Invented for life

Whitepaper

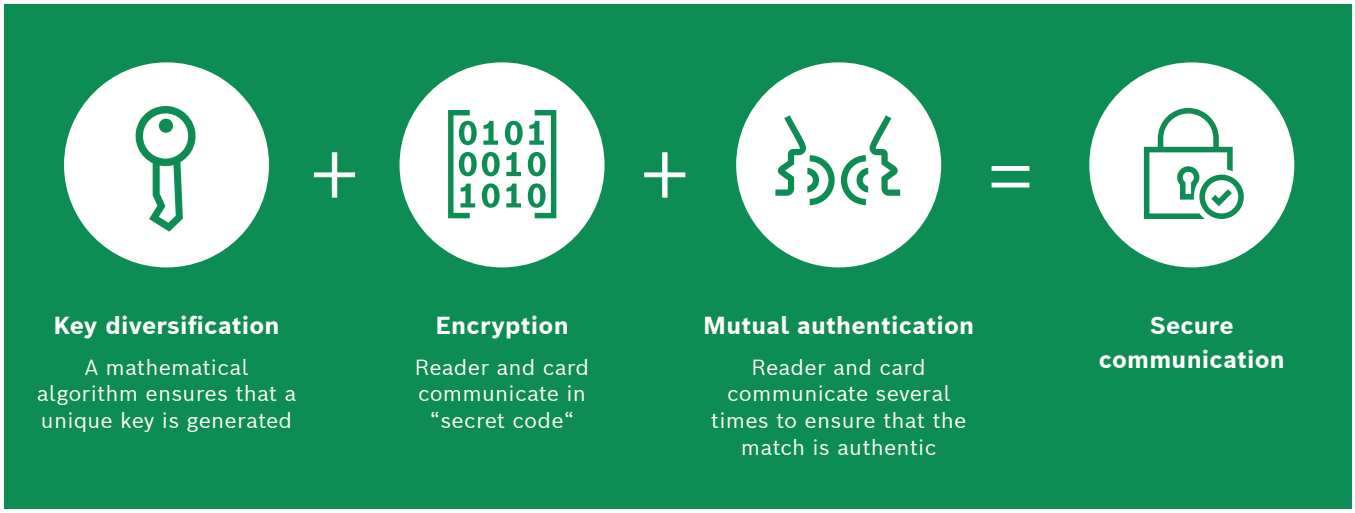
Building Truly Secure Access Control Systems

Physical Access Control Systems (PACS) are mission-critical to enterprises. They ensure the control, monitoring and safety of buildings and restricted areas. Any vulnerability could mean unauthorized physical access to critical areas, thus endangering the personnel, the physical and the informational assets of an organization. That is why it is so important to implement the latest and securest technologies. Building a truly secure access control system requires a complete system analysis: secure credentials, secure hardware and software that provides maximum protection against cyber-attacks. Bosch Access Control solutions combine experience with outstanding technology to ensure a truly secure and reliable operation.

Start using secure credentials

Credentials are crucial, as they represent the “key” to a secured area. Proximity cards (RFID) are still the most widely used type of credential in access control systems. However, there are differences in the security levels of the credentials on the market. 125kHz proximity cards are still used in projects, although this technology has been compromised. Card-copying devices can be used to read unencrypted card data, make copies of the card and so gain illicit access to your premises.

Upgrading the frequency from 125kHz to 13.56MHz allows you to take advantage of the security functions on 13.56MHz processor cards. These high-frequency cards are commonly referred to as “Smartcards”, and several 13.56MHz formats are currently on the market. Although inherently more secure, some 13.56MHz technologies have already been compromised, and no longer offer the highest security standards. It is therefore important to choose the most up-to-date and secure formats.



“Bosch offers **Smartcards** with the most **secure 13.56MHz technologies** on the market, such as **iClass SE/SEOS** and **MIFARE DESFire EV1 or EV2.“**

An aspect of equal importance is card encoding. Many smartcard readers allow only the reading of the Card Serial Number (CSN). Unfortunately, this type of implementation is not fully secure, because the CSN is always stored in a public (unencrypted) card sector. To guarantee maximum security the credential data must always be stored in a secure sector of the card.

“Bosch makes **its own secure code (Bosch Code)** which is stored within the secure area of the smartcard, plus a variety of compatible readers, thus providing the **highest level of security** for credentials.”

Improve security with biometrics and multi-factor authentication

There are several different types of credentials for access control systems, which can be selected according to the security level required. Biometric technologies such as face, fingerprint, iris and palm vein recognition are available. Nevertheless, even biometric readers are no longer immune to manipulation. For example, fingerprint readers can be deceived with artificial fingers made of silicone or other materials. Bosch therefore offers fingerprint readers with fake-finger detection, and we are constantly improving our portfolio.

With multi-factor authentication you combine different types of credentials to increase the level of security. This method requires more than one valid credential to gain access, typically to a highly restricted area, for instance a badge (smartcard) followed by a fingerprint.

You may combine two different readers, or one multi-technology reader connected to a single controller. This method is ideal for retrofitting older access control installations where a complete re-wiring would not be cost-effective.

The Bosch biometric readers offers dual-frequency and multi-smartcard reader technology.

If visual confirmation of identity is required, a video management system can be integrated: The cardholder presents his credential, and a security operator is notified via the management software. The operator can now compare live video from the entrance with database images of the cardholder, before deciding whether to grant access. In this way the operator's human intelligence can be made the ultimate arbiter in high-security areas.

"**Bosch** fingerprint readers deliver performance and the **highest level of security** through **multi-factor identification and fake finger detection.** Bosch software enables **video verification for high security areas** using native integration between the access control and video monitoring systems."

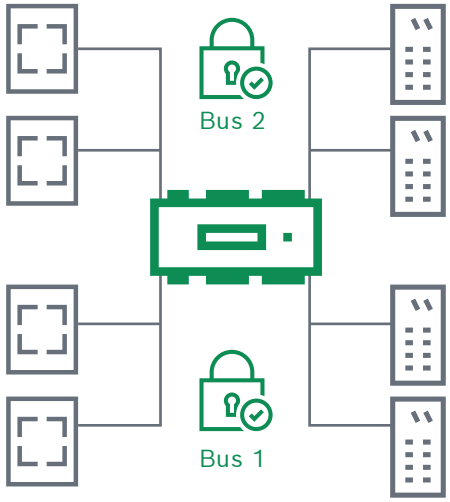
Use secure and encrypted communication technology

The selection of the correct credential is the first step towards building a truly secure access control system; the second step is selecting the reader. Once deciphered by the reader, the credential's data are sent to the access controller and the management software, which verify whether the credential is authorized for the specific area and time. As of today, the most widely used communication interface and protocol between reader and controller is still Wiegand. But due to its unidirectional communication and unencrypted transmissions Wiegand must be considered vulnerable, and not recommended for high-security systems.

The lack of encryption between reader and controller communication is vulnerable to "Man-in-the-Middle" attacks. Using a device known as a "skimmer", an attacker can tap the data transferred between reader and controller without the knowledge of the operators. Once collected, the data can provide unauthorized access even where otherwise secure smartcards are used, a so called Replay Attack. Attackers can inject valid credential data into the system wirelessly via the skimmer using a smartphone, for example via Bluetooth, and thus gain access without even needing to clone the physical credential.

For more secure access control, we recommend using **Open Supervised Device Protocol (OSDP)**. Version 2 (OSDPv2) with Secure Channel Protocol supports **AES encrypted communication** between reader and controller. Additionally, OSDP utilizes two-way communication. This allows constant monitoring of readers, via the same communication channels, in order to detect tampering or device removal. OSDP is an open protocol and has several other benefits, such as the ability to send commands to the reader, improved system interoperability and more.

"Bosch access control systems support **OSDP v2 Secure Channel with AES encryption.** This helps to achieve highest security levels in reader/ controller communication."



Ethernet communications, such as those between the access controller and the server, are also vulnerable to "Man-in-the-Middle" attacks. This kind of attack can collect valid credential data if the network technology used is not encrypted. If there is an internet or Wi-Fi connection present, attackers can intercept data from any point in the local network, without even being physically onsite.

That is why all components in an access control system (reader, controller, server, client, database, etc.) must encrypt their communications.

"Bosch **implements data encryption** in its communications **from card to software (end to end)**, enabling higher security between all components of the Access Control System."

The use of digital certificates in communications ensures trust between devices, and prevents unauthorized hosts from interacting with system services. Bosch solutions implement HTTPS, with its digital certificate authentication, for client-server communication.

Qualified network specialists are essential to undertake the many other measures necessary to implement a secure network infrastructure. These include firewalls, NIDS, VLANs, VPNs, MAC filtering.

Keep data safe

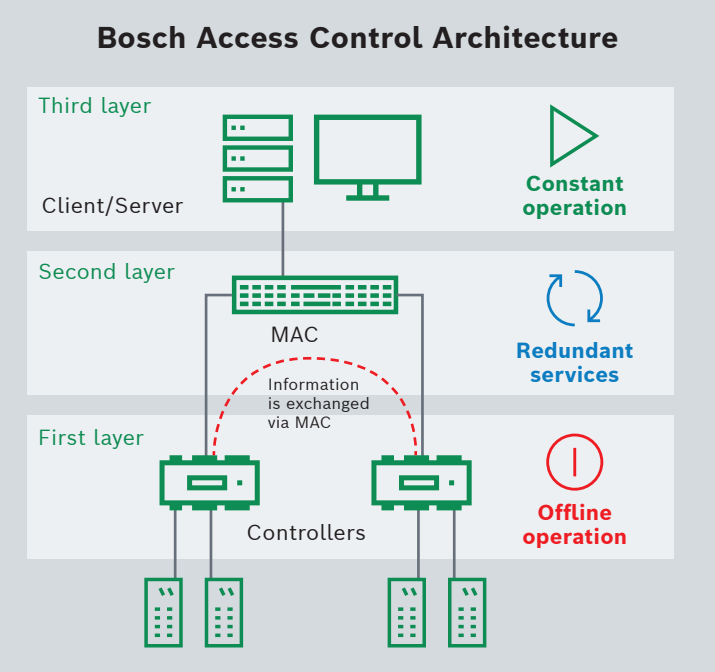
To prevent loss or destruction of information through espionage or natural disasters we build systems based on 3 “pillars” of information security: **Confidentiality, Availability, and Integrity.**

Confidentiality means limiting data access to authorized persons only, and ensuring that data is stored securely. In access control systems, most data is stored on the database server, which must implement encryption methods to prevent illicit access to sensitive data. In Europe and elsewhere the law is increasingly concerned and increasingly strict with data privacy. Thus, access control systems must also guarantee the safety of cardholders’ personal data, such as photos, addresses, medical and biometric information.

“All user information in Bosch Access Control System database can be **stored securely and encrypted, thus allowing system configurations** to satisfy privacy laws such as the EU’s GDPR.”

Availability means making sure that information is always accessible to all authorized and authenticated users and system services. Major access control systems provide round-the-clock interaction with users, their data and their credentials; whether this means granting access at a door, enrolling a new employee, or printing a report. To provide this level of availability a system must include fail-safe mechanisms to ensure that authorized access to required data is guaranteed, and not dependent on a single point of failure.

“Bosch access control system has a **3-tier architecture**, enabling door control even in case of server and database failure. Bosch controllers have enough autonomy to **manage up to 400,000 users** locally, and buffer **2 million events** if server communication is interrupted.”



Data integrity means that all required information is kept usable and unadulterated. For audits and post-event investigations access control systems must provide reliable records of all access events and of any changes in the system configuration. Data backups must be secure, complete and resilient against database failure or corruption.

“**Bosch access control software logs events and configuration changes** and supports schedules for automatic data **backup routines.**”

Use secure software

Software applications in access control perform the crucial tasks of managing personnel records, authorizations and credentials, managing doors, monitoring devices and logging everything that happens in the system. Secure access control software needs to include native features to guarantee safe operation: from simple enforcement of password policies to advanced mechanisms for repelling cyber-attacks.

A common cyber threat is that of “Brute-Force” attacks. These are programs for discovering usernames and passwords through rapid-fire informed guesses. They can succeed in hours, days, or years, depending on password complexity and their own processing power. If successful, a hacker may gain privileged access to all access-control functions and can, for example, grant access to intruders. To minimize the attack’s chances of success, strong passwords must be enforced, as well as mechanisms to block rapid-fire login attempts.

“The Bosch software login mechanism uses complex and encrypted passwords. The minimum login time is set to thwart brute-force attacks while not inconveniencing human operators.”

Many other attack vectors exist, such as malware, SQL injection, Denial-of-Service (DoS), and “man-in-the-middle” tactics. It is of paramount importance that installed software components receive security updates regularly and on time, to be armed against current and future threats.

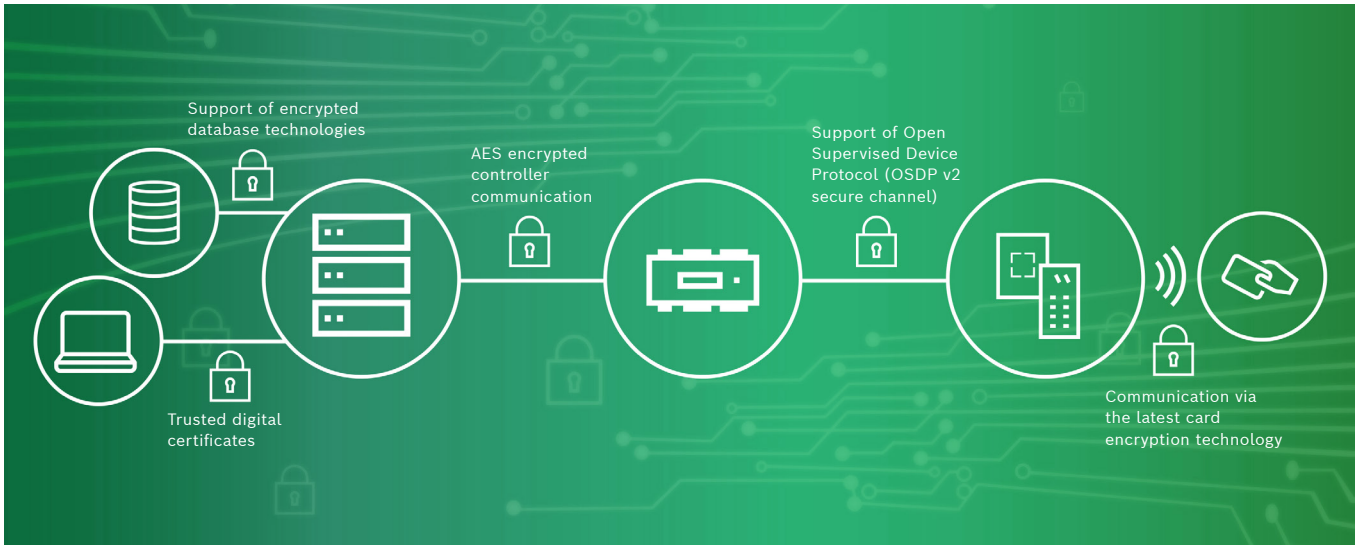
Bosch software components implement many features and functions against the various types of cyber-attacks:

▶ “Secure-by-Design”

Bosch software components are developed according to “Secure-by-Design” principles. For example, in accordance with “Secure-by-Default”, all initial security settings (certificates, complex passwords, etc.) are set for maximum security in the configuration by default. In accordance with the concept of “Least Privilege” each operator, by default, has the rights to perform only those operations that are essential to his job, and to access the system from no other workstation but his own.

▶ Encrypted communications

Data transfer between the reader, controller, server and other components is encrypted. MIFARE DESFire EV1 or EV3 technology and Bosch Codes ensure that credentials are secure. Communication between reader and controller supports the encrypted OSDPv2 protocol.
Between controller and server, as well as between server and other components, a secure, AES- encrypted communication channel protects against a wide range of network-based attacks.



▶ Supports up-to-date IT industry standards for higher security measures

Bosch Client-Server communication supports the use of both self-signed certificates and certificates signed by a Certificate Authority (CA). HTTP Secure (HTTPS) is used through Transport Layer Security (TLS/DTLS) to secure web communication. “Active Directory” (AD) integration through LDAP makes it easier to comply with IT policies and facilitates the management of authorization levels based on AD groups.

▶ Complete events logs and records for forensic investigations and auditing

All system events and operator activities are securely logged, and the data is protected against tampering. Bosch software can also log any changes made to its own configuration. These features allow mandatory investigations and audits to be completed quickly, unequivocally, and with minimum disruption to daily operation.

▶ Product Security at Bosch

Product security is an essential part of Bosch quality to provide to all Bosch customers highly secure and reliable products. Bosch products pass the most rigorous penetration tests and threat analyses. A global Product Security Team has made security an integral part of Bosch’s processes. With the Bosch Product Security Incident Response Team (PSIRT) Bosch has created a central point of contact for managing security incidents, and a process to quickly eliminate any vulnerabilities in its products.

System security involves not only the application, but the whole software environment.
It is therefore extremely important to use the most secure operating systems with the latest security patches, as well as anti-malware tools.

Implement a “culture o security”

Even the most secure access control systems are vulnerable if a culture of security does not pertain in the workforce, from installation to daily operation.

The company responsible for installing the system must be fully qualified, and must understand the complex dynamics of physical barriers, the technologies involved and the daily operation of an access control system. Mistakes during the installation phase are common and can be costly. Installing maglocks outside of the secure area, for example, or with unprotected wiring, provides an opportunity for attackers to deactivate access control devices simply by cutting off their power supply.

Without a culture of security, cardholders themselves are a major cause of security breaches. The common and expected courtesy of holding doors open for the person behind you poses a security risk: “Tailgating”, as it is known, is usually harmless, but is a major problem for security operatives because the number of persons on the premises, and their identities, are no longer known with certainty. If an access control system is to be effective, it is vitally important to train all users in security culture to work with the system, not against it.

In conclusion: consider all aspects

A truly secure physical access control system (PACS) requires up-to-date and secure technologies, from credentials to hardware and software. Bosch Access Control does indeed offer a comprehensive, state-of-the-art portfolio of such products.

Good technology is necessary but not sufficient on its own. Bosch also has the experience to maintain a complete overview of the system and consider every component: **“The security of a system is as strong as its weakest component“.**

Best practices in installation, configuration, network security, hardened operating systems, operator and user training, are all crucial. For certified installers Bosch provides a “Cyber Security Hardening Guide“ to list all measures an installer can take to design and configure a **Truly Secure Access Control System.**

By Felipe Detoni. 05-2022

Bosch Security and Safety Systems

Visit **www.boschsecurity.com/access** for more information.