KADRIS 4
RIS

Access Control

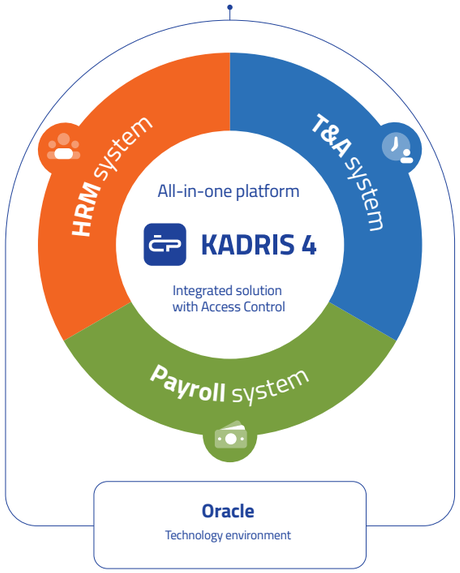
Advanced solutions for Technical Security

01

All-in-one KADRIS 4 platform – integrated solution with Access Control

The KADRIS 4 information system is a platform comprising business solutions for Human Capital Management, Time and Attendance, Technical Security and Payroll. It offers a complete solution with seamlessly integrated HRM, T&A and Payroll information systems. The Time and Attendance system supports digitized time and attendance management and includes Technical Security or Access Control. The Access Control component of the system has been on the market for more than three decades and is constantly evolving.

Business solutions for Human Capital Management, Time and Attendance, Technical Security and Payroll.



KEY FEATURES:

- Contactless identification,
- Easy to use,
- Enables you to use your smartphone to open doors (even in the absence of internet connection),
- Highest level of security and compliance with the requirements of SIST EN 60839-11-1:2013 (grades 3 and 4),
- Software in the cloud (subscription) or on-premise (purchase),
- Integral part of the KADRIS 4 unified platform – HRM ▪ T&A ▪ Payroll information system,
- Scalable according to client's needs,
- Compatible with older versions of the Access Control system,
- Agile deployment of new technologies to enhance security (e.g. MIFARE DESFire),
- Certified integration with alarm systems and other systems (e.g. SAP ERP system).

The advantage of the KADRIS 4 Access Control is, among other features, in-house development and production of Access Control components at the provider's premises in Slovenia, which means stable supply chain, servicing and upgrades. The provider has detailed knowledge of the equipment and can therefore advise the client on the design of the client's new system and ensure trouble-free implementation of extensions and upgrades. For clients who need a specific or bespoke solution, the software can be customized.

02 Technical Security or Access Control

Access Control systems basically allow you to secure your premises and control who can enter the building or access a particular room. They ensure employee safety and protect organization's assets and business information. Nevertheless, they can offer even more.

In addition to the basic functions, Access Control systems can support reception desk with visitor announcements and monitoring, security rounds management, electronic locking of employee lockers, key storage lockers, employee attendance records, room occupancy records, self-service payment machines (closed-loop payment) and several other functions.

Users identify themselves with their ID card or other means of identification, such as their smartphone. It is simpler for users to identify themselves throughout the system with a single ID medium, and it is important that this ID medium is secure, i.e. that the information it contains cannot be copied and that the exchange of this information between the system components is encrypted.

The KADRIS 4 system with Access Control supports such functions, and is integrated both internally and with external systems. Internal integration means that the system components covering specific business functions (HRM, Time and Attendance, Access Control, Payroll) operate as a single system. The Access Control system and the Time and Attendance system are linked especially tightly, as users use the same identification medium for both systems and the settings are shared between the systems. External integration means that the system connects to the client's IT environment in various ways, including via Web Service.

In response to the changes that the COVID-19 pandemic has pushed the world into, KADRIS 4 Access Control provides contactless access using NFC (Android) or BLE (iOS) technology. Moreover, KADRIS 4 Access Control supports a hybrid way of employee engagement, i.e. partly from home and partly on-site, with accurate attendance data available to the management.

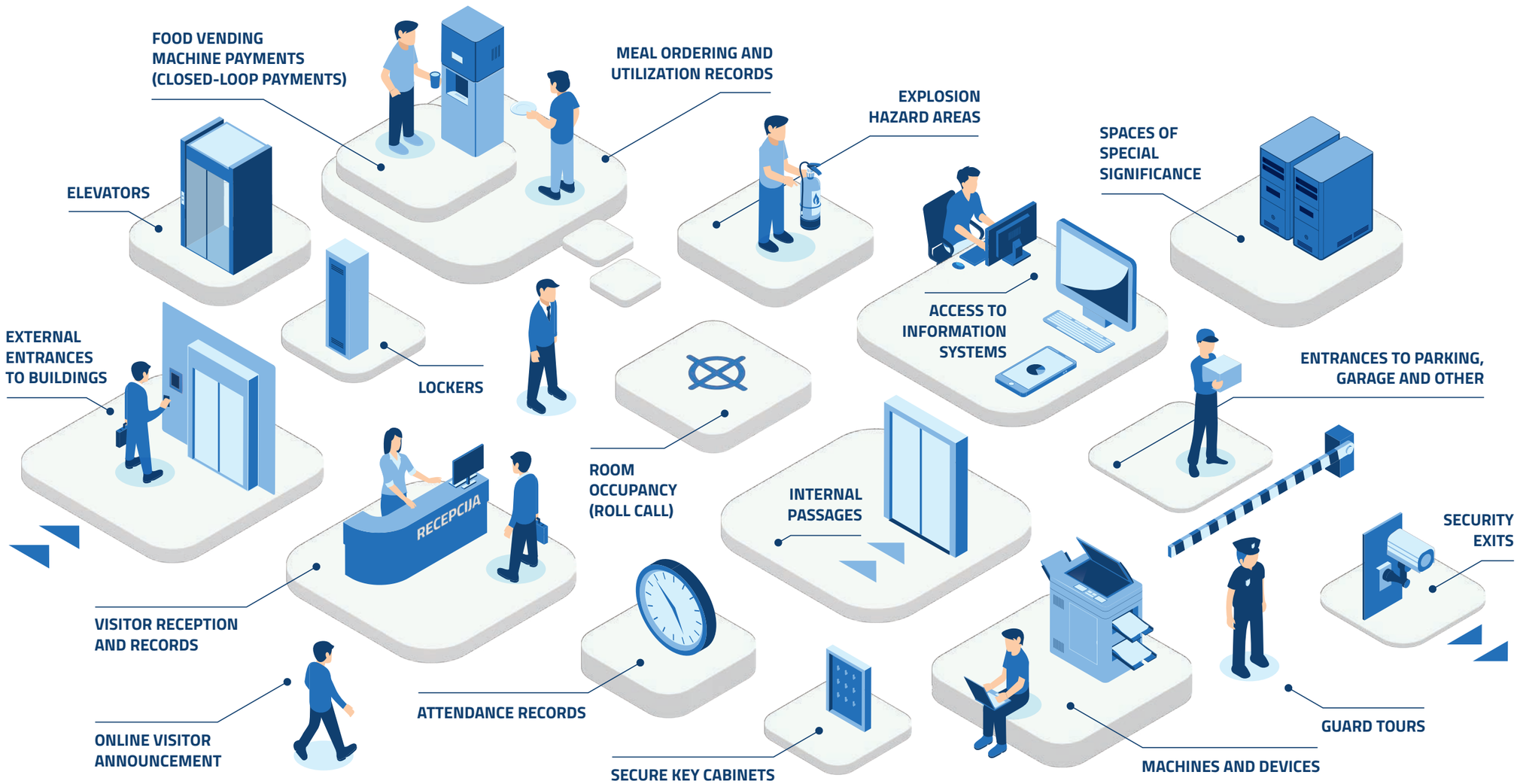
TX-600
Time and Attendance terminal

CMX5 reader

CMX3 reader

03 **Access Control** areas of application

KADRIS 4 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 Access Control functionalities

KADRIS 4 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

Although Time and Attendance is a different functionality than Access Control, the two are seamlessly linked in KADRIS 4, and Access Control is a part of the Time and Attendance component. Users use the same identification medium for both systems and the data on users and their access rights are common to both, which means that no duplication of effort is required when changes are made, and the changes are less prone to error. The Time and Attendance terminal may be used to open doors, as well, in some cases.

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 entails the control of access to information systems and computers by means of a smart ID medium and personal password. To implement Logical Access Control, appropriate ID media, readers, software and Public Key Infrastructure (PKI) are required. The optimum solution of ensuring security in an information system is the combination of a physical ID medium (e.g. card), a single media database, and Single Sign-on System (SSO). Users need to enhance their diligence with regard to ID card, as the user cannot use their computer without it, and upon exiting the office, the user must take it with them, which effects in locking the system (automatic log off). In addition, sharing of cards and passwords is inherently prevented.

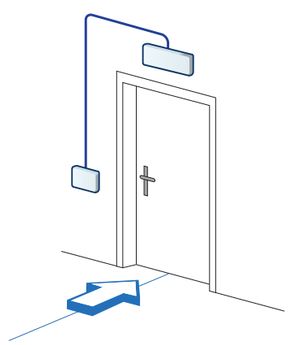
05 Access Control layouts

An Access Control system 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.

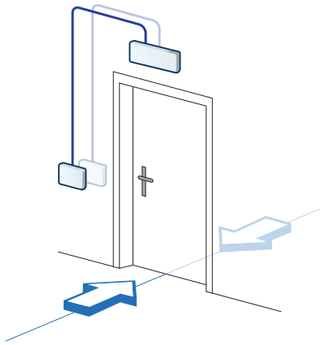
Depending on the client's needs, the Access Control system can be designed as a simple system or as a system with multiple functionalities and a high level of security. Security level is determined by hardware topology, i.e., the physical implementation of connections between system components. Independently 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.



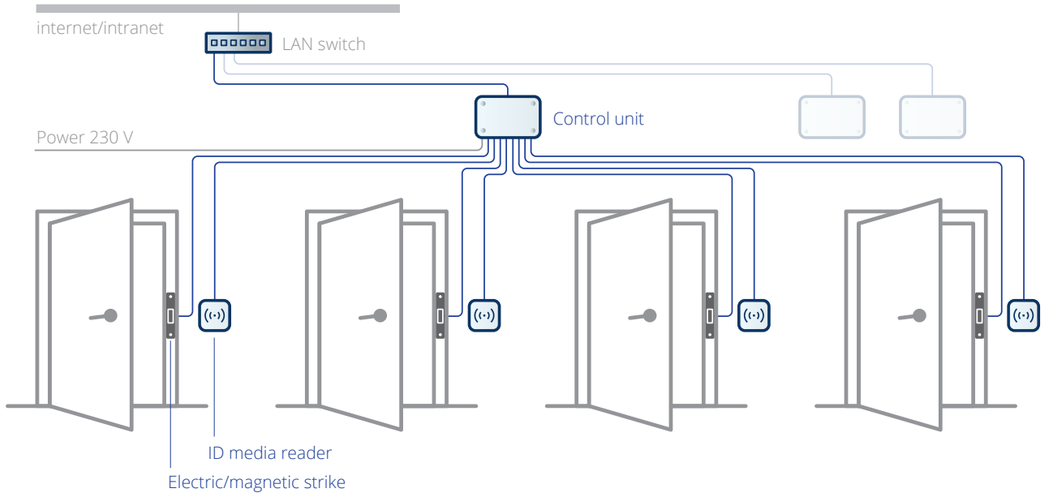
Two-way Access Control is used in cases where access from both sides of a door needs to be controlled (e.g. passage between corridors). Evacuation route standards must be adhered to in such context.

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.

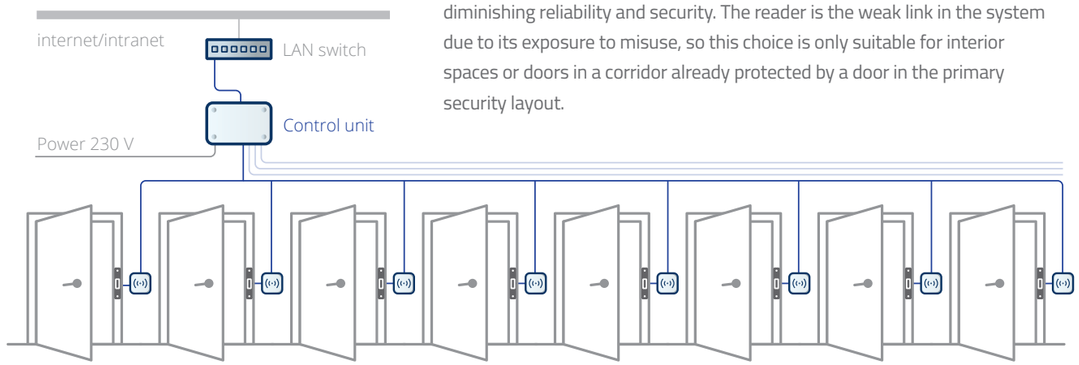
Primary security choice – the highest level of security

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.

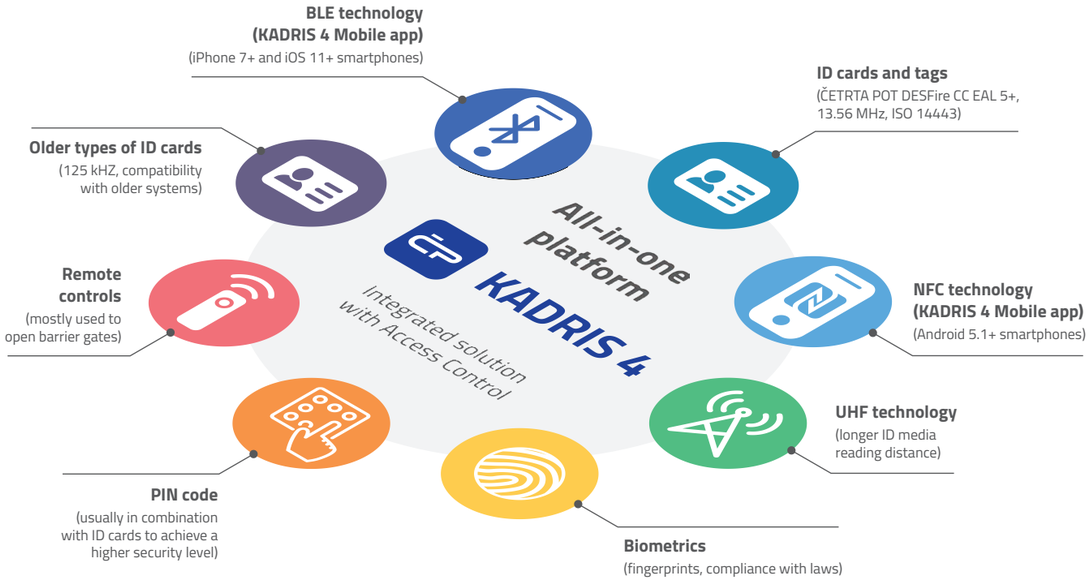


06 Identification media

KADRIS 4 Access Control enables identification by advanced means of identification, the common denominator of which is superior security and reliability. In order to provide system compatibility with older types of equipment, the identification is also possible using certain elements that are no longer in use today, but still provide a relatively high level of security.

Technologies compatible with KADRIS 4 Access Control:

- ID cards (ČETRTA POT DESFire CC EAL 5+, 13.56 MHz, ISO 14443),
- NFC (door opening and identification with Android 5.1+ smartphones),
- Bluetooth BLE (door opening and identification with iPhone 7+ and iOS 11+ smartphones),
- 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).



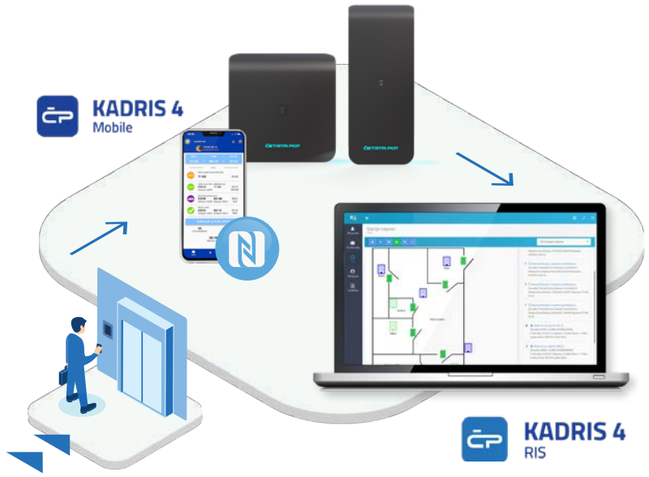
Advantages of a single identification card

- Instead of having a multitude of cards, users only use one card to register their working hours and enter the premises.
- Unified management of Time and Attendance and Access Control cards (issue, revocation, replacement, security checks).
- As card management is unified, changes are made at one point and apply throughout the system (no double entry is needed, and thus any changes are less prone to error).

ČETRTA POT DESFire EV3 ID card

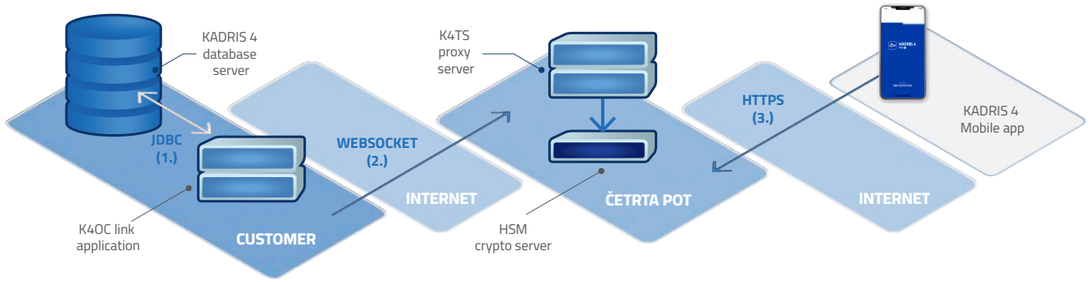
The most common and reliable ID medium is still the card. One of the most technologically sophisticated and secure contactless cards currently on the market is the ČETRTA POT DESFire EV3 from the NXP's MIFARE DESFire smartcard portfolio. Its design allows for greater operational distance and features improved transaction speed. It offers the highest level of data protection and privacy assurance (Common Criteria EAL 5+ certificate). It supports a wide choice of open cryptographic algorithms based on DES, 2K3DES, 3K3DES or AES encryption. It is made according to the established ID card standards (ISO 14443 and ISO 7816) and is compatible with existing MIFARE infrastructure.

KADRIS 4 Mobile app



The most important trend in Access Control is the use of smartphones to open doors. Dedicated mobile apps have taken over the role of an ID medium and became part of the overall security system. The portfolio of identification methods in the context of Access Control has therefore been supplemented by the KADRIS 4 Mobile app, which runs on NFC-enabled Android and BLE-enabled iOS systems. The advantage of the KADRIS 4 Mobile app is that it operates even in the absence of internet or mobile network. When the connection is reestablished, the data is automatically transferred to 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 New in our product line

SECURITY GRADE 3
SIST EN 60839-11-1:2013
CERTIFIED
II
Environmental Class

SECURITY GRADE 4
SIST EN 60839-11-1:2013
CERTIFIED
II
Environmental Class

OnPrem **Cloud** (ISO-27018) **SaaS** **ACaaS**

CMX3 reader **CMX5 reader** **TX-600 Time and Attendance terminal**

08 ID media readers

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:
- ID cards and fobs according to ISO 14443 (ČETRTA POT DESFire), ISO 15693 and NFC,
- smartphones as ID media: Android with NFC, iPhone with BLE,
- reading distance: up to 80 mm.

Built-in security standards:
- ID media tokenization,
- eSE (embedded Secure Element) for encoding/decoding and security key storage,
- AES for ID media authentication and encryption,
- AES for encrypted communication with the control unit.

Technical data:
- operating frequency: 13.56 MHz, Bluetooth 2.4 GHz,
- communication: serial communication RS485-2v, optional USB, communication protocols: AIRg2, 4WX,
- identification indicators: beeper, RGB LED strip on three sides,
- dimensions: CMX3: 90×90×15 mm, CMX5: 145×58×15 mm,
- mounting: CMX3: flush-mounted on the wall (60 mm socket), 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 %,
- IP rating: IP65.

Compliance with standards:
- CE, in accordance with Directive 2014/53/EU (Radio Equipment Directive),
- SIST EN 60839-11-1 certificate for Access Control systems.

Options:
- H ... high frequency of the reader supported, 13.56 MHz,
- M ... NFC and BLE enabled smartphones supported.

TX-600 Time and Attendance terminal

(Preliminary information)

Main characteristics:
- powerful processing unit; 64-bit processor with 4 cores ARM 1.8 GHz,
- Linux operating system,
- color LCD display 7” 16:10 horizontal, resolution 1280×800, brightness 400 nit, contrast 800:1,
- touch screen, capacitive,
- ID media reader,
- light and sound indicator,
- camera (optional),
- real-time clock with synchronization with time servers using the NTP protocol.

Supported ID media:
- ID cards and fobs according to ISO 14443 (ČETRTA POT DESFire), ISO 15693 and NFC,
- smartphones as ID media: Android with NFC,
- reading distance: up to 60 mm.

Integrated security standards:
- AES for ID media authentication and encryption,
- TLS (https) for communication with server.

Technical data:
- operating frequency: 13.56 MHz, Bluetooth 2.4 GHz,
- communication: LAN network 1 GBps, WiFi optional,
- communication protocol: AIRg2, 4 WX (other protocols optional),
- dimensions: 178×185×28 mm (no wall mounting bracket),
- mounting: on the wall with enclosed metal bracket, slanted,
- power supply: Ethernet cable according to PoE standard,
- operating temperature: –10 °C to +60 °C, relative humidity: 5–95 %,
- IP rating: IP44, IP65 optional.

Compliance with standards:
- CE, in accordance with Directive 2014/53/EU (Radio Equipment Directive).

Options:
- C ... built-in camera for additional identification monitoring,
- W ... built-in WiFi and Bluetooth,
- IP ... IP65 rating.

CM03/TP reader

CM03SF reader

CM03FP reader

Supported ID media:
- ID cards and fobs according to ISO 14443 (ČETRTA POT DESFire), ISO 15693 and NFC,
- ID cards and fobs 125 kHz ASK (RO-EM41xx, RW-HITAG, ...),
- smartphones as ID media: Android with NFC,
- reading distance: up to 100 mm.

Integrated security standards:
- ID media tokenization,
- 2 SAM modules (optional) for encoding/decoding and security key storage,
- AES for ID media authentication and encryption,
- AES for encrypted communication with the control unit.

Technical data:
- operating frequency: 13.56 MHz (option H), 125 kHz (option L),
- communication: serial communication RS 485 and USB, communication protocols: AIRg2, 4WX,
- identification indicators: beeper, RGB LED light,
- dimensions: 80×80×25 mm,
- mounting: surface-mounted on a non-metallic surface,
- power supply: 7-12 V DC, 150 mA or USB 5V 200 mA,
- operating temperature: –10 °C to +60 °C, relative humidity: 5–95 %,
- IP rating: IP44.

Biometrics optional (FP):
- built-in fingerprint reader,
- verification: card + fingerprint or identification: fingerprint only,
- biometric sample stored in the reader.

Please note: each reader must individually be approved by Information Commissioner of the Republic of Slovenia.

Compliance with standards:
- CE, in accordance with Directive 2014/53/EU (Radio Equipment Directive)
- SIST EN 60839-11-1 certificate for Access Control systems

Options:
- H ... high frequency of the reader supported, 13.56 MHz,
- L ... low frequency of the reader supported, 125 kHz,
- HL ... high and low frequency supported,
- SF ... built-in keypad,
- FP ... built-in fingerprint reader,
- PRT ... USB communication.

CM500 UHF reader

Technical data:
- 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

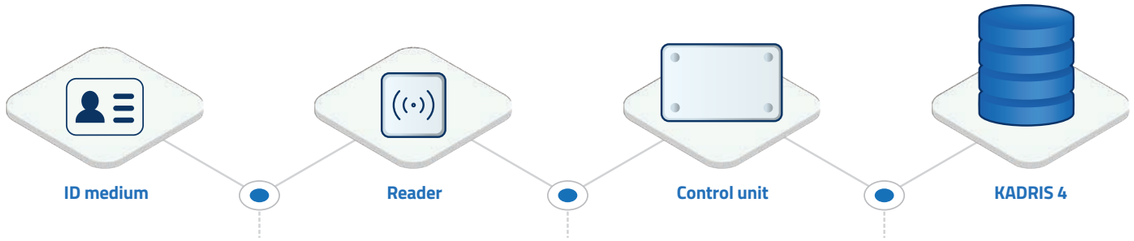
Aperio products are designed to control passage at the location of the door. Communication to the VT-500 control unit is wireless via a module that is wired to the control unit. The product is fully integrated in the KADRIS 4 Access Control. Aperio is suitable for gates where, due to various factors, 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 (ČETRTA POT DESFire),
- reading distance: up to 30 mm.

09 Secure communication between system components

The KADRIS 4 information system 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 Control unit

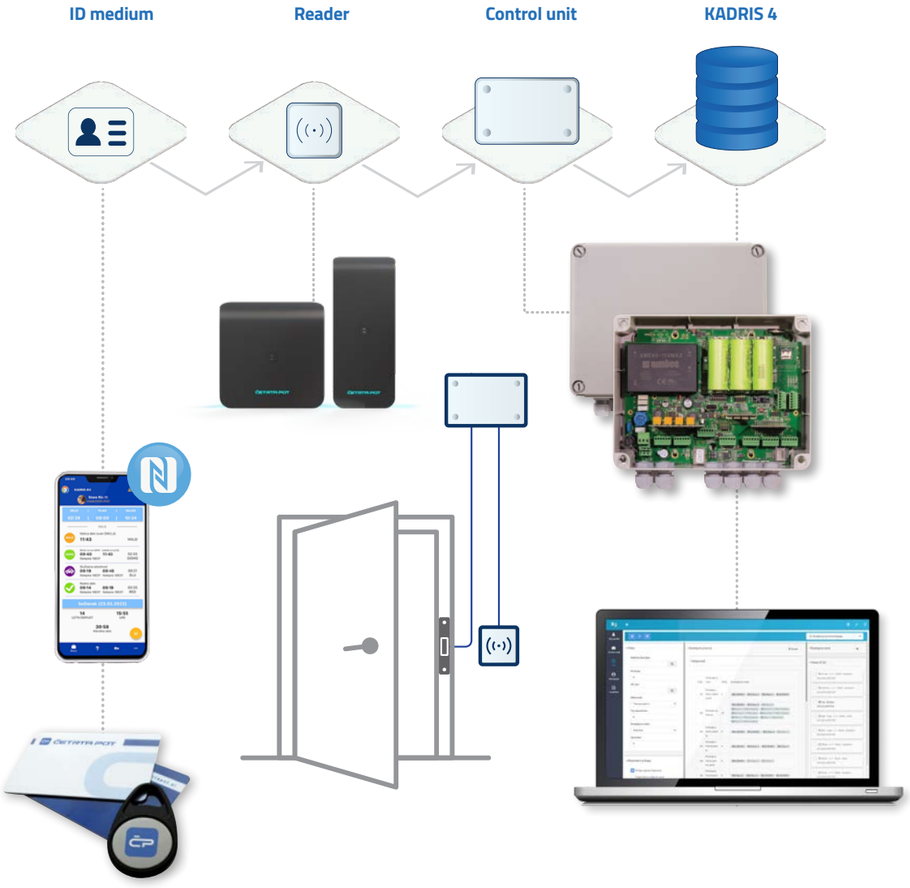
SECURITY GRADE 2 SIST EN 60839-11-1:2013 CERTIFIED II Environmental Class

SECURITY GRADE 3 SIST EN 60839-11-1:2013 CERTIFIED II Environmental Class

SECURITY GRADE 4 SIST EN 60839-11-1:2013 CERTIFIED II Environmental Class

Control unit is the core of the 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 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.



VT-500 control unit

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 ČETRTA 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,
- 4 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 SIST EN 50133-1 (grade 3, category B), and SIST 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 SIST EN 60839-11-2013 security standard

Since 2022, KADRIS 4 Access Control has been certified according to the SIST 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 SIST 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.

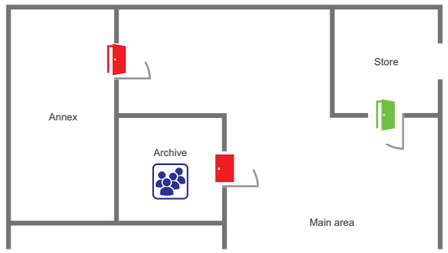
For each set of requirements, the standard specifies the procedures to be followed by the certification authority in verifying system compliance.

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,
- CMX3, CMX5 and CM03/TP ID media readers.

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. This kind of integrated solution is our competitive advantage, making us stand out on the Access Control market in Slovenia and the wider region.

Example of graphical representation of 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 ČETRTA POT

ČETRTA POT is the leading Slovenian IT company specializing in the development and implementation of business solutions and the development and production of hardware for workplace digitization. Our solutions support Human Capital Management, Time and Attendance, Technical Security and Payroll.

We are the only software house in Slovenia that digitizes workplaces on a common platform in compliance with labor laws and regulations. Cooperation with world-leading global providers such as Oracle and Microsoft allows us to offer our clients the choice of digitizing their workplaces with the KADRIS 4 solution (Oracle technology environment) or SPIN D365 (MS Dynamics 365 Business Central technology environment).

In-house development, sophisticated product design and positive customer experience enable us to respond to business challenges and develop solutions tailored to market needs. Our business solutions are used by more than 950 organizations of all sizes from all industries in the private and public sectors. All products (software and hardware) are compliant with labor legislation, certified to the highest security and quality standards and compatible with existing systems.

ČETRTA POT brings together a team of more than 110 reliable, efficient, professionally qualified and competent individuals. Together, we create an environment and work culture where we are united by shared values such as knowledge appreciation, quality of work, interdepartmental collaboration and commitment to fulfill agreements.

VISION and MISSION

Our vision is to understand our clients' needs and digitize their workplaces.
Our mission is to identify pain points, find solutions and offer a choice of high-quality and intuitive business solutions on a variety of technology platforms.

30+
YEARS OF EXPERIENCE

110+
EMPLOYEES

100 %
IN-HOUSE SOFTWARE DEVELOPMENT

100 %
IN-HOUSE DEVELOPMENT AND PRODUCTION OF HARDWARE

950+
CLIENTS or IMPLEMENTATIONS

10+
CERTIFICATES AND PARTNERSHIPS

ČETRTA POT®

Your PATH to a digital workplace

ČETRTA POT, d.o.o., KRANJ
Planina 3 | 4000 Kranj | Slovenija
T: +386 4 280 66 60
F: +386 4 280 66 18
E: prodaja@cetrtapot.si

www.cetrtapot.si

ISO 9001 ISO 27001 ISO 22010 BUREAU VERITAS Certification

SLOVENSKI PROIZVOD SLOVENSKA KAKOVOST SLOVENIAN QUALITY

SAP® Certified Integration with SAP Applications

NXP founded by Philips

ORACLE Partner

Powered by ORACLE Cloud

September 2022, ČETRTA POT, d.o.o., Kranj. All rights reserved. Images are used for illustration purposes only.
Photo: Gorazd Kavčič, ČETRTA POT archive, iStockphoto.