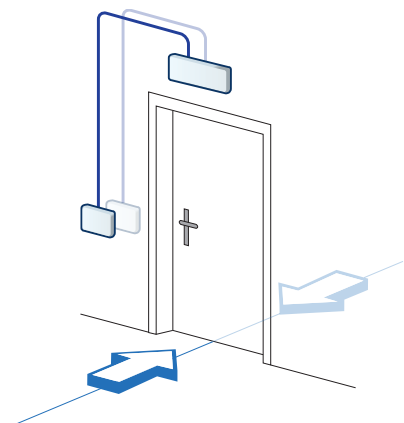
Depending on the client's needs, the Access Control system can be designed as a simple system or as a system with multiple functionalities and a high level of security. Security level is determined by hardware topology, i.e., the physical implementation of connections between system components. Independently of the physical implementation, the software can be configured in different ways to define the right to enter the premises. Rights can be assigned under **simple** Access Control principles, which impose only few restrictions (who is allowed to enter certain doors), under **advanced** Access Control principles (possible to create groups of doors) or **extended** Access Control principles, which allow for more rigorous entry restrictions (adherence to timetables, calendars and work regimes, and the provision of advanced features such as anti-passback).

Reader layout options

One of the decisions to be made regarding the layout is whether the door will be equipped with a reader on one side only (one-way Access Control) or on both sides (two-way Access Control). The latter case requires more equipment and settings, and accordingly provides additional functionalities, such as monitoring the presence of people in a room (room occupancy) and preventing re-entry without exiting first (anti-passback function). Different reader designs are available.



One-way Access Control is the simplest method of controlling access to any area or space (parking space, entrance to the building, room, elevator, ...) where access needs to be controlled and free exit must be ensured.



Two-way Access Control is used in cases where access from both sides of a door needs to be controlled (e.g. passage between corridors). Evacuation route standards must be adhered to in such context.

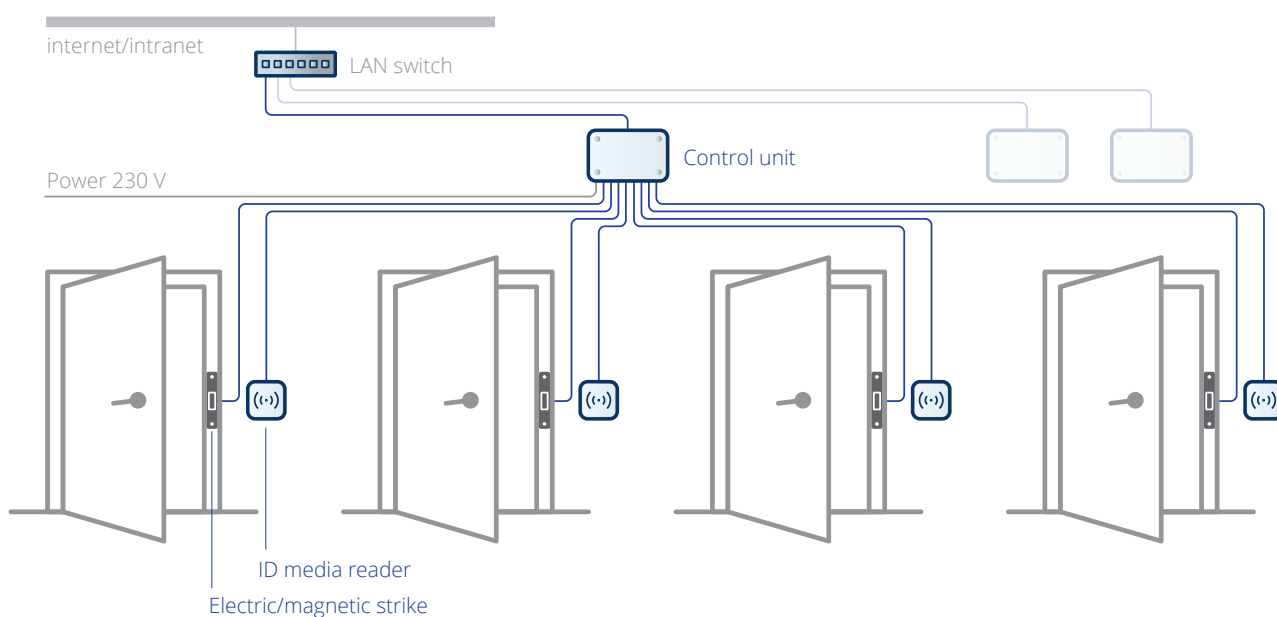
Control unit layout options

Another decision related to the system layout is, for example, what level of security must the system provide. The primary or preferred choice is a layout that provides high security. The secondary choice is appropriate in circumstances where only basic functions need to be provided and cost optimization is important to the client.

Primary security choice – the highest level of security

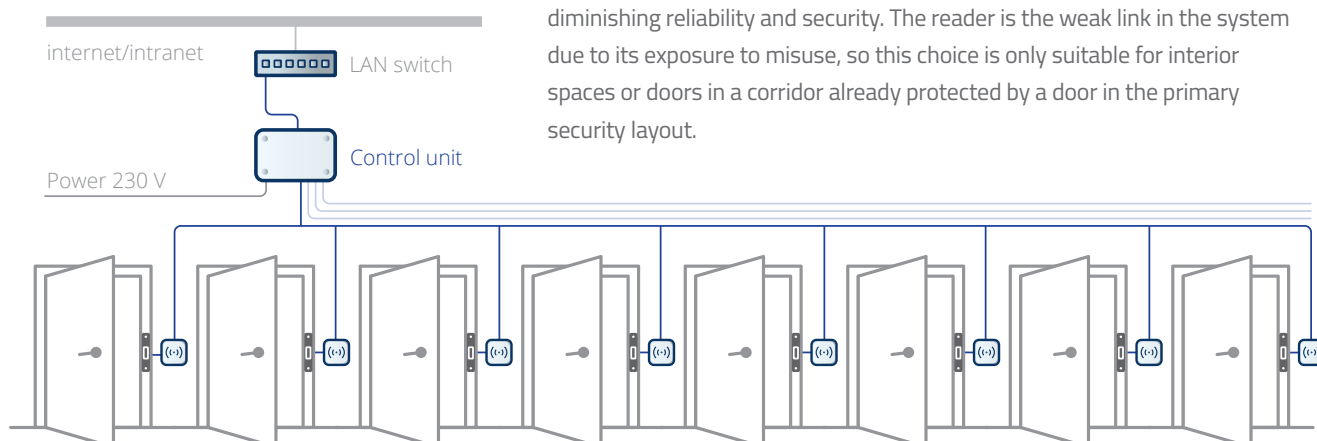
The most common layout is that each control unit in KADRIS 4 is provided with uninterruptible power supply and can operate up to four one-way or two-way gates, including locks and sensors. The entry regime (who and when can enter) can be defined for each gate.

One control unit can operate up to 4 doors. The essential advantage of this design is a high level of security, autonomy in the event of power failure, and autonomy of individual doors in the event of forcible entry at any other door.



Secondary security choice – simple and affordable

If the client does not need high security level and aims at cost optimization, there is the option for one control unit to manage a larger number of gates (more than 4). The individual gate is managed via the reader and not via the control unit. Uninterruptible power supply is not provided, consequently diminishing reliability and security. The reader is the weak link in the system due to its exposure to misuse, so this choice is only suitable for interior spaces or doors in a corridor already protected by a door in the primary security layout.

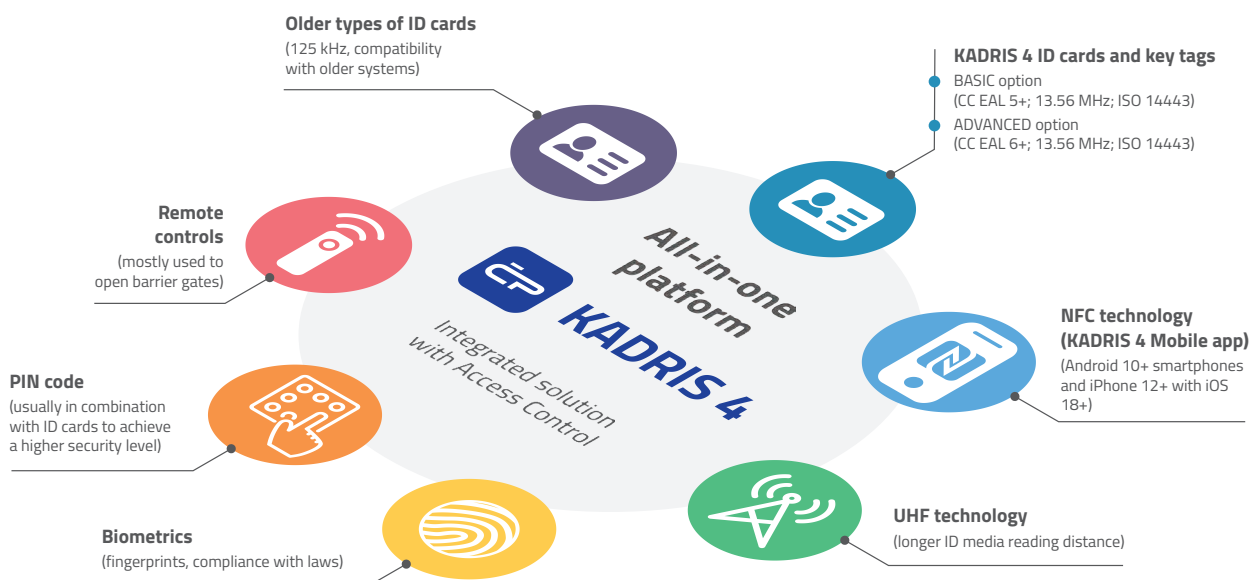


06 Identity media

KADRIS 4 Enterprise Identity & Access Control platform enables identification by advanced means of identification, the common denominator of which is superior security and reliability.

Technologies compatible with KADRIS 4 Enterprise Identity & Access Control platform:

- KADRIS 4 ID cards and key tags
 - BASIC option (CC EAL 5+; 13.56 MHz; ISO 14443)
 - ADVANCED option (CC EAL 6+; 13.56 MHz; ISO 14443)
- NFC (door opening and identification with Android 10+ smartphones, iPhone 12+ and iOS 18+),
- Remote controllers (mostly used to open barrier gates),
- UHF (used when substantial reading distance is required),
- PIN code (usually in combination with ID cards to achieve higher security level),
- Biometrics (fingerprints, as compliant with laws and regulations),
- Older types of ID cards (125 kHz, compatibility with older systems).



Advantages of a single identification credential

- Unified management and one media (card, key tag or mobile app) for Access Control and Time & Attendance.
- Changes are made once and applied throughout the system, reducing duplicate administration and the risk of errors.

KADRIS 4 cards and key tags



KADRIS 4 cards and key tags are secure identification media based on trusted NXP MIFARE technology. Each KADRIS 4 credential is securely personalized with unique security keys that help prevent counterfeiting and unauthorized access. Available in two security options, they enable organizations to select the level of protection that best fits their requirements.

NEW

BASIC OPTION

KADRIS 4 ID cards and key tags – K4IDF

Proven security

Powered by NXP MIFARE DESFire® EV3 technology

-  CC EAL 5+
-  AES-128
-  Physical Access
-  Time & Attendance

For organizations requiring secure and reliable everyday identification.

ADVANCED OPTION

KADRIS 4 ID cards and key tags – K4IDX

Next-generation security

Powered by NXP MIFARE DUOX® technology

-  CC EAL 6+
-  AES-256 + ECC
-  Physical + Logical Access
-  Quantum-ready
-  Relay attack protection

For organizations with advanced security requirements.

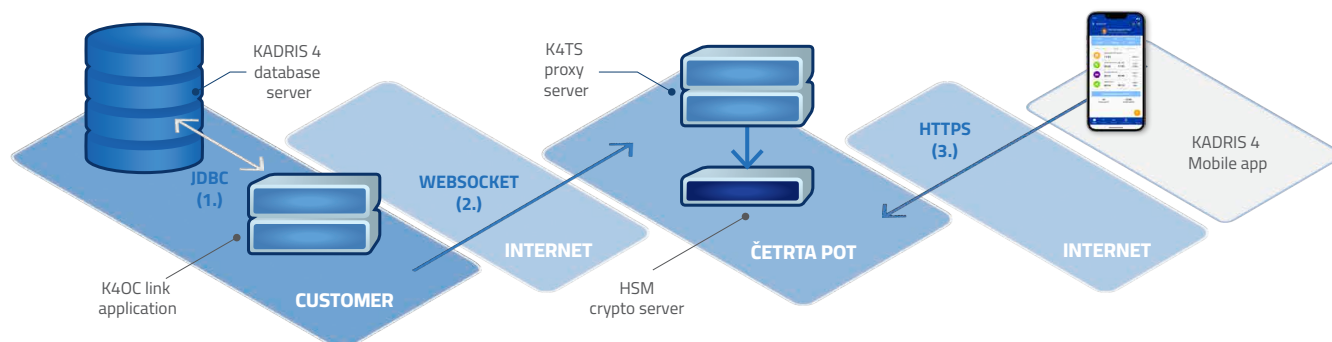


KADRIS 4 Mobile app



The most important trend in access control today is the use of smartphones for door access. Dedicated mobile applications have taken over the role of traditional identification media and have become an integral part of a comprehensive security system. To complement its portfolio of identification methods, KADRIS 4 now includes the KADRIS 4 Mobile app, available for NFC-enabled Android and iOS devices. A key advantage of the KADRIS 4 Mobile app is that it continues to operate even without an internet or mobile network connection. Once connectivity is restored, all data is automatically synchronized with the database.

A smartphone is an external system that cannot be monitored in terms of security. This is why the design of KADRIS 4 Access Control features proxy servers between the internal and external environments. Proxy servers receive requests from external devices (smartphones) through the firewall, the crypto-server performs device authentication, and only then the processes that are normally in place in a closed system with ID cards as a means of identification are carried out. The mobile application is not sufficient on its own; verification in the closed part of the system needs to be carried out, as well. Each new smartphone must be registered in the system and verified. The figure below shows the implementation of the Access Control system that includes smartphones.



07 X-line hardware products

One Platform. One Manufacturer.
One Accountability.



OnPrem



Cloud



ACaaS



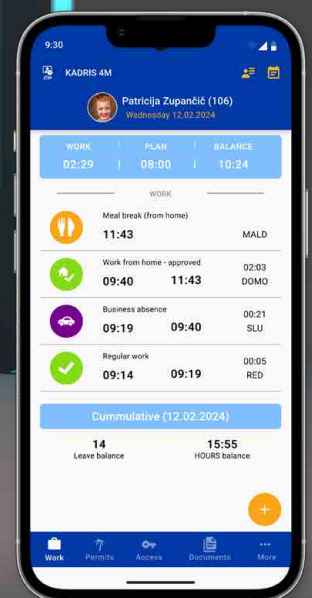
SaaS



CMX3
readers

CMX5
readers

TX-600
Time and
Attendance
terminal



08 Readers & Terminals

Appropriate readers are used to read the ID media, and identification is done in a contactless manner. Certain reader models allow for PIN or fingerprint identification. Creative design of the reader and the Time and Attendance terminal follows the “balanced flat design” principles and includes RGB LED signaling.



CMX3 and CMX5 readers

Supported ID media:

- KADRIS 4 ID cards and key tags compliant with ISO 14443 and NFC standards,
- Smartphones: KADRIS 4 Mobile app (Android and iOS with NFC),
- Bank payment cards (for access to ATM areas),
- ID-media reading distance: up to 80 mm.

Built-in security standards:

- ID media tokenization,
- eSE (embedded Secure Element) for encoding/decoding and storing security keys,

- AES for ID media authentication and encryption,
- AES for encrypted communication with the controller.

Technical specifications:

- operating frequency: 13.56 MHz, Bluetooth 2.4 GHz,
- communication: RS485-2v serial communication, optional USB, AIRg2, 4WX communication protocol,
- identification indicators: buzzer, RGB LED strip backlight along three sides,

- dimensions: CMX3: 90 × 90 × 15 mm, CMX5: 145 × 58 × 15 mm,
- installation: CMX3: flush-mounted on the wall (60 mm box), CMX3 and CMX5: surface-mounted on a non-metallic surface,
- power supply: 7–12 V, 100 mA or USB 5 V 200 mA,
- operating temperature: –10 °C to +60 °C, relative humidity: 5–95%,
- degree of protection: IP65.

Compliance with standards:

- CE, compliant with Directive 2014/53/EU (Radio Equipment Directive),
- EN 60839-11-1 certificate for access control systems.

Options:

- H ... supported high reader frequency 13.56 MHz,
- M ... supported NFC mobile phones.



TX-600 Time and Attendance Terminal

(preliminary information)

Key features:

- high-performance processing unit with a 64-bit ARM processor,
- 7" 16:10 landscape color LCD display, resolution 1280×800, brightness 400 nits,
- contrast ratio 800:1,
- capacitive touchscreen,
- ID media reader,
- visual and acoustic indicator,
- camera (optional),
- real-time clock with synchronization to time servers via the NTP protocol.

Supported ID media:

- KADRIS 4 ID cards and key tags compliant with ISO 14443 and NFC standards,
- smartphones as ID media: KADRIS 4 Mobile app (Android and iOS with NFC),
- ID media reading distance: up to 60 mm.

Built-in security standards:

- AES for authentication and encryption of ID media,
- TLS 1.3 (HTTPS) for secure communication with the server.

Technical specifications:

- communication: 1 Gbps LAN, optional Wi-Fi,
- communication protocol: AIRg2, 4WX (other protocols optionally available),
- dimensions: 178×185×28 mm (without wall bracket),
- mounting: wall-mounted with the supplied wedge-shaped metal bracket,
- power supply: via Ethernet cable in accordance with the PoE standard,

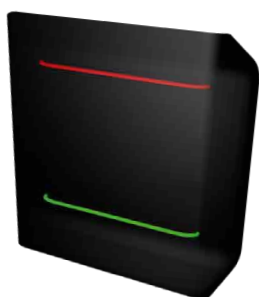
- operating temperature: -10 °C to +60 °C,
- relative humidity: 5-95%,
- protection rating:

Standards compliance:

- CE, compliant with Directive 2014/53/EU (Radio Equipment Directive).

Options:

- C ... built-in camera for additional identification verification,
- W ... built-in Wi-Fi and Bluetooth,
- IP ... IP65 protection.



CM500 UHF reader

Technical specifications:

- dimensions: 290×290×100 mm,
- mounting: on a post or a wall,
- power supply: 12 to 24 V DC or PoE+,
- operating frequency: 865 to 868 MHz,
- ID media: card, vehicle sticker, combined card option (13 M + UHF),
- reading distance: theoretically 8 m, 3–5 m in practice,
- communication: TCP/IP,
- possible to connect additional antenna (depending on the model) to control multiple gates.



Aperio digital cylinder/handle

Aperio products are designed to control passage at the location of the door. Communication to the VT-500 control unit is wireless via a module that is wired to the control unit. The product is fully integrated in the KADRIS 4 Access Control. Aperio is suitable for gates where, due to various factors, the implementation of wiring is not feasible or economical. One VT-500 control unit can control up to 32 doors in this scenario.

Aperio digital cylinder replaces the conventional key cylinder on the door. Therefore, the cylinder

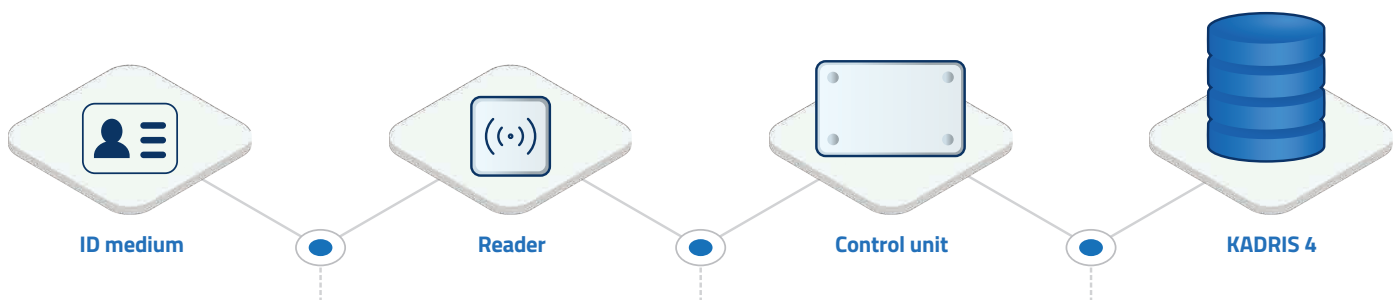
responds only when an ID card with appropriate access rights is presented. Aperio handle replaces the conventional door handle. The handle can only be used when an ID card with appropriate access rights is presented.

Supported ID media:

- ID cards compliant with ISO 14443 and ISO 15693 standards (ČETRTRA POT DESFire),
- reading distance: up to 30 mm.

09 Communication infrastructure between system components

KADRIS 4 software platform ensures uncompromising security at the level of communication between the system components, i.e. between readers, controllers and the database.



Communication between ID media and readers

Data transfer from the ID medium to the reader is encrypted (AES 128-bit encryption). Each ID medium has its own unique key assigned with the diversification process (calculated from the master key). The unique key is stored securely in the ID medium and is authenticated by the 3-way handshake principle, which prevents misuse (card copying or false identification).

Three levels of security are available:

- medium ID verification,
- application ID verification,
- authentication.

The master key is stored in the secure element of the reader. Organizations with specific security requirements have the option of acquiring their own master key.

Communication between readers and control unit

At the level of data exchange between the reader and the control unit, the possibility of encryption and 3-way handshake authentication is implemented, as well. The reader is the exposed part of the system as it is mounted on a wall and is therefore easily accessible, which is why we need to ensure that the control unit can verify reader's identity, while encryption is used to prevent any unauthorized interference with the system (cyber-attacks).

Communication between control units and database

Communication between the control unit and the database is conducted through the database server over the intranet or Internet using HTTPS protocol.

Advantages of such communication concept:

- data encryption, and in this respect GDPR compliance,
- remote hardware management (firmware updates, diagnostics, troubleshooting).

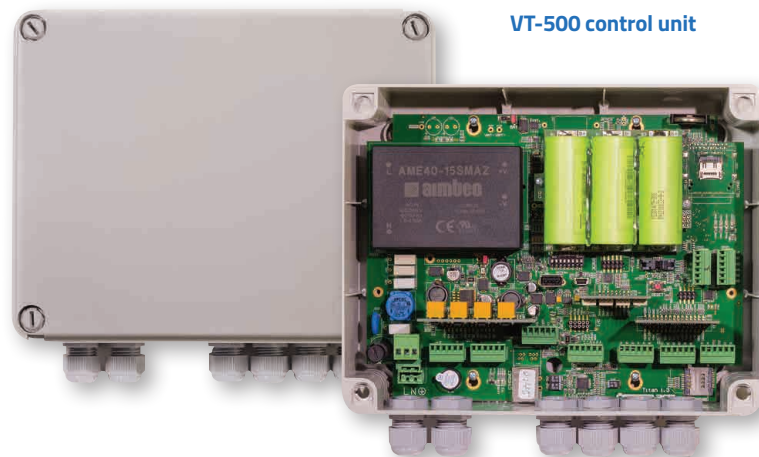
10 Access controllers



Control unit is the core of the Enterprise Identity & Access Control system. It captures data from ID media by means of readers, communicates with the databases, and controls latch release mechanisms.

The VT-500 control unit of the KADRIS 4 Enterprise Identity & Access Control system offers different levels of autonomy, depending on the version of the built-in uninterruptible power supply. In the most powerful version, which complies with EN 60839-11-1, grade 4, autonomy of four hours is guaranteed. The grade 3 compliant version holds autonomy for two hours, while grade 2 does not require uninterruptible power supply.





Technical features:

- Standalone microcomputer system with embedded Linux operating system,
- Supports a variety of standard-compliant ID media (standards ISO 14443, ISO 15693, ISO 18000 and ISO 18092), such as ČETRITA DESFire EV3, MIFARE Classic, NFC- or BLE-enabled mobile phones, iCode, Legic, Hitag, EM4xxx, uCode and other UHF media, RF remote controllers, biometrics, license plate recognition and other, depending on the reader type,
- Software and hardware support to manage four two-way or one-way passages (up to 16 one-way passages in the case of the secondary security choice),
- Direct connection to Ethernet TCP/IP network,
- 2 slots for SAM security cards,
- 230 V AC, 50 W power supply, built-in 12 V DC power supply for electric strikes (NC or NO),
- Battery-powered with LiFePO₄ technology, autonomy of at least 4 hours when powering 4 readers (does not include electric strikes) only for VT-500.4 (grade 4),
- Supports state-of-the-art communication methods (Ethernet, USB, RS 485, RS 232, service port: JTAG),
- Fully autonomous operation in the event of internet outage,
- Data retention and clock operation for up to a week after power off,
- Functions: monitoring which door are open, anti-passback function, opening using a request-to-exit pushbutton (intercom line, fire escape), control of sliding doors, turnstiles and elevators, connection with fire alarm system,
- A variety of connections to other units is supported with serial communication or digital input/output lines (fire and alarm system, automatic doors and other),
- Autonomous operation with a database of up to 100,000 users/ID media (large storage for ID card database, database tables, and Time and Attendance events),
- CE certification (EN 55032, EN 61000-3-2, EN 61000-3-3, EN 60950-1, EN 50581),
- Compliance with EN 50133-1 (grade 3, category B), and EN 60839-11-1:2013 (grade 4) and SZPV-411 guideline,
- Built-in surge protectors and elimination of interference on power and communication lines,
- Enhanced security with SAM cards,
- Automatic or configurable daylight-saving time settings,
- Help Desk is provided, modifications according to customer's requirements are possible.

11

Certified Enterprise Security

EN 60839-11-1

(Grades 2–4)

Since 2022, KADRIS 4 - Enterprise Identity & Access Control has been certified according to the EN 60839-11-1:2013 international standard, which specifies general requirements for the functionality of electronic access control systems, and characteristics of system components. Requirements of the standard are classified into grades 1 to 4, with grade 4 representing the most stringent criteria.

The requirements of EN 60839-11-1 fall into several categories:

- Required characteristics of access points to the protected area (requirements for readers at entrances and exits),
- Required properties of event display, alert and logging,
- Duress detection,
- Allowing access in individual cases (override function),
- Recognition of users who are allowed to enter and exit,
- Intrusion detection,
- Detection of loss of communication between parts of the system,
- System autonomy in the event of power failure,
- Requirements for interfacing with other systems,
- Compliance with regulations on electromagnetic immunity of equipment,
- Compliance with regulations on exposure to environmental influences.

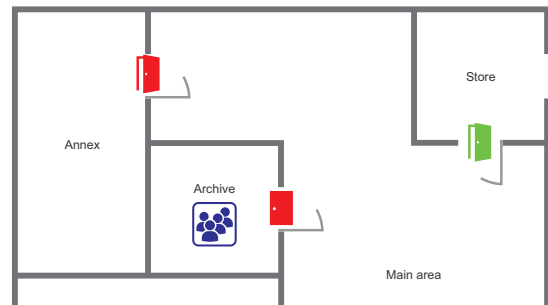
For each set of requirements, the standard specifies the procedures to be followed by the certification authority in verifying system compliance.

KADRIS 4 can be configured in line with grade 2, 3 or 4 requirements. The system is therefore suitable for clients who only need basic functionality, as well as for areas of special importance such as important production halls, critical infrastructure, financial institutions or government and military facilities, which require the highest security grade 4 according to this standard. Certified KADRIS 4 equipment includes the following:

- KADRIS 4 software,
- VT-500 control unit with battery for uninterruptible power supply,
- ID media readers CMX3 and CMX5.

All certified equipment has been developed by in-house experts with proprietary know-how, and has been manufactured using our own production facilities. This means that we have in-house expertise to ensure that our systems and components have a long life-cycle, high flexibility, scalability and integration with external systems.

Example of graphical representation of Identity & Access Control elements on a floor plan (icons for open/closed doors and alarms)



Overview of required and optional functionalities according to EN 60839-11-1



Functionality	Grade 2	Grade 3	Grade 4
Prevention of entry without prior exit (anti-passback – APB)	NO	Hard APB	Hard APB Soft APB – only alert Global APB – APB at the level of entire system Timed APB User status reset (disable/override)
Dual access – two ID media from a set of defined media must be presented within a certain timeframe for the entry to be granted	NO	NO	YES
Floor plan – graphical display of access control elements on the floor plan (icons for open/closed doors, alarms, clickable icons for detailed information)	NO	YES	YES
Monitoring and logging of transactions, events, alerts and alarms	YES (Reception Desk module)	YES (Reception module and Topology module – floorplan)	YES (Reception module and Topology module – floorplan)
Identification using a contactless card	YES	YES	YES
PIN-only identification	YES	Not allowed	Not allowed
Identification using a contactless card + PIN code	NO	Optional	YES
Duress PIN	NO	Optional	YES
Definition of rooms (zones) for room occupancy (roll call) functionality	NO	NO	YES
One-time opening of doors for a specific user	NO	YES	YES



12 Behind KADRIS 4

Your long-term European technology partner

KADRIS 4 is the international platform and market brand of the Slovenian company ČETRТА POT.

For more than **35 years**, we have been designing, developing and manufacturing enterprise **Identity & Access Control, Time & Attendance and Workforce Management** solutions in Slovenia.

Unlike vendors focused on a single technology layer, we develop the complete ecosystem in-house from hardware and firmware to software, identity technologies and long-term technical support.

Why partner with KADRIS 4?

- **One Platform. One Manufacturer. One Accountability.**
One technology partner responsible for hardware, firmware, software, ID media and technical support.
- **European engineering & manufacturing**
Developed and manufactured in Slovenia with direct access to engineering expertise and product development.
- **Fast partner enablement**
Technical onboarding, product training and direct engineering support to accelerate successful implementations.
- **Long-term business opportunity**
Recurring software maintenance, platform expansion and long-term customer relationships.
- **Direct technical support**
Work directly with the engineers developing the platform – not through multiple technology vendors.
- **Scalable enterprise platform**
Expand from Access Control to Time & Attendance, Mobile Credentials and Workforce Management within one integrated ecosystem.

International Partnerships

Interested in becoming a KADRIS 4 partner or discussing business opportunities?

✉ hungary@kadrisk4.com

☎ +36 30 835 76 93

✉ prodaja@cetrtpot.si

☎ +386 4 280 66 60

🌐 www.cetrtpot.com/en

About ČETRТА POT

The Slovenian company behind the KADRIS 4 platform

For more than 35 years, ČETRТА POT has been developing and manufacturing enterprise Identity & Access Control, Time & Attendance and Workforce Management solutions for organisations across Europe.

ČETRТА POT d.o.o.

Founded	1990
Headquarters	Kranj, Slovenia
Experience	35+ Years
Customers	950+ Organisations
Core solutions	Enterprise Identity & Access Control Time & Attendance Workforce Management Payroll

Contact	ČETRТА POT d.o.o. Ljubljanska cesta 24D, 4000 Kranj, Slovenia T +386 4 280 66 60 E prodaja@cetrtpot.si W www.cetrtpot.com
----------------	--



SAP Certified
Integration with RISE with SAP S/4HANA Cloud



Partner

