BOSCH ACCESS CONTROL SYSTEMS

Maximize openness, availability and scalability

BOSCH

Access Control Systems - Content

- Overview
- Bosch Access Control Products
- Integrations
- System design examples and how to order guide
- Internal information

ACCESS CONTROL SYSTEMS OVERVIEW

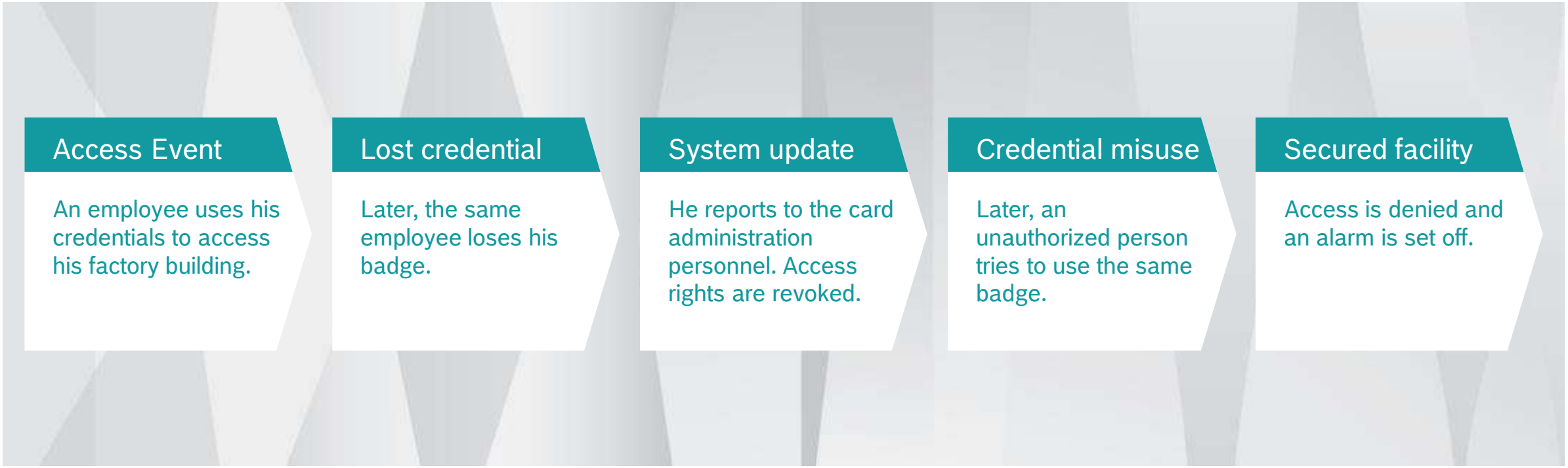
BOSCH

Access Control Systems
Overview

Flexible access control systems allow workers to get on with their jobs, while protecting staff from uninvited guests and businesses from property and information theft. We offer integrated systems for many different applications.

Access Control Systems
Principle

Access credentials can be updated in real-time to ensure only the right people get in and intruders are kept out, even in cases of user error.



Access Control Systems
Solution benefits

- A complete Bosch access control solution covering software, controllers and a variety of readers and credentials
- Ideal for mid-sized to large applications
- Comprehensive system with many features and integration with Bosch solutions as well as third-party products

Your advantages

- Reliable and effective security
- Future-proof system that expands with your needs
- Flexible installation options thanks to the modular concept

Today’s challenges

Why do you need an access control system?

Increasing demand for security

Growing need to restrict access to buildings and areas

Mechanical access systems are prone to misuse

More flexible working time models

Why is access control so important?

Typical applications

Access control is one of the most important subsystems in a security installation

Access in a company

⇨ **Structured Access**

Protect secure areas

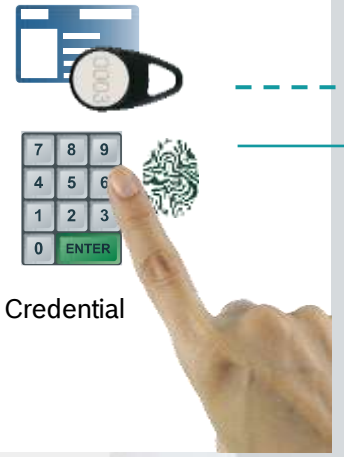
⇨ **Security**

Unlock doors in the case of an emergency

⇨ **Safety**

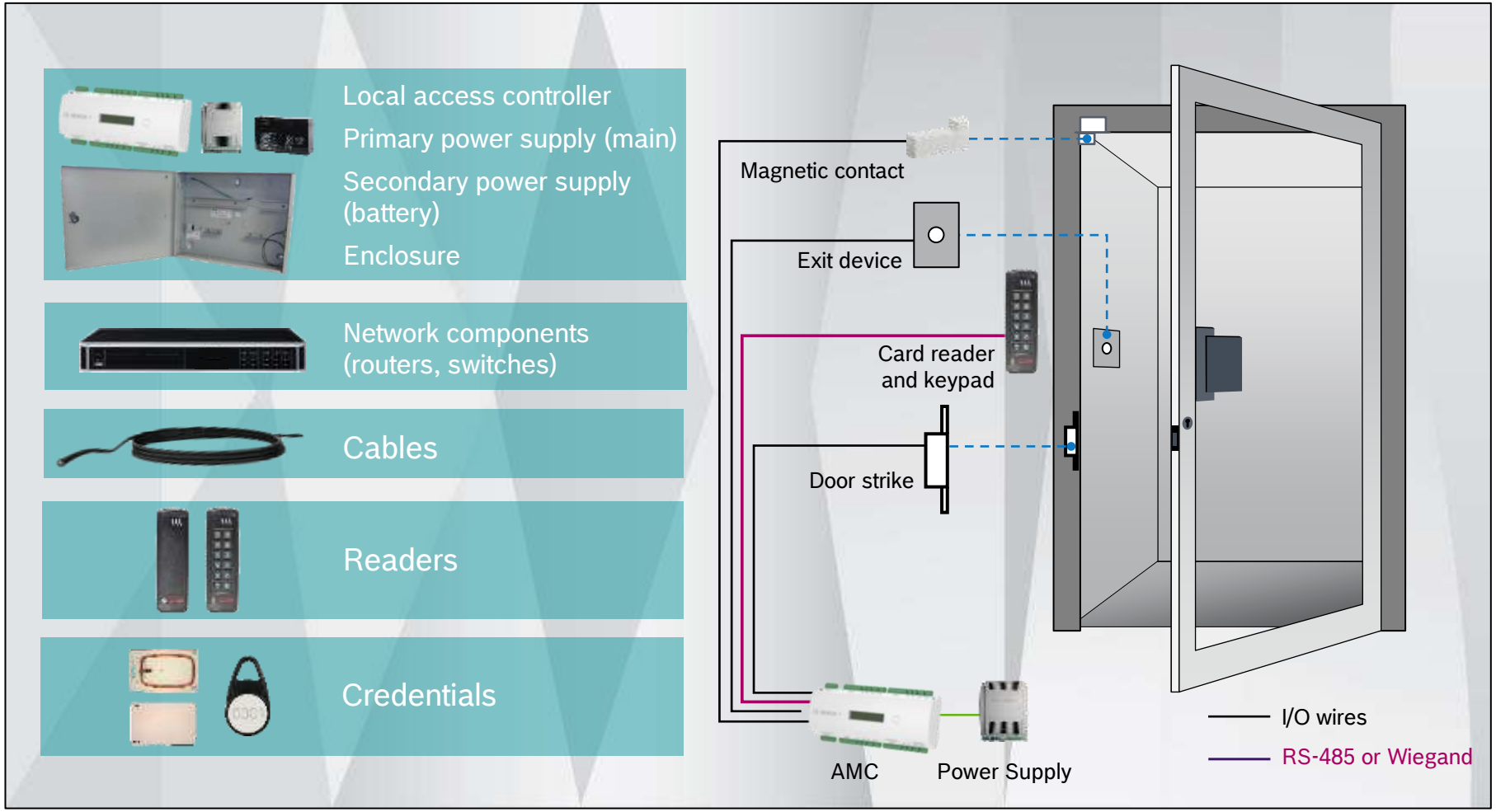
Credentials and readers

New to access control? – This is how it works in basic terms

	Identification	Interface	Decision	Operation
Component	 Credential	 Reader	 Controller	 Server/Client
Function:	Via card, key-fob, pin, biometric data	Via card reader, keypad, display or biometric reader	Interface between server/reader to grant/deny access	System operation, configuration and data-base management

Access control basics

Main components of an access control system



An Access Control system might be extended with several other items:

- Magnetic lock
- Door Closer (draw back mechanism)
- Long range readers and active cards (car park)
- Barriers
- Inductive loops (car park)
- Weight measuring/scaling (cars, trucks, persons)
- Infrared beams (at speed gates at airports, at barriers, etc.)
- Cameras
- …

BOSCH ACCESS CONTROL PRODUCTS

SOFTWARE

BOSCH

Our Access Control Solutions

From medium to large scale projects

- **BIS Access Engine (BIS-ACE)** is an ideal solution for high-end integrated projects e.g. airports, transport, stadiums,...
- **Access Management System (AMS)** is the suitable software for medium- to large-sized projects which need high scalability of cardholders and doors such as retail or office buildings

Overview of the Bosch access control products
Software

Building Integration System (BIS) with integrated Access Engine (ACE)

Access Management System (AMS)

Access Management System (AMS) at a glance

What is it?

Access control software for commercial buildings, retail, healthcare and education

Support of up to 400,000 cardholders, up to 10,000 doors, up to 40 workstation clients and up to 400 divisions

Highest resilience thanks to 3-tier architecture

Integration with BVMS and third-party video management systems

Integration with B and G Series Intrusion Control Panels

Access Management System

Intuitive graphical user interface (GUI) for easy operation

- Dark GUI to reduce operator fatigue
- Icons presented in a simple and easy to understand way
- Color scheme aligned with BVMS GUI to make the operation as smooth as possible when using both systems
- User-friendly alarm concept:
  - New alarms slide in from the side and rank themselves in the correct position in the alarm list according to their priority
  - Initial flashing of an alarm icon when it is raised, statically highlighted after a few seconds to prevent confusion
- Disabling of irrelevant commands for better UX:
  - Only relevant commands can be executed
  - Irrelevant commands are shown in grey

Access Management System

Easy-to-use map view for comprehensive overview

- Building and floor plans are easily imported in JPG/PNG format
- Intuitive icon and color scheme provide clear situational awareness
- All devices (readers, doors, intrusion panels and points) are easily moved on the map via drag and drop for set-up
- Locations of events are indicated on the map when clicking on the event
- I/Os, intrusion detectors and defined access or intrusion areas are displayed with icons
- Entrances are monitored for quick reaction in the case of forced open or open too long

Access Management System

Swipe ticker for constant overview of access events

Shows access events:

- Over selected doors
- With direct link to map
- On free floating window

- Shows cardholder data and photo
- Shows reader offline states

- Prevents misuse of ID cards
- Validation / check of photo (i.e. whether the photo is too old)

Information shown when cardholder requested access:

Green check mark:
Access (granted and taken)

Yellow warning sign:
Authorized but did not enter

Red warning sign:
NOT authorized

Access Management System
AMS fully integrated into BVMS

Manual video verification

Management of access devices and events in BVMS

Search for cardholder activities and activities at entrances

Efficient operation of access and video within one GUI

Access Management System

B and G Series fully integrated into AMS

Central user management of all access and intrusion authorizations

Central alarm management

Easy and remote handling of intrusion events via AMS

Efficient operation of access and intrusion within one GUI

Access Management System

Threat level management for high level of safety on site

- Proactive preparation for various high and low threat situations
- Quick initiation of safety measures in the case of an imminent threat / emergency
- Behavior of all doors changed within seconds

Threat levels are defined and configured by the user to change the behavior of all doors with just one click

- Possible high threat levels: attack, fire
- Possible low threat levels: sports event, family day in a company, parents' evening in a school

Threat level state can be changed quickly and easily via three ways:

- Trigger threat level at the operator workstation
- Push emergency button
- Present specially configured "emergency card" to any reader

Access Management System

Threat level management for high level of safety on site

Up to 15 different threat levels can be configured with the following options:

Secured (Lockdown):

- Certain or all doors are completely blocked
- Access rights of cardholders are invalid for these doors

Open (Evacuation):

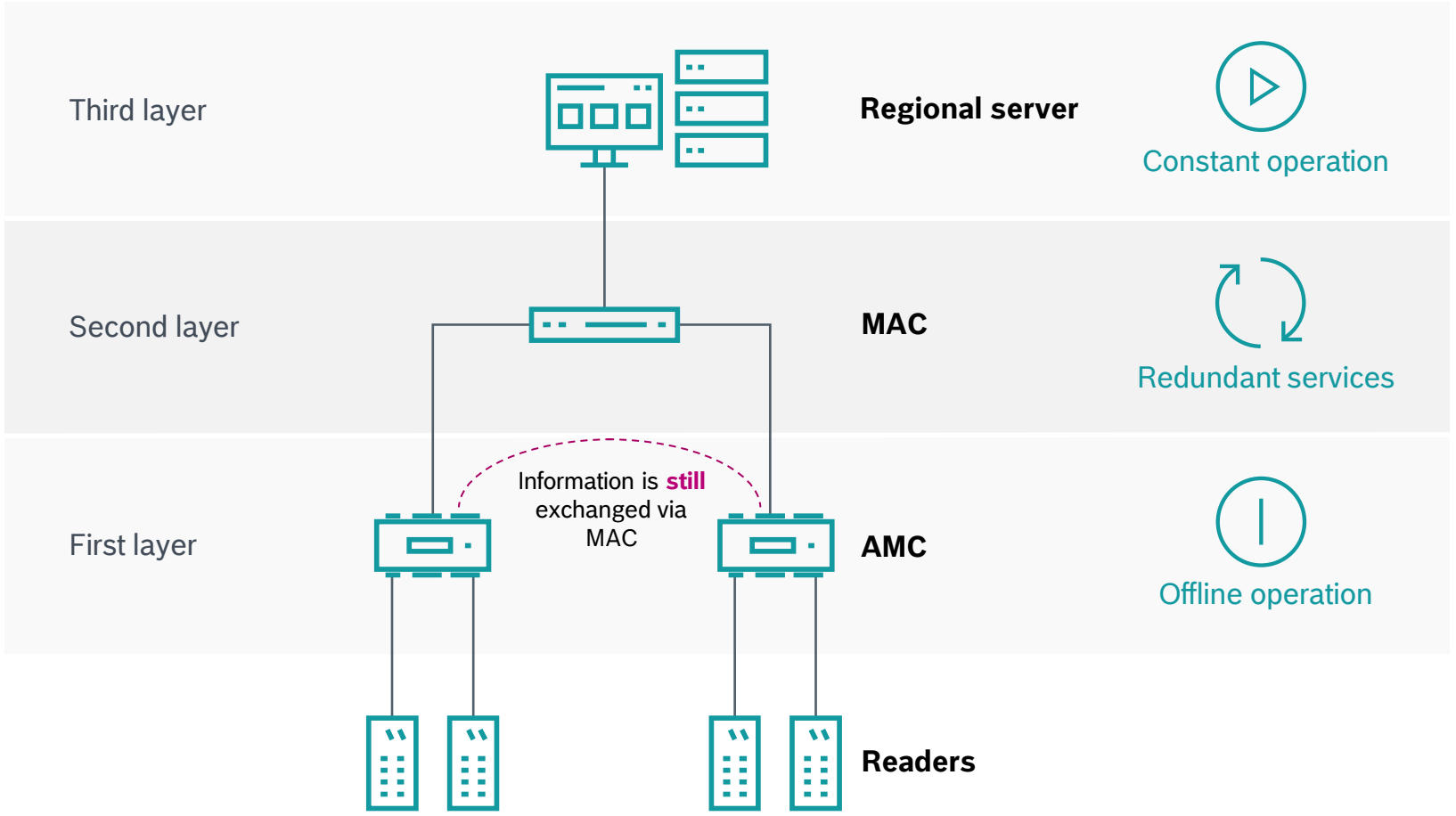
- Certain or all doors are completely unlocked
- No access credentials are needed to open the doors, allowing everybody to enter / leave without barriers

Customized (Controlled Lockdown / Lockout):

- Individual definition of each door's behavior
- Possibility to assign security levels (from 1 to 100) to cardholders and doors; in this case door opens only if the cardholder's profile is equal or higher than the door's current security level

Access Management System

Highest availability thanks to 3-tier architecture



- Highest availability thanks to three-tier architecture
- Additional third layer Master Access Controller (MAC) between the server and the controllers
- If the server fails, the controllers still communicate with each other and share relevant information through the MAC
- Consequence: even functionalities that include two or more readers such as anti-passback, access sequence check or guard tour can still be performed
- If the AMS server and the MAC are down, cardholders can still enter and leave because of the database which is saved directly on the AMCs. Thanks to this offline capability, it is possible to save millions of events even during down times.

Access Management System

AMS protects you from cyber crime and loss of personal data

Data Privacy:

- Strict access authorizations to personal data
- Only relevant data can be collected
- Print out consent to store personal data
- Data storage duration to comply with company policy

Data Security:

- Secure-by-design: encryption, authentication, certificates
- Secure-by-default: all security settings on high per default
- Principle of least knowledge: assign granular privileges for operators

Access Management System
Future-proof investment

Scalability within the different license types: Lite, Plus and Professional

High scalability to up to 400,000 cardholders, up to 10,000 doors and up to 400 divisions

AMS works across multiple sites and time zones, allowing you to expand the system according to your needs

When your security requirements grow, switch to full Building Integration System - keep the same hardware components

Overview of the Bosch access control products
Software

Building Integration System (BIS) with integrated Access Engine (ACE)

Access Management System (AMS)

BIS Access Engine (BIS-ACE) at a glance

What is it?

Access control software for large and integrated projects such as public buildings or transport

Support of up to 400,000 cardholders per server, up to 10,000 doors per server, up to 80 workplace clients per server and up to 400 divisions

Multi-server option for maximum scalability

Open interfaces to connect visitor management, carpark management, facility management and 3rd party systems

Highest availability through 3-tier-architecture in a single-server system and 4-tier-archtecture in a system with several servers

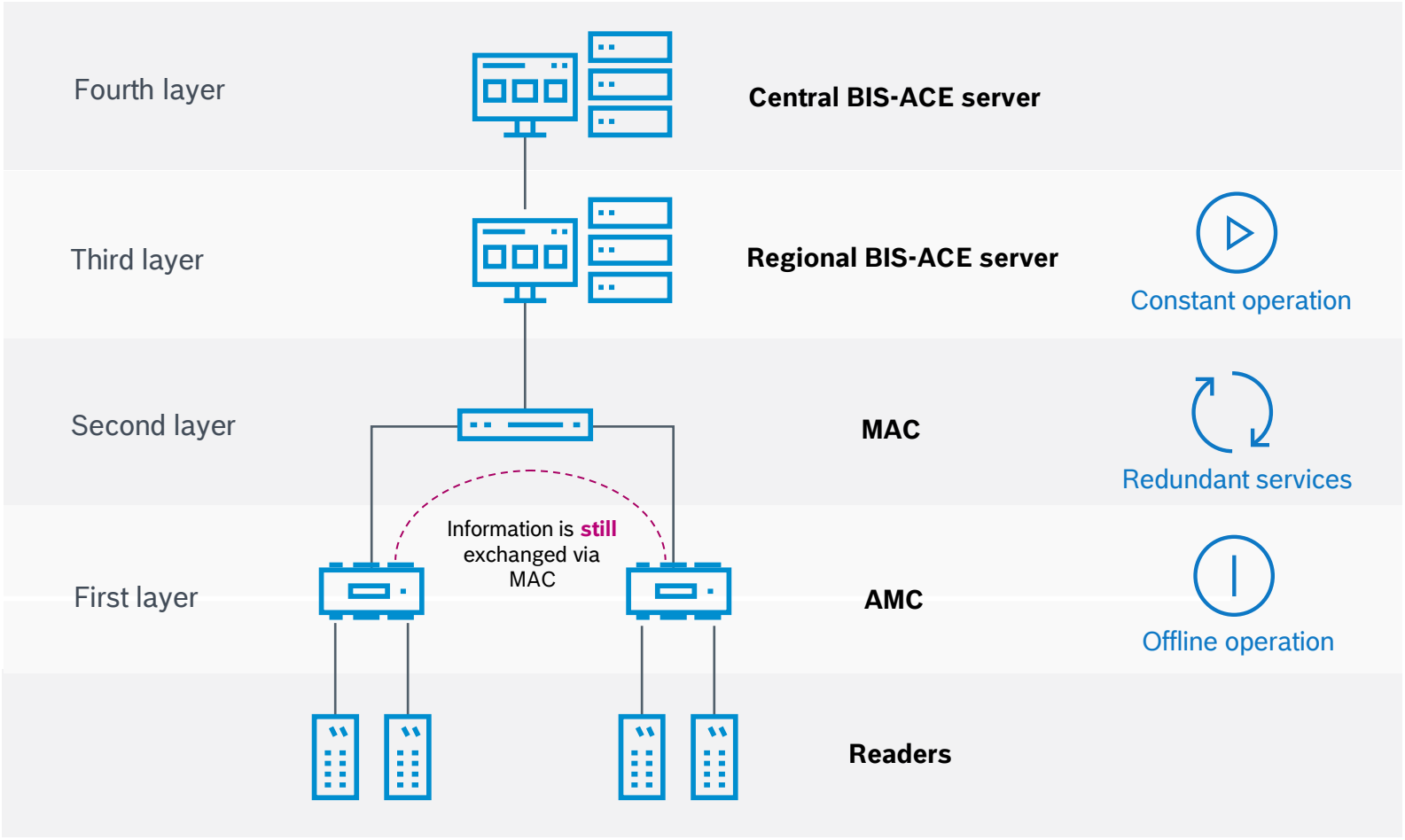
BIS Access Engine

Seamless integration of Bosch products

- Well-tested integrations of Bosch subsystems (Fire, Intrusion, Access, Video, PA/VA) and key technologies (IVA, VRM)
- **Continuous optimization of Bosch integration** through early access to latest developments
- Single interface for of all security systems domain for **efficient operation**
- Controlling, monitoring and investigation via one single point
- One-stop technical support covers all systems

BIS Access Engine

Highest availability thanks to 4-tier architecture



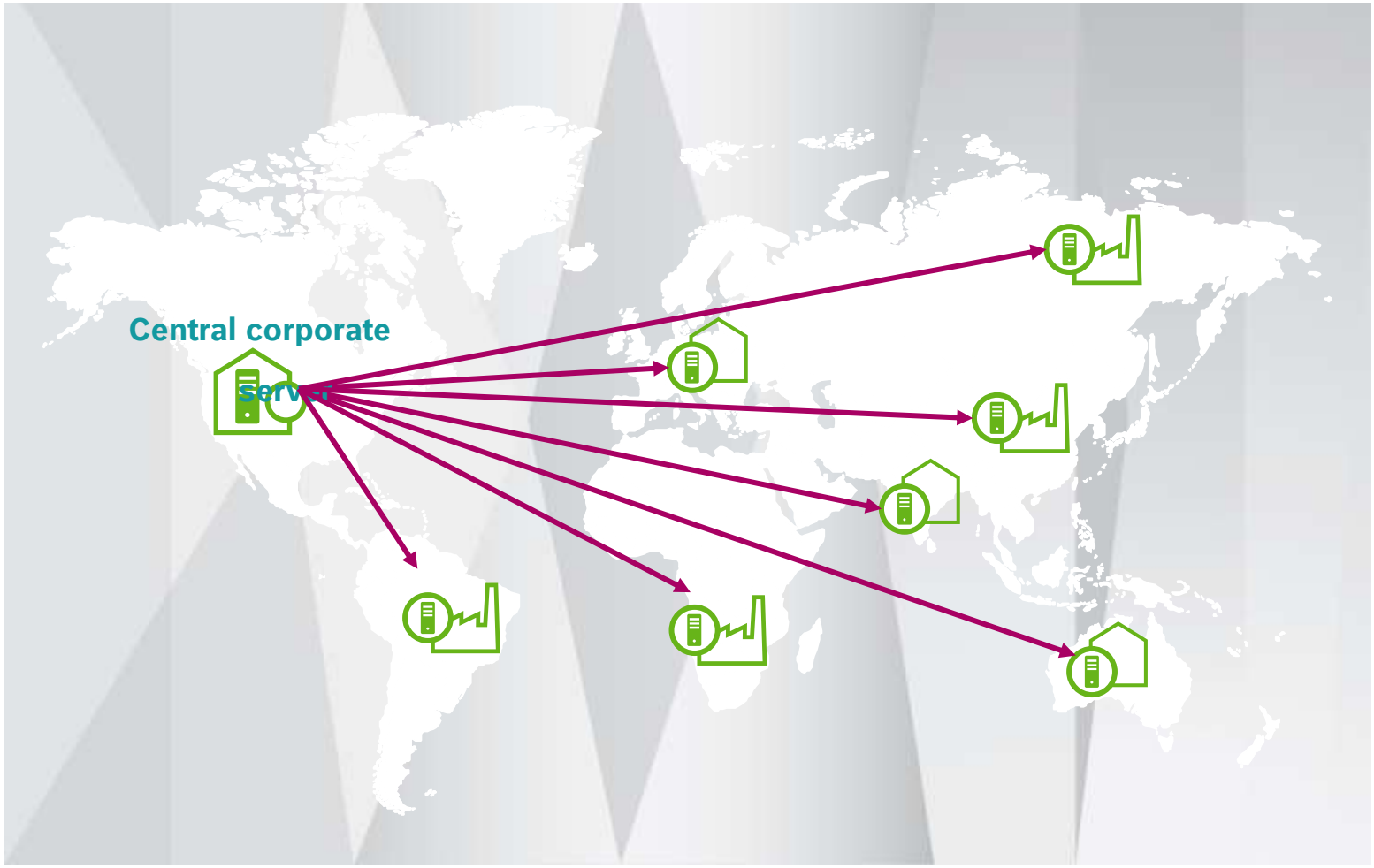
- Additional third layer Master Access Controller (MAC) between the server and the controllers
- If the server fails, the controllers still communicate with each other and share relevant information through the MAC
- Consequence: even functionalities that include two or more readers such as anti-passback, access sequence check or guard tour can still be performed
- If the BIS-ACE server and the MAC are down, cardholders can still enter and leave because of the AMCs' own database. Thanks to this offline capability, it is possible to save millions of events even during down times

Administrative tasks:

- Central server as fourth layer: central HR can enroll new employees globally
- Regional server as third layer: security managers define authorizations on a regional level

BIS Access Engine

Central Cardholder Management for distributed sites



BIS enables central access control across many sites from one single authorization server

Ideal for large enterprises with many different sites and in many different regions

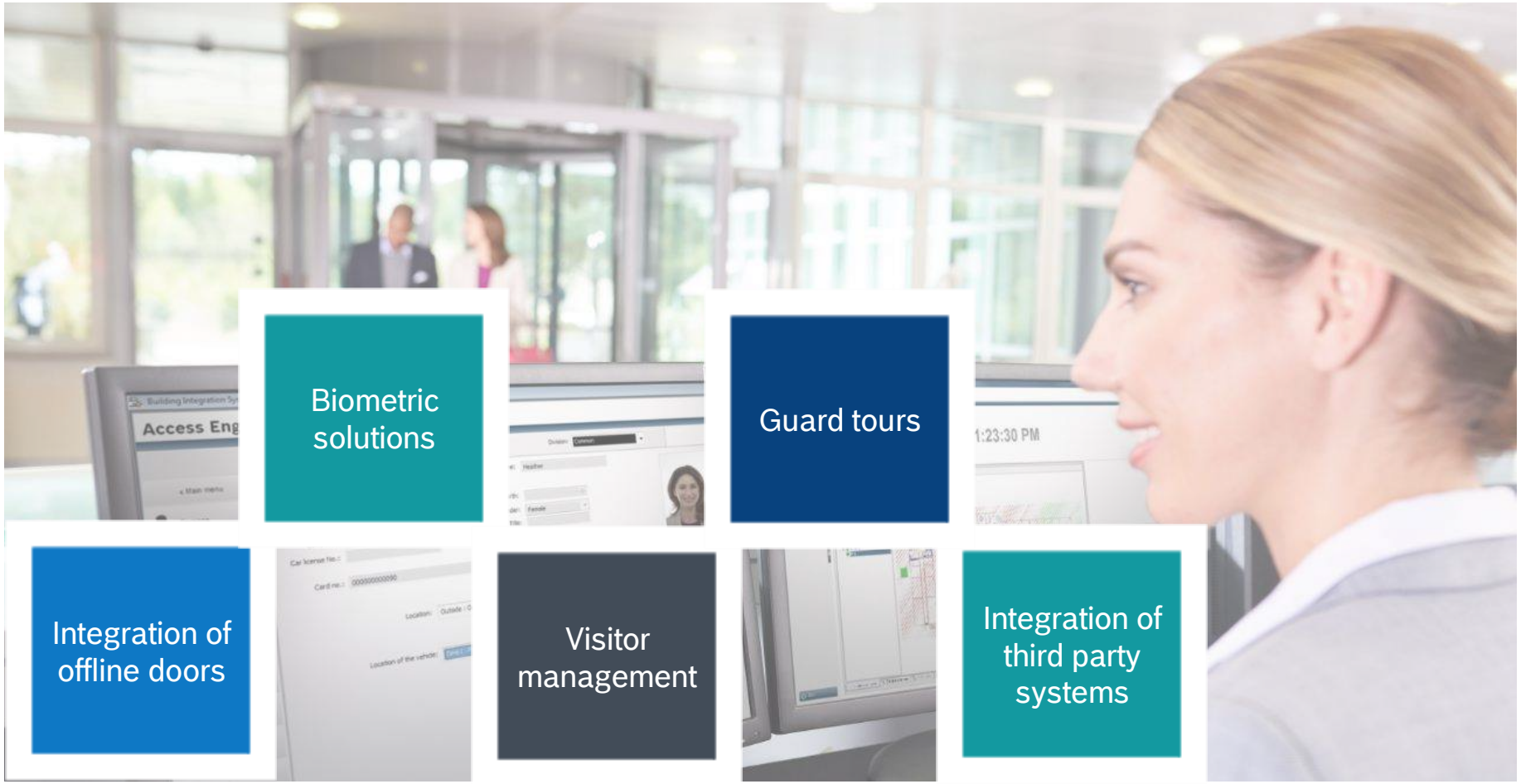
Manage global cardholders and authorizations from the central server and fulfill compliance regulations

Changes in cardholders and authorizations at the corporate server are replicated to all sites

Central alarm and event monitoring of all sites from the corporate server

BIS Access Engine
Multiple applications

A comprehensive system
with many functionalities
which is expandable
via SDK
and open interfaces



BIS Access Engine
Integration of third party systems

BIS/ACE offers full connectivity to 3rd party systems via “Classic OPC” for legacy systems or “OPC UA” for new integrations like building management or IoT, allowing for integrations of most diverse 3rd party systems to provide end-to-end solutions.

Direct integration via TCP/IP or USB

Existing third-party interfaces to:

- Key cabinets
- Card printer
- Webcam
- Signature scanner

Third-party develops interface based on Bosch API

- Identity management
- Visitor management
- Time & Attendance
- Additional check
- License plate recognition

Solution	Partner
Signature Scanner	signotec
Visitor management	HID, INSYRES
Intelligent anti-tailgating	fastcom
Time & Attendance	INSYRES, digital factors
Key and asset management	deister electronic, KEMAS
Wireless Handheld reader	CYPRESS
Wireless online locking system	Simons Voss technologies
Intercom	2N, JACQUES, VINGTOR STENTOFON
Building automation	OTIS, rexroth A Bosch Company

Have a look at the app notes at our website.

BIS Access Engine

BIS-ACE protects you from cyber crime and loss of personal data

Data security is optimized to fulfill data privacy regulations and to provide smooth business continuity

User accounts are protected against brute-force-attacks and misuse

BIS-ACE protects personal data in a secure SQL database

BIS-ACE supports encrypted communication between servers, clients, controllers and readers

BIS Access Engine
Future-proof investment

- High scalability to up to 400,000 cardholders per AMC, up to 10,000 doors per server and up to 400 divisions
- BIS-ACE works across multiple sites and time zones, allowing you to expand the system according to your needs
- Regular SW updates keep your system current with latest IT advances and data privacy regulations

HARDWARE

BOSCH

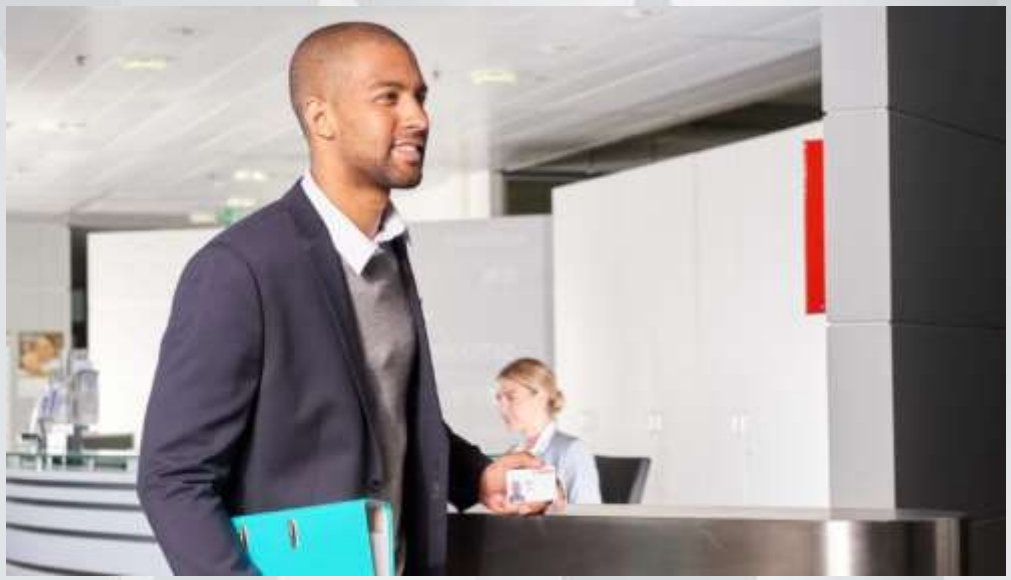
Overview of the Bosch access control products
Hardware

Access Modular Controller (AMC)

Readers & Cards

Access Modular Controller at a glance

What is it?



Support of RS-485 and Wiegand readers

Service display for initial configuration and trouble shooting

Easy installation and maintenance

Intelligent access manager for one to eight entrances, stores locally up to 400,000 cardholders

Event buffer memory for up to two million offline events

Continuously working thanks to offline capability

Access Modular Controller

Speed of installation

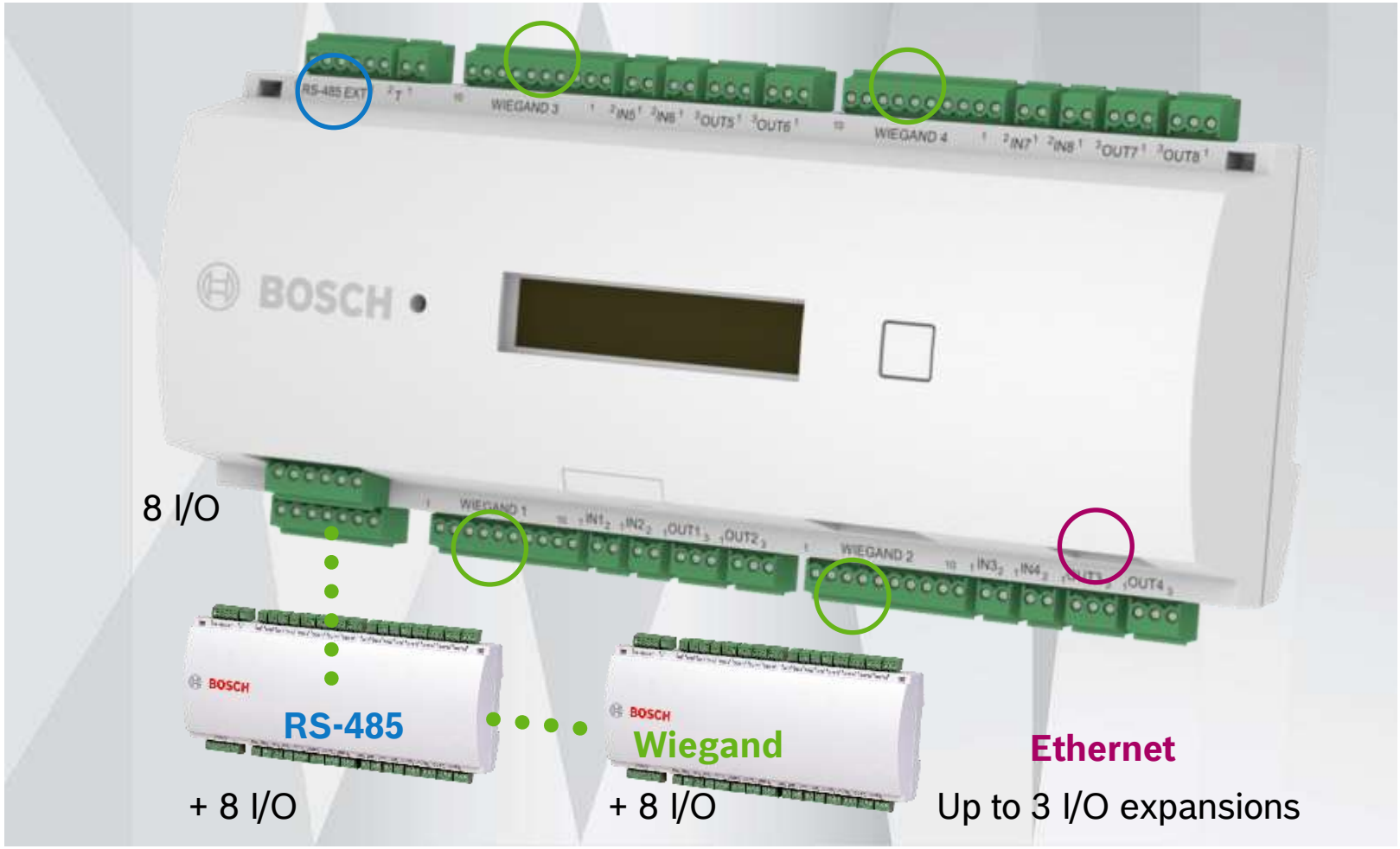
- Optimized design to reduce installation time and maintenance efforts:
  - service display for maintenance purposes and trouble shooting
  - modular concept for easy system planning and stocking
  - housing with removable terminal strips and DIN-rail mounting for fast installation
- Thanks to the fast and reliable Ethernet host interface, cardholder updates are realized within seconds

Access Modular Controller
Reliability

- The AMC is continuously working thanks to its offline capability and the supervised battery extensions
- Event buffer memory up to 2 million offline events to not lose any data
- Fast and secure operations thanks to own developed operating system
- 3 years warranty

Access Modular Controller

Future-proof investment



Flexible and scalable system

- ➔ Possibility to enlarge the system thanks to the modular expansion possibilities :
  - Expansion boards allow for I/O's expansions
  - Wiegand port expansion module
  - Support of RS-485 and Wiegand readers
- ➔ Protection of investment thanks to AMC's compatibility with different Bosch access SW products

Access Modular Controller

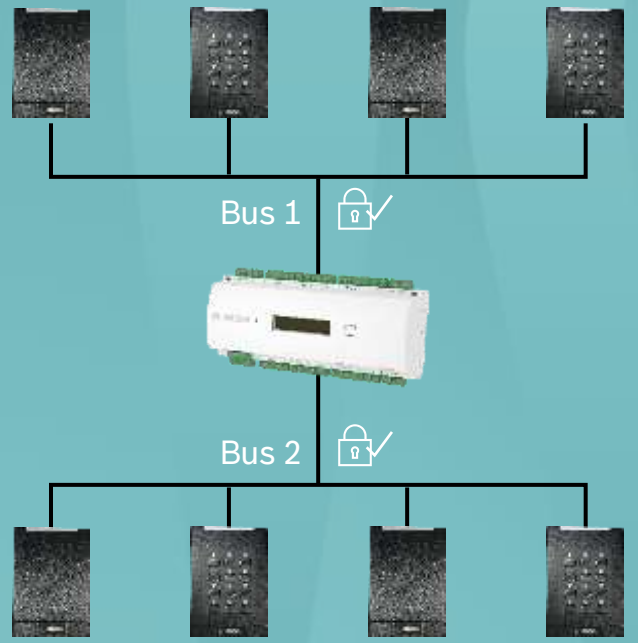
Connection of the card readers – Wiegand and RS-485 are possible

Wiegand:

4 devices can be connected to one AMC controller.
(8 with Bosch AMC Wiegand extension)

Defined point to point connection

RS-485:



8 devices can be connected in series to one AMC controller (see example)

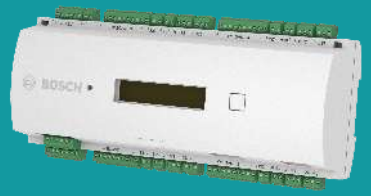
Flexible connection

Access Modular Controller

Wiegand and RS-485 – Functionalities and benefits

	Wiegand	RS-485 (OSDP)
Wide range of readers selection	✓	✓
Cable length	<150m	1200m
Conductors / Data transfer	Standardized (Bosch protocol using 10 wires)	Only 4 conductors for full functionality
Communication	Unidirectional	Bi-directional
Connectivity	Point to point	Serial bus
Installation costs	↗	↘
Encryption	No encrypted data interface	Encrypted data interface with OSDPv2
Flexibility	Low	High

Access Modular Controller
Product Family

Family	Controllers	Extensions	Power Supply Unit
			
	➔ Wiegand ➔ RS-485	➔ 16 Input / Output (3) ➔ Wiegand Extension (1)	➔ Support of 12 V/7 Ah, 12 V/14 Ah and 24 V/7 Ah batteries
Enclosures	**Single Controller**	**19“**	**Dual Controller**
			
	➔ Enclosure 1 Din rail (1 controller, 1 power supply)	➔ Panel 4 Din rails ➔ Panel 2 Din rails	➔ Enclosure 2 Din rails (2 controllers, 2 power supplies)

Overview of the Bosch access control products
Hardware

Access Modular Controller (AMC)

Readers & Cards

Credentials at a glance

What is it?

Enable access to a physical facility or area

Access card, token, tag, Personal Identification Number (PIN)

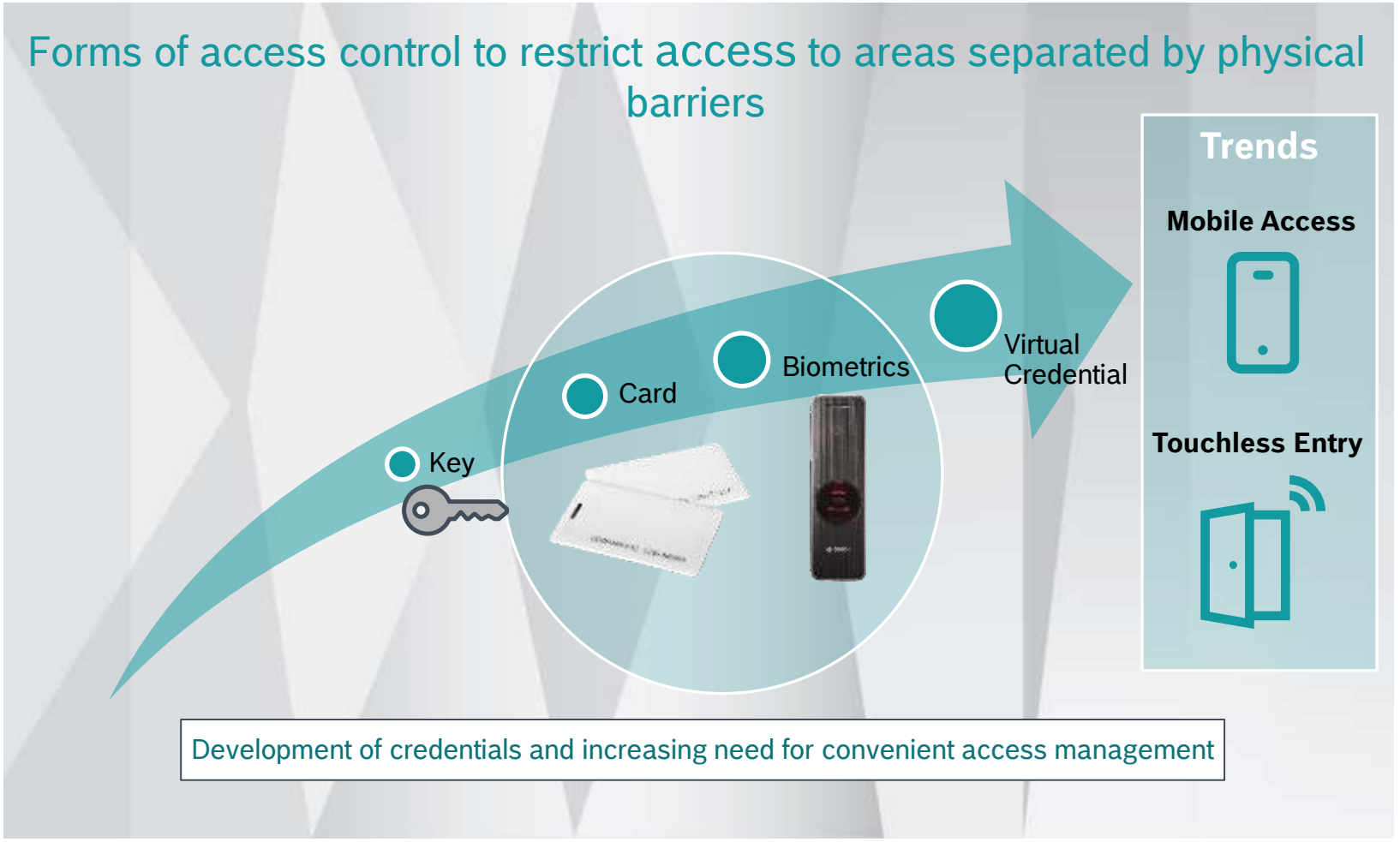
Biometric: finger print, hand geometry or iris pattern

Serve as an identification method for an individual

Are presented to a reader

Credentials

Trends of Credentials



Credential development

Keys
- Many identical physical keys and one key cylinder for one door
- No key diversification

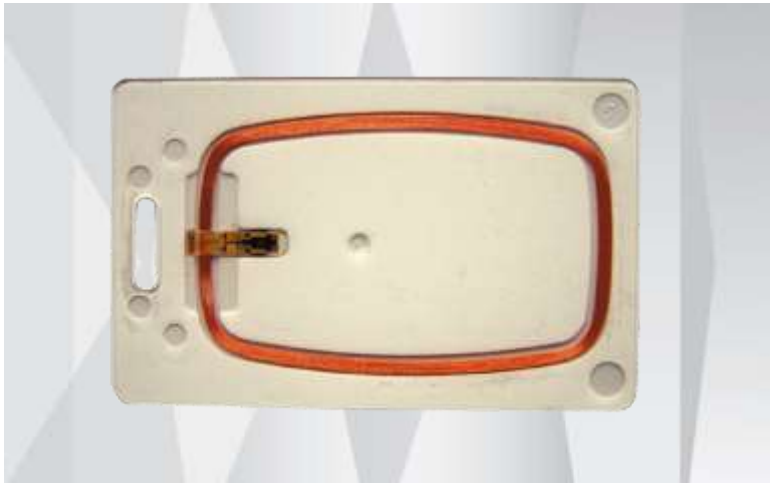
Cards
- A physical card, also known as access badge, can be used to gain entrance at an automated access control entry point
- Locks don't need to be changed when a card is lost and access can easily be given or denied to different users

Biometrics
- Often used as a second factor for authentication to add an additional layer of security
- Can also be used without any additional credentials for more convenience

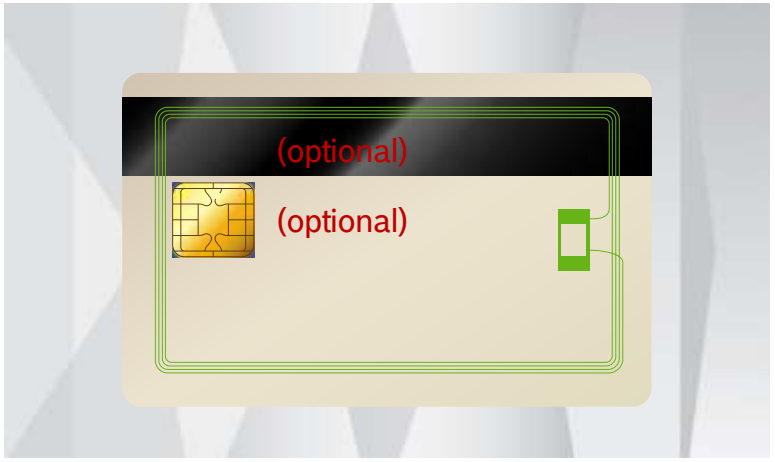
Virtual credentials
Credentials that can be offered via E-Mail / mobile app to any smart device (e.g. smartphone, tablet)

Credentials

Card technologies - Proximity cards and smart cards



- **Proximity cards (prox cards)** are read-only devices that are encoded once and then used to transmit a fixed numeric value to a reader. The underlying mechanism is a ***radio frequency identification (RFID)*** token, which is embedded in an ID card. The cards contain a chip and an antenna which, when brought to the geographic vicinity of a reader's radio field, enables the card to draw power from the reader to communicate
- The typical prox card uses the ***125 kHz*** frequency band
- Recommended for legacy systems only



- **Smart cards** are standard-sized plastic cards with an embedded integrated circuit (IC) chip. The chip includes components for storing, transmitting, and processing data. Data transfer can be conducted by using contacts on the card surface (contact chips) or electromagnetic energy/radio frequencies (contactless chips).
- Contact smart cards include PKI (public key infrastructure) cards, whereas in contactless cards, the underlying mechanism is a ***radio frequency identification (RFID)*** token, which is embedded in an ID card. The typical Smart card uses the ***13.56 MHz*** frequency band.

Credentials

Proximity credential data vs. CSN

EM / PROX Cards - Proximity credential data:

- For **EM/ Prox Cards**, the credential data can be a combination of facility code and a card number. The number range can be customer defined
- Most likely This is NOT a UNIQUE number
- The data is not secured and can easily be read by everybody
- No Encryption

The proximity credential data and CSN identifies a card

Smart Cards - Card Serial Number (CSN)

- For **Smart Cards** there is a Unique Identification (UID) number, also called CSN (Card Serial Number)
- CSN is not secured and is always available in an open card sector that can be publically read

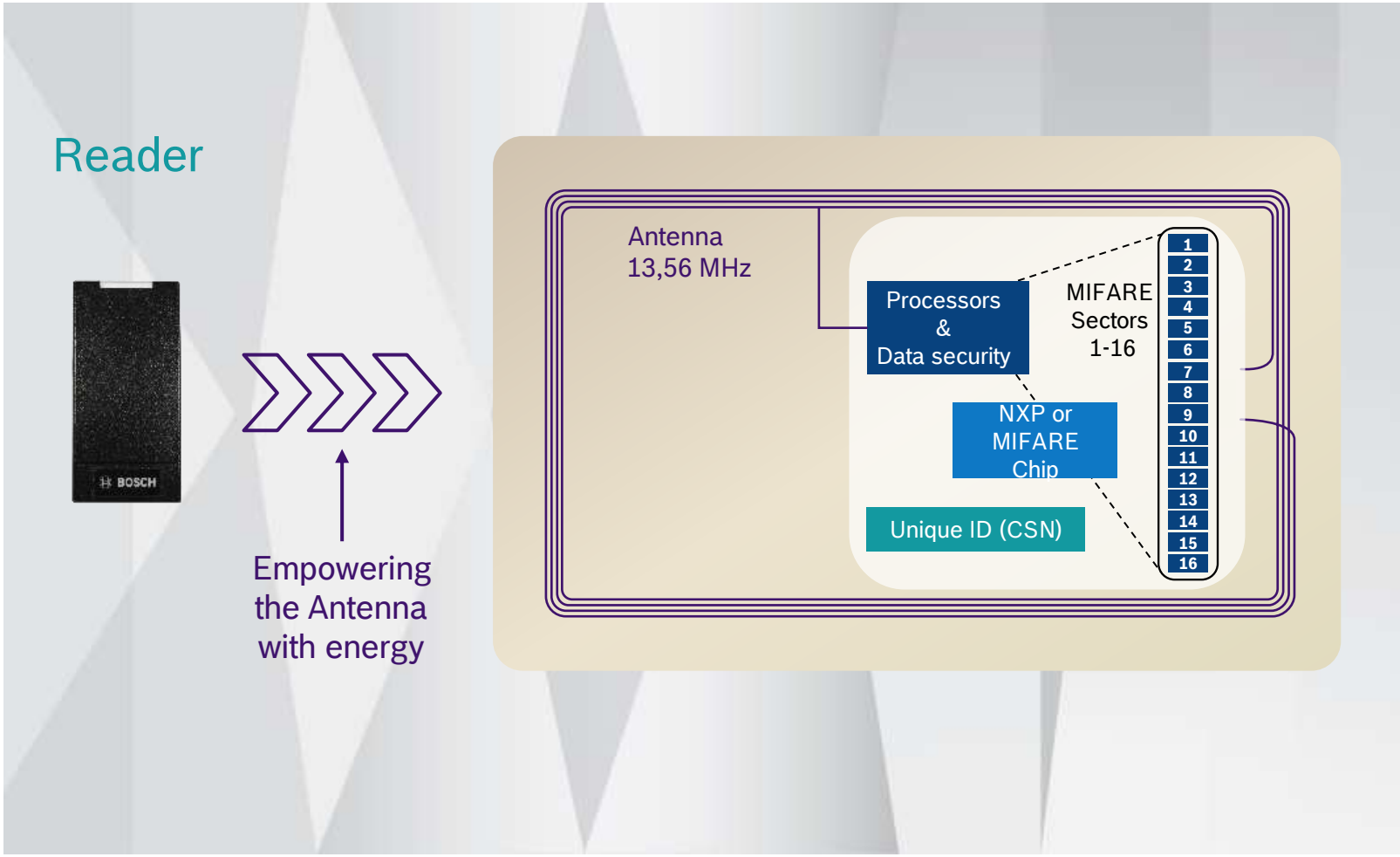
Credentials

Adding security with Smart Cards – Secure data element

Bosch offers a variety of Smart Card readers equipped with the needed firmware to read the **secure** data element (Bosch Code) on the Bosch credentials

Credentials

Smart Cards 13,56 MHz – Example MIFARE Classic 1K



- The standard Smart Card chip is embedded in the PVC substrate
- Every Smart Card chip has a public card serial number (CSN)
- The Smart chip is connected to an antenna in order to communicate with the reader
- The antenna is tuned for a frequency of 13,56 MHz

Credentials

Most common technologies

Brand	Frequency	Technology	Status	Protection	Security
MIFARE Classic	13,56MHz	SmartCard	Protected	Read key, encryption	Compromised
MIFARE Plus *	13,56MHz	SmartCard	Protected	Read key, encryption	Compromised + non compromised
MIFARE DESFire EV1/EV2	13,56MHz	SmartCard	Protected	Read key, encryption	Non compromised
iCLASS	13,56MHz	SmartCard	Protected	Read key, encryption	Compromised
iCLASS SE	13,56MHz	SmartCard	Protected	Read key, encryption	Non compromised
LEGIC prime	13,56MHz	SmartCard	Protected	Read key, encryption	Compromised
LEGIC advant*	13,56MHz	SmartCard	Protected	Read key, encryption	Non compromised
HID Prox	125kHz	Proximity	Unprotected	-	Transparent string
EM	125kHz	Proximity	Unprotected	-	Transparent string
Hitag1	125kHz	Proximity	Unprotected	-	Transparent string

* Not included in Bosch portfolio

Readers at a glance

What is it?

Provides direct feedback to the owner of a credential if for example access is granted

Direct interface between credential owner and access management system

Electronic component of a physical access control system

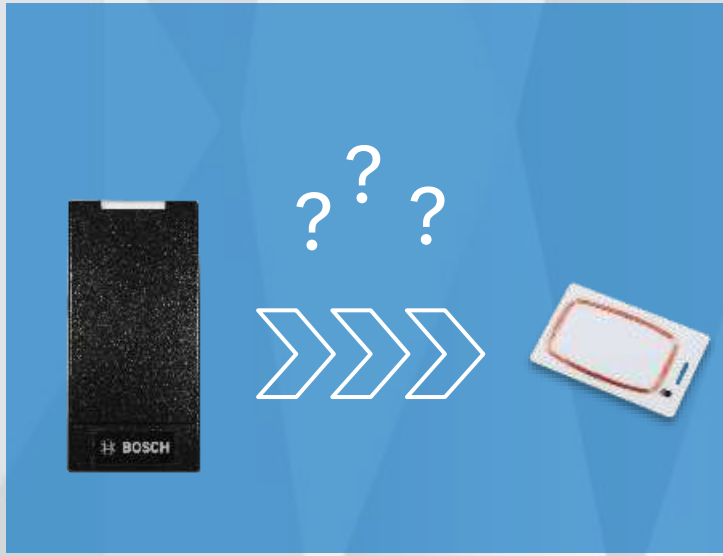
Contact readers, contactless readers, biometric readers, keypad readers, etc.

Receives the information carried by the credential

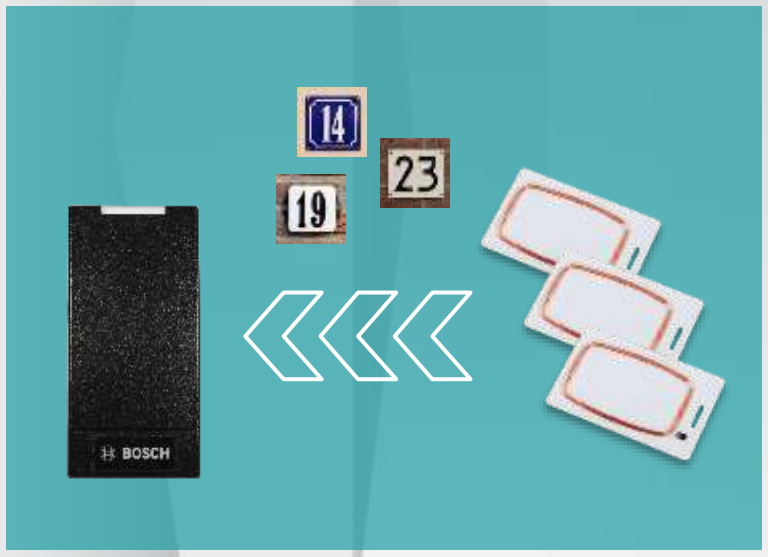
Readers

Communication between reader and cards – general process

1. **Reader searches constantly for a card**



2. **Reader detects multiple cards**



3. **Reader sends credential data to access controller**

If only CSN is read the access is directly checked with the database

Readers and credentials

Adding security with Smart Cards – Mutual Authentication

iCLASS and MIFARE authentication process:

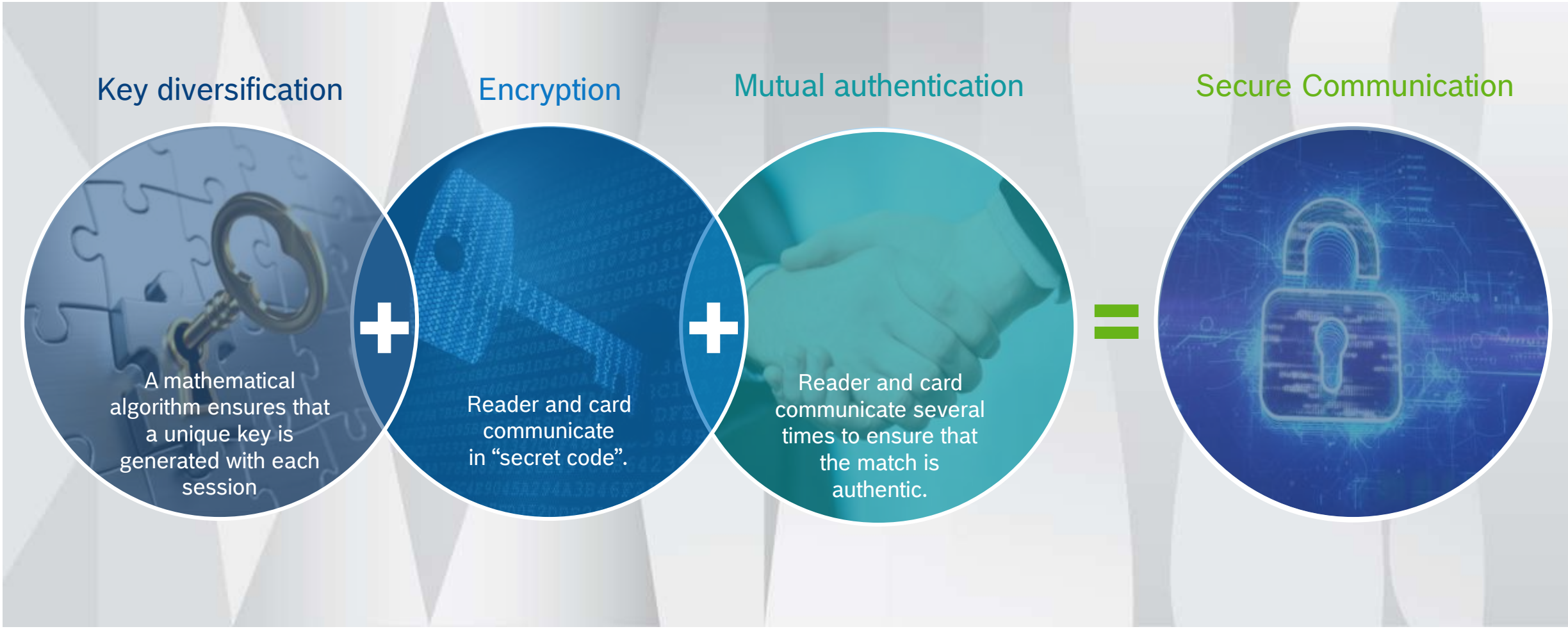
Additionally to the reading process of the card, there is a further security step for smart cards. The reader and the card go through a **complex mathematic process** in which they compare security keys carried within both the card and reader. This process is called **Mutual Authentication**. It ensures that the communication between the card and reader **can never be copied and repeated** back to the reader.

Both **iCLASS and MIFARE** are “contactless smart cards” by definition

If the keys **DO NOT match, the mutual authentication process is terminated** and the reader shows no reaction at all.

Readers and credentials

How does secure communication work?



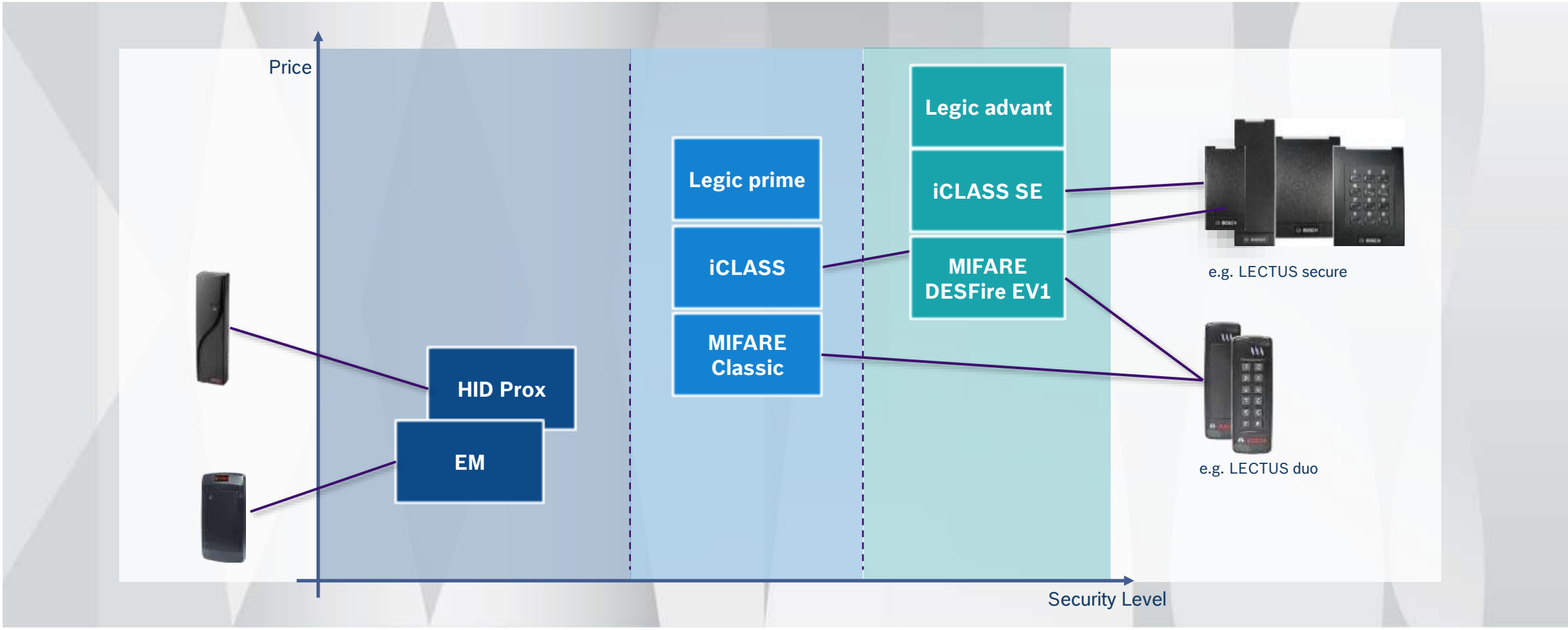
Readers and credentials

Basics to choose the right card to the reader

Readers and credentials must be based on the same technology and coding, plus read keys

Readers and credentials

Choosing the security level



Readers and credentials

Reader interfaces: Wiegand and OSDP

For the communication between an access reader and an access controller,

a physical interface as well as a communication protocol are needed

The two most common used technologies in access control:

1) The Wiegand interface and the Wiegand protocol

2) The RS-485 interface and the OSDP (Open Supervised Device Protocol)

Wiegand is currently widely used in many installations,

but RS-485 is quickly catching up and taking over the market

Readers and credentials

Reader interfaces: Wiegand and OSDP

	Wiegand	RS-485 (OSDP)	Benefit RS-485 (OSDP)
Cable length	<150m	1200m	Saves costs in HW and maintenance especially for larger installation sites
Conductors / Data transfer	Typical 7	Standardized 4	Logical transmission protocols for flexible use of reader functions instead of fixed signals
Communication	Unidirectional	Bi-directional	Bi-directional communication allows continuous reader supervision and more powerful reader commands via secure protocols like OSDP
Connectivity	Point to point	Serial bus	Serial bus connection allows for greater flexibility resulting in minimizing HW and maintenance costs
Installation costs			Especially in larger installations, the price per door is normally lower when using OSDP. Sustainable solution in long-term regarding trend in security
Encryption	No encrypted data interface	Encrypted data interface	Encryption is implemented in the OSDP V2 as a standard and can be activated optionally

Readers and credentials

The right combination

Transmission via…	Identification via… CSN	Identification via… Bosch Code
WIEGAND	Vulnerable Identification Vulnerable Transmission	Secure Identification Vulnerable Transmission
OSDP	Vulnerable Identification Secure Transmission	Secure Identification Secure Transmission

BOSCH READER PORTFOLIO

Bosch Reader Portfolio

Technology Overview

Proximity Readers

Proximity readers act as an interface between the proximity card and the access controller. The data is transferred from the card to the reader on 125 kHz frequency band.

Smart Readers

Smart readers act as an interface between the smart card and the access controller. The data is transferred from the card to the reader on ***13.56 MHz*** frequency band. Bosch offers all customers highest security standards with their unique Bosch data elements. All RS-485 Smart Card readers come equipped with specialized FW to access a secure sector and read the Bosch code on the Smart cards.

Biometric Readers

AMS and BIS-ACE support also biometric identification. The Biometric Fingerprint reader comes with the ability to read the secure Bosch code data from the Bosch MIFARE DESFire cards and multiple card technologies including 125kHz and 13.56 MHz.

Bosch Reader Portfolio

Proximity Readers

Material description	Card Reader, HIDprox, mullion	Standalone device	Standalone device	Card Reader, EM, mini mullion
Commercial type number (CTN)	**ARD-MINIPROX**	**ARD-PROX-PPL**	**ARD-ENTRYPROX**	**ARD-AYK12**
				
Bosch controller compatibility	AMC2-4WCF, APC-AMC2-2WCF, AEC, B/G-series	AMC2-4WCF, APC-AMC2-2WCF, AEC, B/G-Series	Standalone device	AMC2-4WCF, APC-AMC2-2WCF, AEC, B/G-series
Software compatibility	BIS-ACE, AEC, AMS	BIS-ACE, AEC, AMS	BIS-ACE, AEC, AMS	BIS-ACE, AEC, AMS
Interfaces	Wiegand	Wiegand	Wiegand	Wiegand
Supported protocol	Wiegand	Wiegand	Wiegand	Wiegand
Panel connection	Pigtail	Pigtail	Terminal strip	Pigtail
Supported credential technology	HID Prox	HID Prox	HID Prox	EM4102
Bosch code	–	–	–	–
Power supply	5 – 16 VDC	5 – 16 VDC	10 – 16 VDC	5 – 16 VDC
Environment class	IP55	IP55	IP55	IP65
Maximum reading distance	13 cm	6 cm	6 cm	8 cm
Keypad	no	no	yes	no
Dimensions (H x W x D)	152 x 43 x 25,4 mm (indoor and outdoor)	79,6 x 44 x 17 mm (indoor and outdoor)	133 x 70 x 35 mm (indoor and outdoor)	80 x 40 x 13 mm (indoor and outdoor)
	Data Sheet	**Data Sheet**	**Data Sheet**	**Data Sheet**

Bosch Reader Portfolio

Smart Card Readers (Wiegand) - iClass

Name	LECTUS secure 1000 WI	LECTUS secure 4000 WI	LECTUS secure 5000 WI	LECTUS secure 9000 WI
Material description	**Card reader, iCLASS, Wiegand**	**Handsfree card reader, iCLASS, Wiegand**	**Card reader with keypad, iCLASS, Wiegand**	**Handsfree card reader, iCLASS, Wiegand**
Commercial type number (CTN)	**ARD-SER10-WI**	**ARD-SER40-WI**	**ARD-SERK40-W1**	**ARD-SER90-WI**
				
Bosch controller compatibility	AMC2-4WCF, APC-AMC2-2WCF, AEC, B/G-series	AMC2-4WCF, APC-AMC2-2WCF, AEC, B/G-series	AMC2-4WCF, APC-AMC2-2WCF, AEC, B/G-series	AMC2-4WCF, APC-AMC2-2WCF, AEC, B/G-series
Software compatibility	BIS-ACE, AEC, AMS	BIS-ACE, AEC, AMS	BIS-ACE, AEC, AMS	BIS-ACE, AEC, AMS
Interfaces	Wiegand	Wiegand	Wiegand	Wiegand
Supported protocol	Wiegand	Wiegand	Wiegand	Wiegand
Panel connection	Pigtail	Pigtail	Pigtail	Terminal strip
Supported standard	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B
Supported credential technology	ISO14443A CSN, MIFARE Classic, MIFARE DESFire, iCLASS, iCLASS SE, Seos	ISO14443A CSN, MIFARE Classic, MIFARE DESFire, iCLASS, iCLASS SE, Seos	ISO14443A CSN, MIFARE Classic, MIFARE DESFire, iCLASS, iCLASS SE, Seos	ISO14443A CSN, MIFARE Classic, MIFARE DESFire, iCLASS, iCLASS SE, Seos
Bosch code	–	–	–	–
Power supply	5 – 16 VDC	5 – 16 VDC	5 – 16 VDC	5 – 16 VDC
Environment class	IP55 (IP65 with gasket)	IP55 (IP65 with gasket)	IP55 (IP65 with gasket)	IP65
Maximum reading distance	7.6 cm	11.4 cm	14 cm	33.6 cm
Keypad	no	no	Yes	no
Dimensions (H x W x D)	103 x 48 x 23 mm (indoor)	122 x 84 x 24 mm (indoor)	122 x 85 x 28 mm (indoor)	333 x 333 x 39 mm (indoor and outdoor)
	Data Sheet			**Data Sheet**

- 13.56 MHz proximity readers for connecting to access controllers with Wiegand interfaces
- Available with four different form factors, LECTUS secure readers meet nearly all installation requirements

Bosch Reader Portfolio

Smart Card Readers (Wiegand and RS485 (OSDP V1)) – MIFARE

Name	LECTUS duo 3000C	LECTUS duo 3000 CK	LECTUS duo 3000 E	LECTUS duo 3000 EK
Material description	**Card reader, MIFARE classic**	**Card reader with keypad, MIFARE classic**	**Card Reader, MIFARE EV1**	**Card reader with keypad, MIFARE EV1**
Commercial type number (CTN)	**ARD-AYBS6260**	**ARD-AYBS6360**	**ARD-AYBS6280**	**ARD-AYBS6380**
				
Bosch controller compatibility	AMC2-4WCF, APC-AMC2-2WCF, AMC2-4R4CF, AEC	AMC2-4WCF, APC-AMC2-2WCF, AMC2-4R4CF, AEC	AMC2-4WCF, APC-AMC2-2WCF, AMC2-4R4CF, AEC	AMC2-4WCF, APC-AMC2-2WCF, AMC2-4R4CF, AEC
Software compatibility	BIS-ACE, AMS	BIS-ACE, AMS	BIS-ACE, AMS	BIS-ACE, AMS
Interfaces	Wiegand, RS-485	Wiegand, RS-485	Wiegand, RS-485	Wiegand, RS-485
Supported protocol	Wiegand, OSDPv1	Wiegand, OSDPv1	Wiegand, OSDPv1	Wiegand, OSDPv1
Panel connection	Terminal strip	Terminal strip	Terminal strip	Terminal strip
Supported standard	ISO 1443A	ISO 1443A	ISO 1443A	ISO 1443A
Supported credential technology	ISO14443A CSN, MIFARE Classic	ISO14443A CSN, MIFARE Classic	ISO14443A CSN, MIFARE DESFire, MIFARE Classic	ISO14443A CSN, MIFARE DESFire, MIFARE Classic
Bosch code	yes	yes	yes	yes
Power supply	8.5 – 16 VDC	8.5 – 16 VDC	8.5 – 16 VDC	8.5 – 16 VDC
Environment class	IP65	IP65	IP65	IP65
Maximum reading distance	3 cm	3 cm	3 cm	3 cm
Keypad	no	yes	no	yes
Dimensions (H x W x D)	137 x 44 x 27,5 mm (indoor and outdoor)	137 x 44 x 27,5 mm (indoor and outdoor)	137 x 44 x 27,5 mm (indoor and outdoor)	137 x 44 x 27,5 mm (indoor and outdoor)
	Data Sheet		**Data Sheet**	

- The LECTUS duo 3000 classic line consists of a keypad and a non keypad version for MIFARE Classic and MIFARE DESFire. They come equipped with the Bosch coded MIFARE data sector and support reading the CSN of ISO14443A cards as well.
- Both reader types provide a Wiegand and RS485/OSDP interface, selectable easily by DIP switch.
- Three LED indicators and a beeper give clear feedback to the user during operation. The reader's logo is illuminated in the dark.

Bosch Reader Portfolio

Multitech smart card readers (RS-485 OSDP V2 encrypted) – iClass and MIFARE

Name	LECTUS Secure 1000 RO	LECTUS Secure 2000 RO	LECTUS Secure 4000 RO	LECTUS Secure 5000 RO
Material description	**Card reader, OSDP**	**Card reader, OSDP**	**Card reader, OSDP**	**Card reader with keypad, OSDP**
Commercial type number (CTN)	**ARD-SER10-RO**	**ARD-SER15-RO**	**ARD-SER40-RO**	**ARD-SERK40-RO**
				
Bosch controller compatibility	AMC2-4R4CF	AMC2-4R4CF	AMC2-4R4CF	AMC2-4R4CF
Software compatibility	BIS-ACE, AMS	BIS-ACE, AMS	BIS-ACE, AMS	BIS-ACE, AMS
Interfaces	RS-485	RS-485	RS-485	RS-485
Supported protocol	OSDPv2 SC	OSDPv2 SC	OSDPv2 SC	OSDPv2 SC
Panel connection	Terminal strip	Terminal strip	Terminal strip	Terminal strip
Supported standard	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B
Supported credential technology	MIFARE DESFire, MIFARE Classic, iCLASS, iCLASS SE, Seos	MIFARE DESFire, MIFARE Classic, iCLASS, iCLASS SE, Seos	MIFARE DESFire, MIFARE Classic, iCLASS, iCLASS SE, Seos	MIFARE DESFire, MIFARE Classic, iCLASS, iCLASS SE, Seos
Bosch code	–	–	–	–
Power supply	5 – 16 VDC	5 – 16 VDC	5 – 16 VDC	5 – 16 VDC
Environment class	IP55 (IP65 with gasket)	IP55 (IP65 with gasket)	IP55 (IP65 with gasket)	IP55 (IP65 with gasket)
Maximum reading distance	7.6 cm	7.6 cm	13 cm	13 cm
Keypad	no	no	no	yes
Dimensions (H x W x D)	103 x 48 x 23 mm (indoor and outdoor)	153 x 48 x 23 mm (indoor and outdoor)	122 x 85 x 24 mm (indoor and outdoor)	122 x 85 x 28 mm (indoor and outdoor)
	Data Sheet			

- Highest level of security due to OSDPv2 AES 128bit encryption.
- 13.56 MHz proximity readers for connecting to access controllers with OSDP interfaces
- They come equipped with the Bosch coded MIFARE data sector and support reading the CSN of ISO14443A cards as well.
- Interoperable with a growing range of technology environments and form factors

Bosch Reader Portfolio

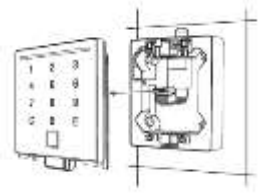
Multitech smart card readers (RS-485 OSDP V2 encrypted) – MIFARE and LEGIC

Name	LECTUS select	LECTUS select	LECTUS select	LECTUS select
Material description	**Card reader with keypad, OSDP (black)**	**Card reader, OSDP (black)**	**Card reader with keypad, OSDP (white)**	**Card reader, OSDP (white)**
Commercial type number (CTN)	**ARD-SELECT-BOK**	**ARD-SELECT-BO**	**ARD-SELECT-WOK**	**ARD-SELECT-WO**
				
Bosch controller compatibility	AMC2-4R4CF	AMC2-4R4CF	AMC2-4R4CF	AMC2-4R4CF
Software compatibility	BIS-ACE, AMS	BIS-ACE, AMS	BIS-ACE, AMS	BIS-ACE, AMS
Interfaces	RS-485	RS-485	RS-485	RS-485
Supported protocol	OSDPv2 SC	OSDPv2 SC	OSDPv2 SC	OSDPv2 SC
Panel connection	Terminal strip	Terminal strip	Terminal strip	Terminal strip
Supported standard	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B	ISO 1443A, ISO 15693, ISO 14443B
Supported credential technology	MIFARE DESFire EV1 & EV2, LEGIC advant	MIFARE DESFire EV1 & EV2, LEGIC advant	MIFARE DESFire EV1 & EV2, LEGIC advant	MIFARE DESFire EV1 & EV2, LEGIC advant
Bosch code	yes	yes	yes	yes
Power supply	8 – 30 VDC	8 – 30 VDC	8 – 30 VDC	8 – 30 VDC
Environment class	IP54	IP54	IP54	IP54
Maximum reading distance	7.6 cm	7.6 cm	7.6 cm	7.6 cm
Keypad	yes	no	yes	no
Dimensions (H x W x D)	88 x 99 x 27 mm	88 x 99 x 27 mm	88 x 99 x 27 mm	88 x 99 x 27 mm
	Data Sheet			

- Compact design, front cover, rear panel and surface-mounted housing made of plastic
- Easy installation
- They come equipped with the Bosch coded MIFARE data sector and support reading the CSN of ISO14443A cards as well.
- Flush-mount: on standard flush-mounting box Ø 60 mm
- Surface-mount: directly on the wall - cable entry options from above, below and behind the device
- Sabotage monitoring

Accessories:

Wallmount Box Lectus Select
ARA-SELECT-WWA (white)
ARA-SELECT-SWA (silver)



Bosch Reader Portfolio

Biometric Reader and Enrollment Reader

Name	BioEntry W2	Lectus enroll 5000
Material description	**Fingerprint reader, OSDP, multiCLASS**	**USB enrollment reader, MIFARE EV1**
Commercial type number (CTN)	**ARD-FPBEW2-H2**	**ARD-EDMCV002-USB**
		
Bosch controller compatibility	AMC2-4WCF, APC-AMC2-2WCF, AMC2-4R4CF	-
Software compatibility	BIS-ACE, AMS	BIS-ACE, AMS
Interfaces	Wiegand, RS-485	-
Supported protocol	Wiegand, OSDPv2 SC	-
Panel connection	Terminal strip, RJ45 (PoE)	USB
Supported standard	ISO 1443A	ISO 14443A
Supported credential technology	EM, HID Prox, MIFARE Classic, DESFire EV1, HID-Corporate-1000, iCLASS, iCLASS SE, Seos	MIFARE classic, DESFire EV1 (Bosch data record)
Bosch code	yes	yes
Power supply	12 VDC or PoE	Powered by USB
Environment class	Indoor / outdoor product (IP67/ IK09)	Indoor
Maximum reading distance	13 cm	-
Keypad	no	no
Dimensions (H x W x D)	172 x 50 x 43 mm (indoor and outdoor)	112 x 54 x 27 mm
	Data Sheet	**Data Sheet**

Bosch Reader Portfolio

Biometric Readers – BioEntry W2 reader

Biometry at its highest standard

- Convenient cardholder registration including the enrollment of fingerprint templates in just one management system (AMS or BIS-ACE)
- Fingerprint templates can be stored either in secure database or locally on the reader
- BioEntry W2 provides class-leading performance and security by featuring the latest fingerprint algorithm coupled by a powerful quad-core CPU
- The device offers flexibility and sustainability by featuring multitechnology support of credentials, including EM, iClass and MIFARE DESFire*
- Packed in a rugged IP67/IK09 housing with sleek metallic finish, BioEntry W2 is a perfect access control solution for tough environment and outdoor installation

Features

Best-In-Class Performance
- 1.2GHz quad-core CPU

Improved Accuracy & Security
- High-precision OP5 optical sensor

High storage capacity
- Supports up to 400k users
- Data can be stored either on device or on secure database of AMS / BIS-ACE

Rugged Structure
- IK08 impact protection
- IP67 ingress protection
- Ideal for outdoor installation

Multi RFID Card Reading
- LF(125KHz), HF(13.56MHz) dual-band
- Reads all card types that HID multiCLASS supports (EM/HID Prox / MIFARE / iCLASS / MIFARE Classic/ MIFARE DESFire / NFC)
- Highest security standard by supporting Bosch coded MIFARE credentials

* One card format at a time is supported

Bosch Reader Portfolio

Biometric Reader - IDEMIA SIGMA Lite

Name	IDEMIA SIGMA Lite	IDEMIA SIGMA Lite	IDEMIA SIGMA Lite	IDEMIA SIGMA Lite
Material description	**Bio finger reader, LED indicator**	**Bio finger reader, LED indicator**	**Bio finger reader, LED indicator**	**Bio finger reader, LED indicator**
Commercial type number (CTN)	**293678615**	**293678628**	**293673665**	**293678636**
				
Bosch controller compatibility	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF
Software compatibility	BIS-ACE	BIS-ACE	BIS-ACE	BIS-ACE
Interfaces	Wiegand, RS-485	Wiegand, RS-485	Wiegand, RS-485	Wiegand, RS-485
Supported protocol	Wiegand, OSDPv2 SC	Wiegand, OSDPv2 SC	Wiegand, OSDPv2 SC	Wiegand, OSDPv2 SC
Panel connection	Pigtail	Pigtail	Pigtail	Pigtail
Supported standard	-	ISO 15693	-	ISO 14443A
Supported credential technology	-	HID iClass, iClass SE, Seos	HID Prox	MIFARE Classic, MIFARE DESFire
Bosch code	-	-	-	-
Power supply	12 - 24 VDC or PoE	12 - 24 VDC or PoE	12 - 24 VDC or PoE	12 - 24 VDC or PoE
Environment class	IP65	IP65	IP65	IP65
Keypad	no	no	no	no
Dimensions (H x W x D)	156 x 68 x 62 mm	156 x 68 x 62 mm	156 x 68 x 62 mm	156 x 68 x 62 mm
	Data Sheet	**Data Sheet**	**Data Sheet**	**Data Sheet**

Bosch Reader Portfolio

Biometric Reader - IDEMIA SIGMA Lite+

Name	IDEMIA SIGMA Lite+	IDEMIA SIGMA Lite+	IDEMIA SIGMA Lite+
Material description	**Card reader, iClass, touchscreen**	**Card reader, Prox, touchscreen**	**Card reader, Multi, touchscreen**
Commercial type number (CTN)	**293673644**	**293678678**	**293678660**
			
Bosch controller compatibility	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF
Software compatibility	BIS-ACE	BIS-ACE	BIS-ACE
Interfaces	Wiegand, RS-485	Wiegand, RS-485	Wiegand, RS-485
Supported protocol	Wiegand, OSDPv2 SC	Wiegand, OSDPv2 SC	Wiegand, OSDPv2 SC
Panel connection	Pigtail	Pigtail	Pigtail
Supported standard	ISO 15693	-	ISO 14443A
Supported credential technology	HID iClass, iClass SE, Seos	HID Prox	MIFARE Classic, MIFARE DESFire
Bosch code	-	-	-
Power supply	12 - 24 VDC or PoE	12 - 24 VDC or PoE	12 - 24 VDC or PoE
Environment class	IP65	IP65	IP65
Keypad	yes	yes	yes
Dimensions (H x W x D)	156 x 68 x 62 mm	156 x 68 x 62 mm	156 x 68 x 62 mm
	Data Sheet	**Data Sheet**	**Data Sheet**

Bosch Reader Portfolio

Biometric Reader - IDEMIA MorphoWave Compact and IDEMIA VisionPass

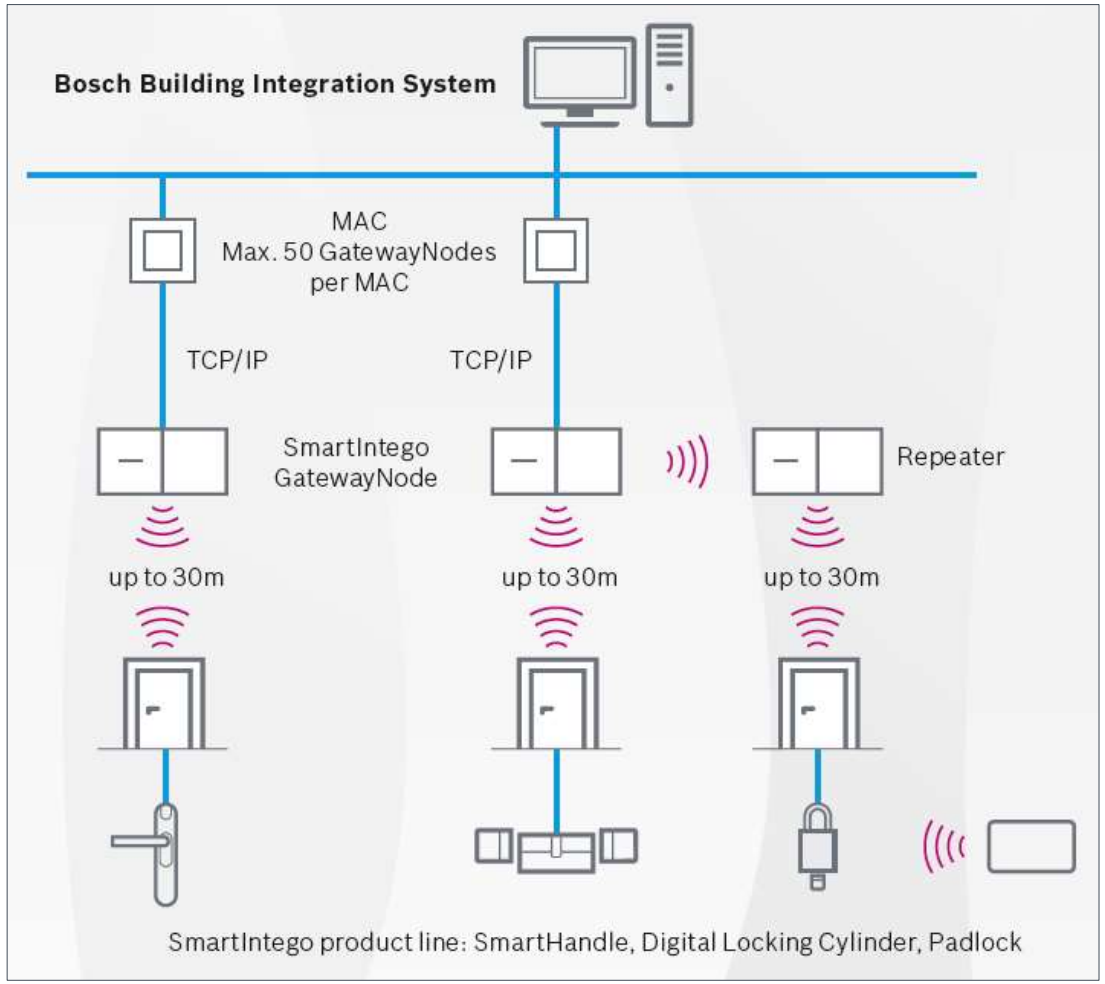
Name	IDEMIA MorphoWave Compact	IDEMIA SIGMA Lite+
Material description	**Contactless 3D fingerprint reader, MDPI**	**Facial recognition reader, MDPI**
Commercial type number (CTN)	**293722319**	**293744604**
		
Bosch controller compatibility	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF	AMC2-4WCF, APC-AMC2-2WCF, AMC2- 4R4CF
Software compatibility	BIS-ACE	BIS-ACE
Interfaces	Wiegand, RS-485	Wiegand, RS-485
Supported protocol	Wiegand, OSDPv2 SC	Wiegand, OSDPv2 SC
Panel connection	Pigtail	Pigtail
Supported standard	ISO 14443A (MiFare) and ISO 15693 (iClass and SEOS)	ISO 14443A (MiFare) and ISO 15693 (iClass and SEOS)
Supported credential technology	HID iClass, iClass SE, Seos HID Prox MIFARE DESFire	HID iClass, iClass SE, Seos HID Prox MIFARE DESFire
Bosch code	-	-
Power supply	12 - 24 VDC or PoE+	12 - 24 VDC
Environment class	IP65	IP65
Keypad	yes	yes
Dimensions (H x W x D)	250 x 152 x 216 mm	156 x 68 x 62 mm
	Data Sheet	**Data Sheet**

INTEGRATIONS

BOSCH

Integration

IP-based wireless locking with SimonsVoss' SmartIntego



- The integration of the Bosch Building Integration System (BIS) with SimonsVoss' SmartIntego allows for an IP-based management of **digital locks**
- SmartIntego locks communicate via their GatewayNodes to the BIS Access Engine (BIS-ACE)
- Each GatewayNode is capable of communicating with up to 16 locking devices
- There is no need for cables to be connected or installed, as all locks are battery-operated
- Digital locks can handle the transmission standards of the card formats MIFARE® Classic and MIFARE® DESFire® (CSN)
- Verticals: Office Buildings, Education, Hospitals and health care
- Available in EMEA, AP, NAM

Integration

IP-based wireless locking with SimonsVoss' SmartIntego

Key Features: Electronic logbook, Remote door release, White list, Office toggle mode, Anti-passback, Battery charging control

SmartIntego system components and their benefits:

The **SmartIntego GatewayNode** has a reach of up to 30 meters and is capable of communicating with up to 16 locking devices via an 868 MHz wireless connection.

The **SmartIntego Digital Locking Cylinder** provides fit for purpose solutions throughout the buildings and is extremely easy to install.

The **SmartIntego Digital SmartHandle** is the right choice for aesthetic surroundings.

The **SmartIntego Digital Padlock** protects personal belongings and is even suitable for outdoor use.

Integrations
IDEMIA biometric readers

Fingerprint readers

- MorphoAccess SIGMA Lite
- MorphoWave

Face recognition

- VisionPass
  - 2D + 3D + IR camera
  - Adjusts to user's height from 120..220cm
  - Up to 40k users
  - Mask detection and efficient with mask
  - For indoor and outdoor installations

- **Sigma Lite / Lite+**

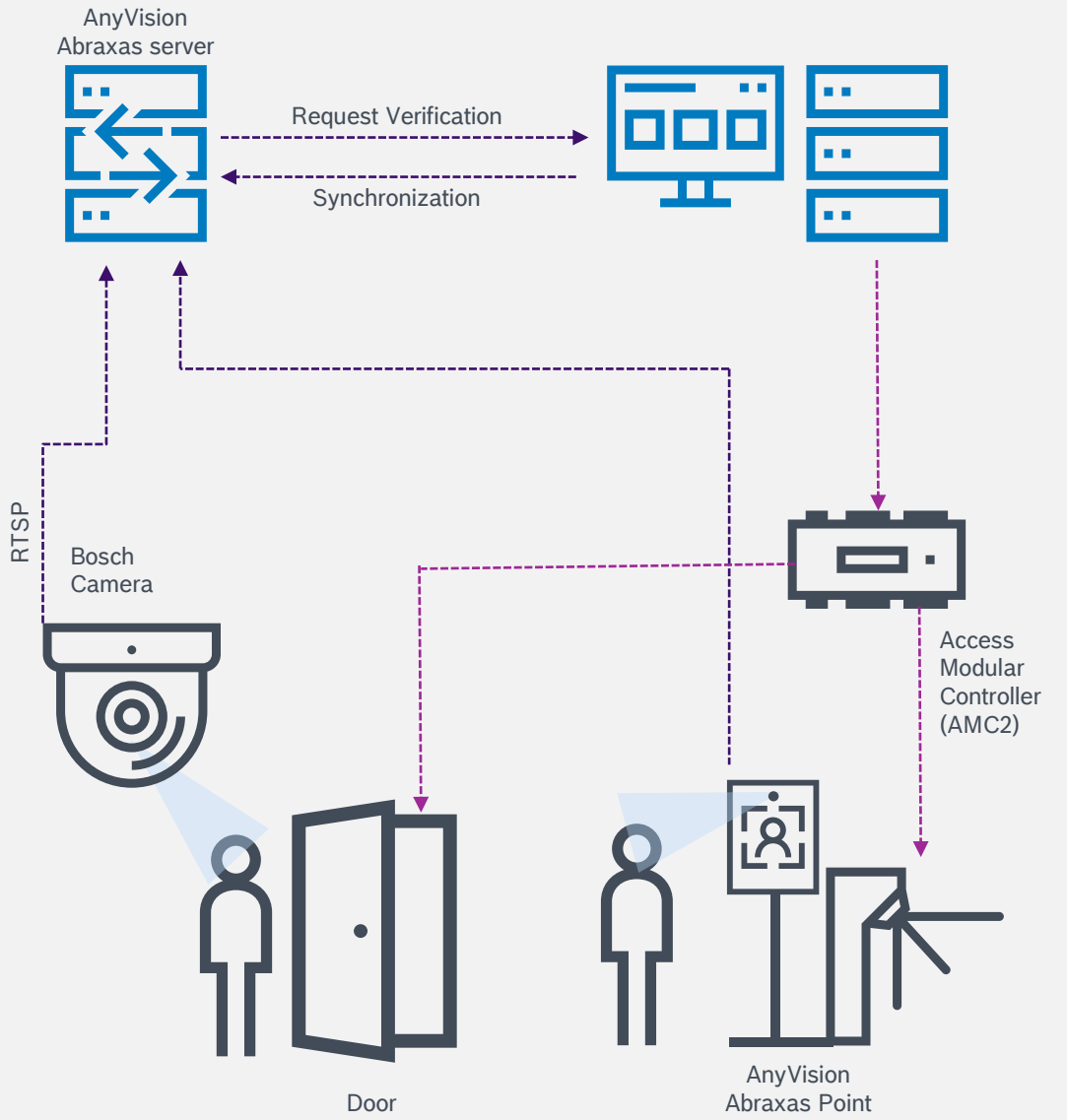
- **VisionPass**

- **Morpho*Wave***

Integrations
Oosto OnAccess (face recognition)

Integration via ACE-API

- Former Anyvision Abraxas Point
- Integration verified by Bosch
- Documentation available
- App Note available and released



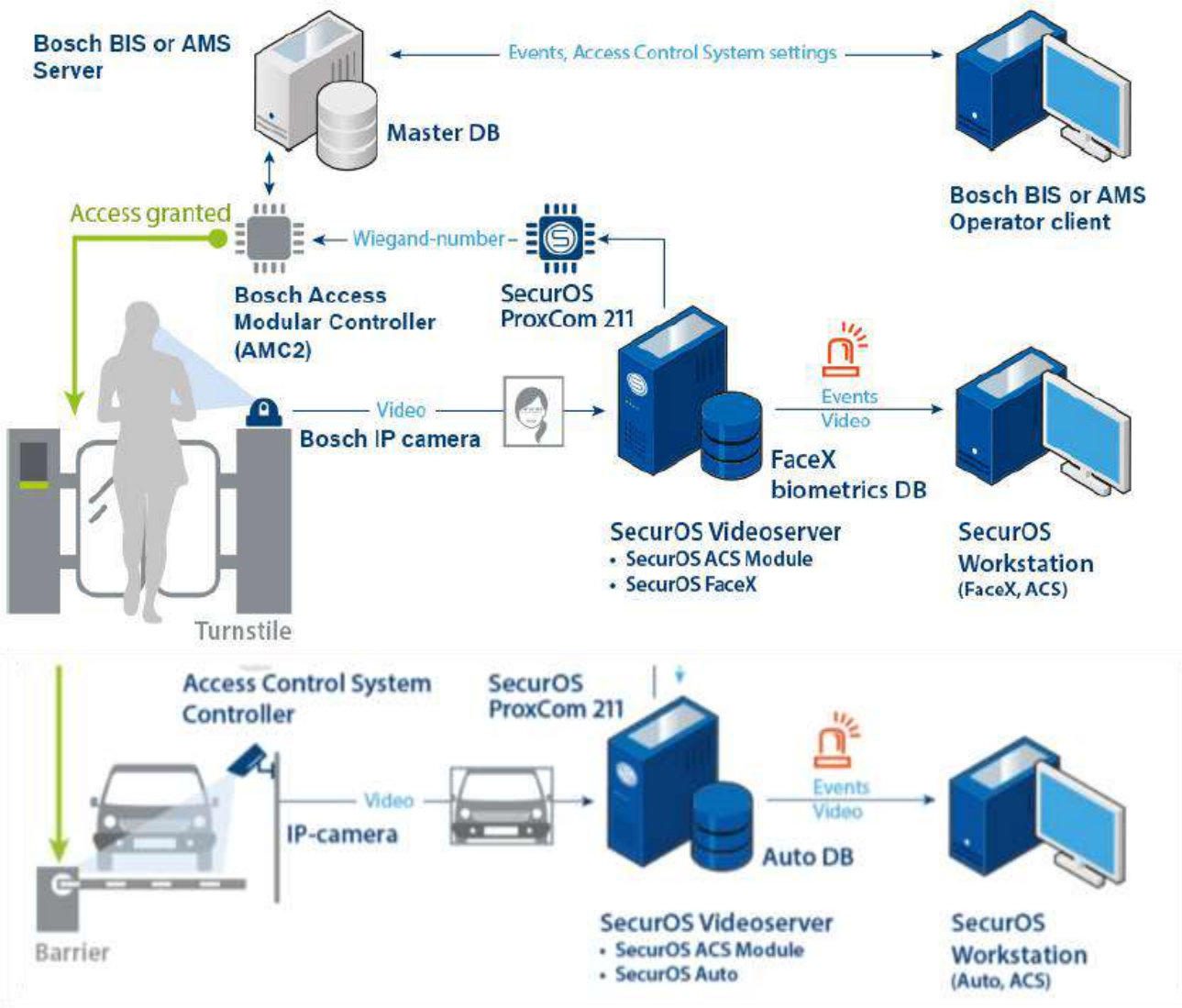
Integrations
ISS SecurOS

Face Recognition

► SecurOS Face

License Plate Recognition

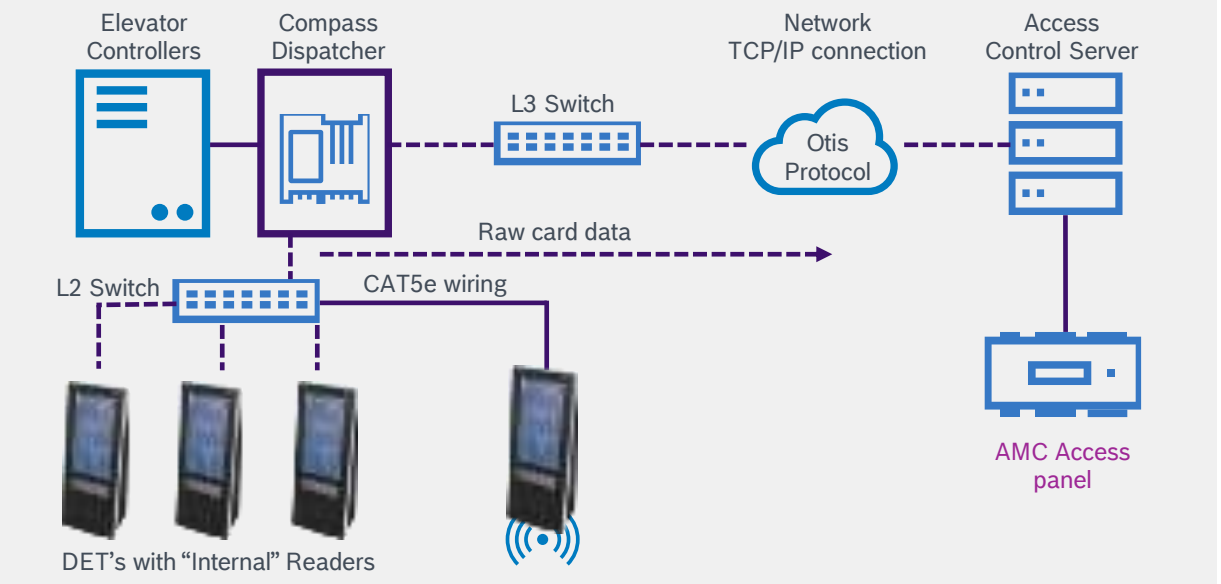
SecurOS Auto



Integrations
Otis Compass

Elevator Dispatch Systems

- With Otis readers

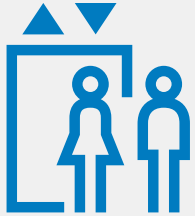


01

Enter destination

02

Receive Elevator Assignment



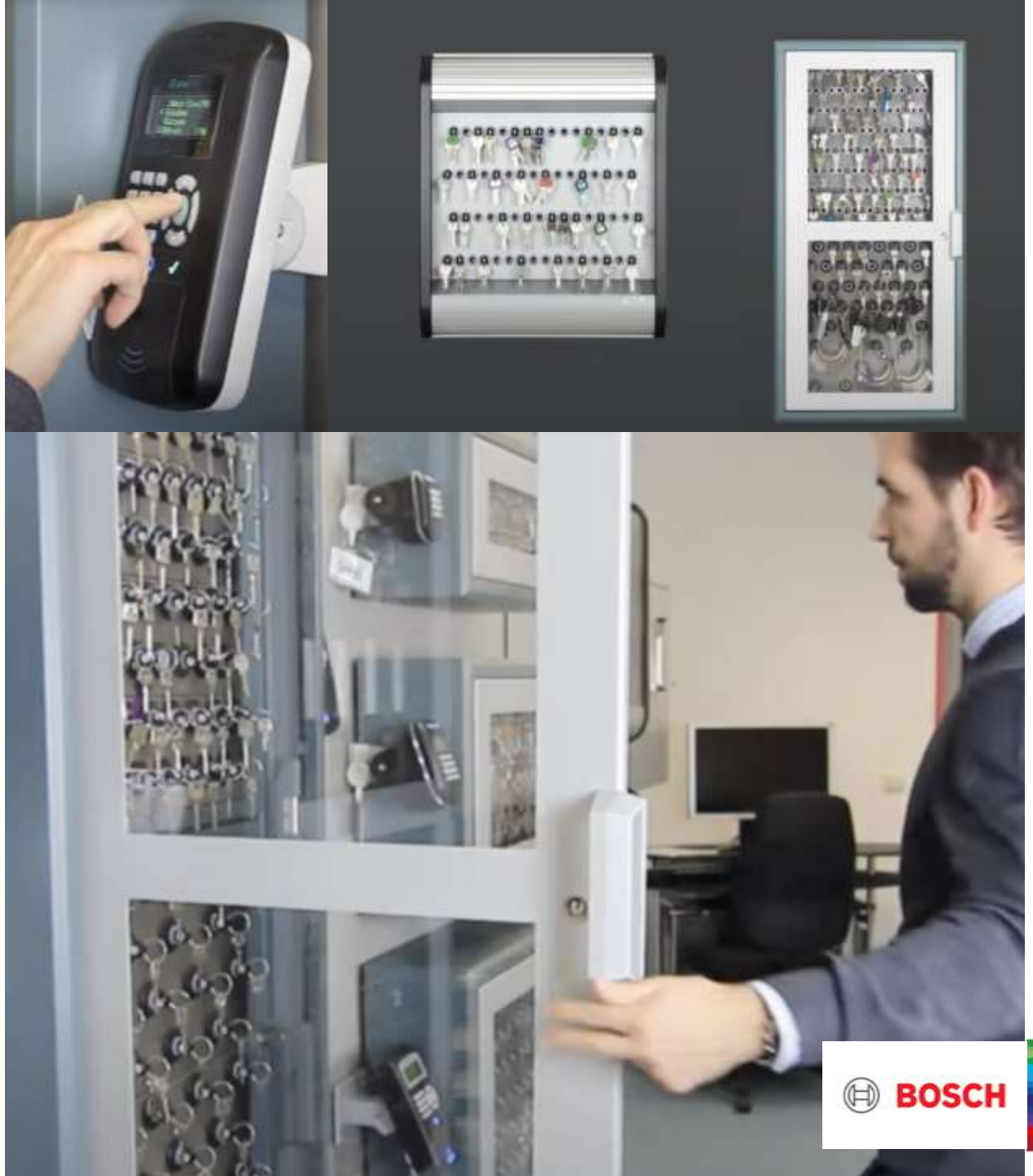
03

Proceed to Assigned Elevator

Integrations

Deister Key Management Systems

- Maxx and flexx for keys
- proxSafe for deposit boxes & drawers



SYSTEM DESIGN EXAMPLES AND HOW TO ORDER

Bosch Access Control Solutions

Suitable for many applications

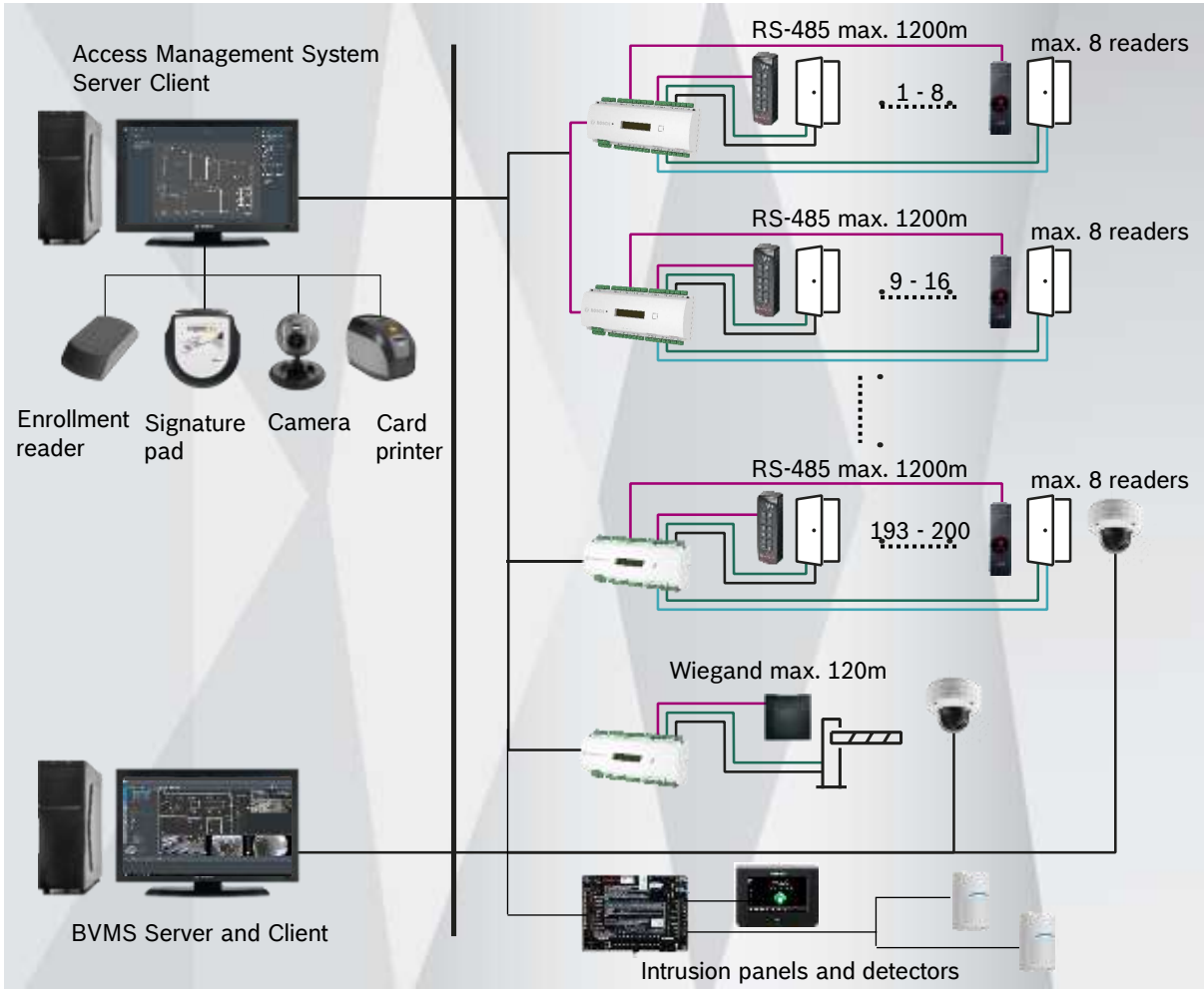
- Office buildings
- Retail
- Train stations
- Airports
- Manufacturing plants
- Governmental buildings
- Conference centers
- Critical infrastructure
- Health care
- Education
- Concert halls
- Warehouses





System Design

Access Management System with 150 doors



System requirements
• 150 doors • 1200 cardholders • Three operators

AMS features	AMC features	Reader features
• Max. 10,000 doors • Max. 200,000 cardholders • 5 cards per person • 1024 authorizations per MAC • Graphical location map • Video integration for video verification via BVMS • Intrusion integration via G Series	• 2 RS-485 buses • 8 inputs • 8 relays • TCP/IP, RS-485 connection	• Support OSDPv2 secure channel • Outdoor resistant (up to IP67) • Multitechnology support (125kHz and 13.56MHz) • Wiegand and RS485 support • Keypad or fingerprint for verification

Products	Item type
Readers	ARD-AYBS6380, ARD-FPBEW2-H2, ARD-SER90-WI
Lock	4710760066
Magnet contact	ISN-CSM35-W
REX button	4710760047
AMS Software	1 x AMS-BASE-PLUS30, 1 x AMS-XDRS-128V30, 2 x AMS-XCLI-1V30
Controller	APC-AMC2-4R4CF, APC-AMC2-4WCF
Power supply	APS-PSU-60
Battery	D126
BVMS Software	MBV-BPLU-100
Cameras	NDE-8504-R
Intrusion control panel	B8512G
Intrusion touch screen keypad	B942
Intrusion detectors	ISC-CDL1-W15G

THANK YOU

BOSCH