Cybersecurity in Keyless Access Management

Whitepaper for Critical Infrastructure

ASSA ABLOY
Global Solutions

assaabloyglobalsolutions.com

Experience a safer
and more open world

Contents

1. Introduction

Digitalisation shapes every industry. New technologies are updated and adapted in critical infrastructure to streamline operations. Wireless security devices offer endless possibilities for infrastructure protection, but they might raise questions about cybersecurity. In this white paper we want to educate how wireless technology enables safe and secure access management.

Accessing locations near and remote with a digital key

For most employees, a smartphone is a true multifunctional work device. A smartphone can make and receive calls, locate appointments, assist and help, and even act as a device for authenticate and pay. To add to its many uses, it can also easily be used as a secure digital key – or credential token – to access different sites and premises.

Trust in the centre of digital solutions

When cybersecurity is included and prioritised in all digital solutions, actions and access points, wireless solutions can make critical infrastructure sites smarter, more connected and safer. Cybersecurity concerns devices, people and practices. In the centre of all is trust – both in devices and in knowing that your employees and contractors are equipped to use the devices safely.

1.1 Why is cybersecurity important?

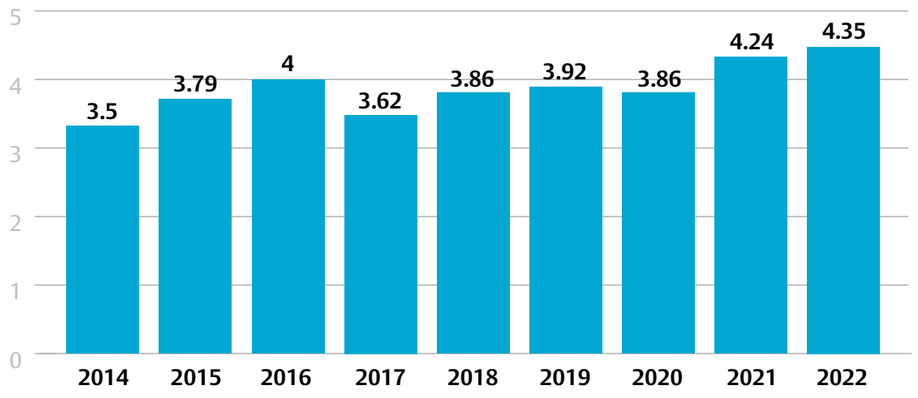
Everything is increasingly interconnected and digital. Companies rely on the Internet, and much of our personal information is stored online and our devices. Encountering risks that jeopardise our safety as individuals, or risks that create damage to companies and public infrastructure, is a real threat, even when simply using an open network. Therefore, cybersecurity measures within the solutions are needed to strengthen integrity and safety.

Did you know?

Cybercrime can be divided into two types: data security breaches and sabotage. Breaches aim to obtain not just personal data but also intellectual property. Sabotage aims to break down infrastructure and important systems. The global average cost of data breaches is on the rise. As of 2022, the average cost per breach amounted to 4.35 million U.S. dollars. (Statista)

Average cost of a data breach worldwide, 2014-2022

(in million U.S. dollars)



Details: Worldwide; Ponomon Institute; 2014 to 2022; 550 organizations

2. Cybersecurity worries and challenges of critical infrastructure today

Security, safety and operational managers working in critical infrastructure oversee multiple operations, which requires complete situational awareness. Many services must be provided 24/7 uninterruptedly, and that's why infrastructure, assets and personnel must be protected. Operations and equipment, such as vehicles, need monitoring, tracking and access management. All this must comply with local laws and regulations.

From an information security point of view, infrastructure professionals might find it difficult to compare cybersecurity aspects between available solutions and keep up with the latest threats and developments in cybersecurity. Even if a supplier has answers and descriptions, practical impact can be hard to understand – let alone compare. That's why we want to share information on some of the different aspects regarding wireless security and cybersecurity in this white paper.

2.1 Wireless access management: What are mobile credentials?

A mobile credential is a digital key that you use with your smartphone. Mobile credentials replace physical keys, cards and fobs to access buildings and important infrastructural elements, and they have significant advantages, like ease of use and multiple layers of security. For example, ABLOY BEAT access rights are granted as mobile credentials that can be used with a dedicated BEAT application, or integrated with the organisation's own existing app.

How do mobile credentials offer layers of security?

Firstly, there is the cybersecurity offered by both the device manufacturer and the mobile network provider. Then there is the digital credential itself, which is housed encrypted within the device. ASSA ABLOY's Seos®-based credentials, for example, offer advanced cryptography and privacy protection, which means the data will be incomprehensible for a person or a device that does not need to read it – if they were able to even access the data in the first place.

What about device safety?

Smartphones already utilise fingerprint, face ID and other biometrics and password security. On top of this, extra authentication can be mandated in the credential app and solution itself. There is also behavioural protection, as people will likely spot a missing phone long before they realise they have lost a key. All of this creates multi-layer protection for the wireless and mobile access solution.

2.2 Implementing essential cybersecurity layers

Layering cybersecurity increases physical security. There are three important procedures that should be layered – encryption, authentication and authorization.

1. Encryption
Information can be concealed with encryption. Encryption protects all data that travels between devices by encoding information or scrambling readable text to make it meaningless and protect it from unauthorised users. On the following page, we will explain encryption in further detail.

2. Authentication
Authentication identifies the user and the access management system. Once all parties can be sure of who is on the other end of the line, access rights can be granted and used. Authentication for the user includes the app's identification measures as well as the phones biometrics or passwords to validate the user. This information is also authenticated by the access management system. If invalid data is received, the management system or lock will not read the data.

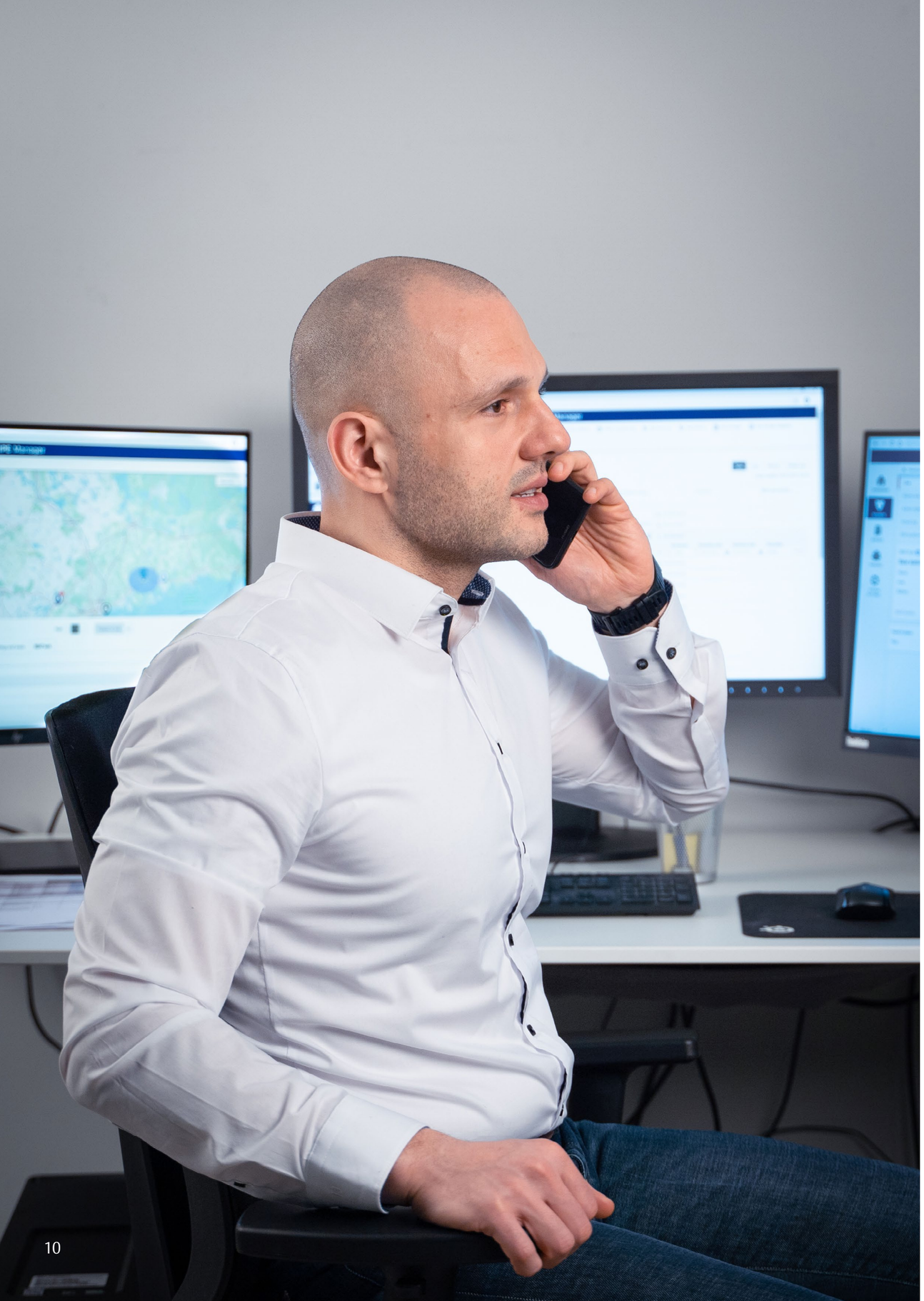
3. Authorisation
Authorisation determines what each user is allowed to do within an application or with received data, for example, if a user is allowed to first receive access rights and then share them personally. With access rights, users can be limited to only receive and use their personal access rights and never share them forward. This tightens physical security as well.

2.3 What is encryption?

Encryption scrambles readable data so that it appears as random, which helps to prevent unauthorised use of encrypted data. There are two popular methods to encrypt data. First there is symmetric encryption, where all devices use the same secret key for encryption and decryption. Secondly there is asymmetric encryption, where each device has their unique encryption key.

The ABLOY BEAT solution utilises asymmetric encryption, which means that access right data is always uniquely encrypted from point to point. In an end-to-end encrypted security channel data that travels from the management system to the lock and the smartphone will be encrypted in multiple instances.

All BEAT locks are uniquely encrypted with a private key. This means that a lock's data cannot be decrypted with another lock's decryption keys. If someone decrypts one lock in a security system, all other locks still have their unique keys and remain protected. A single compromised lock will not break the system nor affect any other devices within the system.



What are cybersecurity risks and attacks?

Brute-force attacks
Hackers can try to crack passwords and credentials by guessing out different combinations until they find the right login information to gain unauthorised access. This type of attack can be efficiently stopped with encrypted credentials. Even if in theory the system could still be hacked with brute force, in practice it would take some 10 000 years to decrypt all data to break through.

Stolen lock
A hacker might try to steal a lock, but a stolen lock will not cause harm to any other locks in the security system. That's because all locks are unique and have their unique decryption keys. To put it simply, a stolen lock has no effect on other locks.

Stolen or compromised handset
A smartphone with access rights might get stolen. Firstly, most modern smartphones require biometrics and passwords to be unlocked. Secondly, all granted access rights will automatically expire after a certain period. But if a phone is lost or stolen, access rights can be immediately invalidated through the BEAT backend once a user realises their device is missing. If a smartphone would get hacked, it can also be mitigated and invalidated from the security system.

3. Digital locking solutions in the market now

Digital locking solutions provide exceptional security and privacy protection for critical infrastructure. There are wired and wireless solutions, and wireless solutions commonly utilise NFC-technology or Bluetooth®. Wired solutions have limitations and site requirements on where they can be placed. NFC is a wireless solution that can work without a continuous power source, but these devices activate only when they are in very close proximity.

Battery-powered Bluetooth® locks offer a continuous power source and wireless flexibility, which is why it is the chosen technology for our growing BEAT digital portfolio. Competing solutions appear to be solving the same challenges our customers face, but unlike BEAT, these locking devices might not have been designed for keyless purposes, resulting in suboptimized user experience, security and endurance.

Future-proof connectivity and designed for keyless access

- You can open locks with a smartphone. BEAT solutions battery life lasts more than 5,000 access cycles or five years, depending on the frequency of use.
- BEAT starts off as an offline solution, and the locking devices can be placed within or outside network coverage. Locks can be operated without an active cellular connection if access rights are updated on the smartphone before entering an offline area.
- Bluetooth® offers future possibilities for connectivity, like remote opening and IoT monitoring with access management software and gateway devices. This way you could react to vandalism and unauthorised access much quicker – and have peace of mind of by having total awareness of your security situation without site visitations.

4. Introducing ABLOY BEAT

ABLOY BEAT is a keyless solution specifically made for critical infrastructure protection. All BEAT products are operated with a mobile application over a Bluetooth® connection. Keyless BEAT solutions are designed for safe wireless access management, and to make sure that BEAT is safe now and in the future, we implement multiple cyber security layers.

Why is BEAT secure to use?

1. Encryption protects all data that travels between devices by encoding information or scrambling readable text to hide and protect it from unauthorised users. We use advanced, next generation Seos® encryption technology with improved IoT capabilities, as well as industry standard security protocols and practices.

2. Authentication identifies the user and the access management system. All locks and clients in the system have an individual verified and trusted identity, and only authorised clients can get access to BEAT locks. We authenticate all user traffic and follow a trust no one policy, meaning that there is not a single device or user that can bypass our authentication process.

3. Authorisations are securely delivered from BEAT's backend system to locks. Each authorisation in a mobile device is valid through a limited short period. All data sent from the locks is end-to-end encrypted, so even the authorised mobile clients cannot read the contents. Compromised and stolen devices can be mitigated and invalidated through the backend.

Firmware updates for known vulnerabilities
We detect possible issues and vulnerabilities with researchers. Fixes for the firmware of our products are easily updated on the go. Whenever a lock is used it reaches online mode and updates on the background.

BEAT security aspects

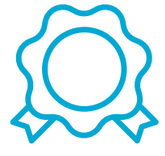
Convenient user identification without compromising security

Offline function gives protection against losing network coverage

Over-the-air firmware upgrade with any trusted user mobile phone

E2e encrypted messaging

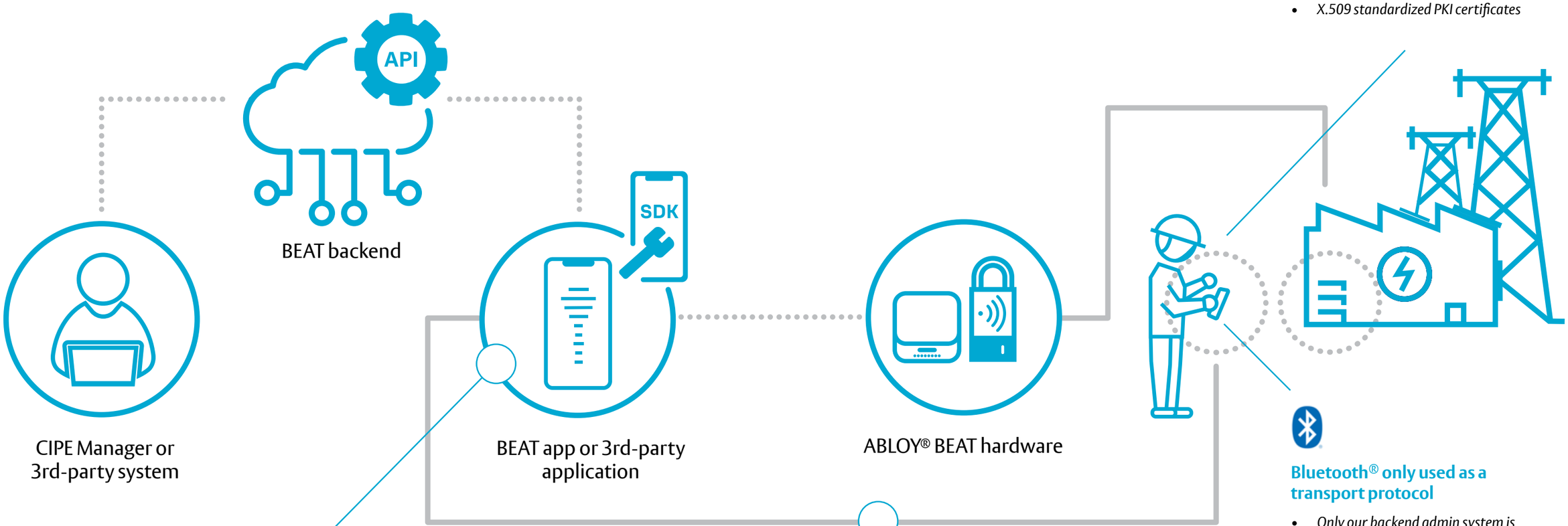
Global PKI as the modern IoT approach for authentication



Reviewed by 3rd party security institutes

How does BEAT work?

Mobile credentials, or access rights, are stored on user's smartphone in a Secure Enclave, and the information of a credential is stored in a cloud. All information between devices travels through the Internet. What makes a product cybersecure is that in each stage the credential is used, security protocols are set in place and followed to prevent attacks.



Public Key Infrastructure (PKI) and private key identity

- *Asymmetric encryption with no shared secrets*
- *X.509 standardized PKI certificates*

Bluetooth® only used as a transport protocol

- *Only our backend admin system is trusted by the lock*
- *Less prone for man in the middle an attack*

Trusted Service Manager (TSM)

- *Enabling secure registration of a mobile device*
- *Invitations originated from original organization only*

End-to-end security channel

- *Only our backend admin system is trusted by the lock*
- *Less prone for man in the middle an attack*

5. Playbook: is the BEAT solution right for you?

Our evolving BEAT portfolio has future-proof products that offer security and connectivity. These questions can help you decide if BEAT is the solution you are looking for:

- Would you like to gain improved situational awareness through mobile access control?
- Do you want to eliminate the risk of lost keys and get rid of physical key management?
- Would you like to track the flow of people and employees at your premises?
- Do you need to manage keys, locks and access rights independent from your physical whereabouts?
- Could you cut down costs and save travel time with simpler logistics?
- Are you looking for an access solution that can be integrated to your existing systems?
- Do you want to stay in the forefront of critical infrastructure protection?

If you answered any of the questions above "yes" or "maybe", reach out to our experts to learn more:

CONTACT US

6. Why your safety matters to us: our security policy

Responsible disclosure of vulnerabilities ensures that security access infrastructure is tested and proven reliable. That's why ASSA ABLOY values the insight and commitment of security researchers and other vulnerability investigators to make the world a safer place. For us disclosure is essential for improving the quality of our products and services, and the safety of our customers that rely on them.

We have set a security policy for responsible disclosure, which entails for example that:

- ASSA ABLOY will disclose known vulnerabilities and their fixes to its customers in a manner that protects ASSA ABLOY and its customers.
- ASSA ABLOY is open to communication and working with security researchers who come to us with a shared interest to improve security and coordinate distribution of information that includes both the vulnerability and the solution that addresses it.
- Read our full security policy.

7. Glossary

- **Asymmetric encryption** = In asymmetric encryption multiple separate keys are used for encryption and decryption. Asymmetric encryption is also known as public key infrastructure encryption.
- **Authentication** = An important layer of cybersecurity, that identifies the user and the access management system.
- **Authorization** = An important layer of cybersecurity, that determines what each user is allowed to do with received data.
- **BLE** = Bluetooth® Low Energy is a low-power wireless connectivity standard.
- **Cloud** = Cloud stores data on internet servers, that can be accessed remotely when needed.
- **Encryption** = An important layer of cybersecurity, that scrambles readable data so that it appears as random, which helps to prevent unauthorised use of encrypted data.
- **End-to-end encryption** =E2EE is a security method that prevents data from being secretly modified or accessed by any other than the true sender and recipient. Data is encrypted by the sender and stored encrypted, only decrypted by the recipient.
- **Hacker** = A person who tries to break into a computer system, for example, to gain unauthorised access to certain data.
- **IoT** = Internet of things describes devices with sensors that are connected, communicating and exchanging data with other devices.
- **NFC** = Near field communication is a short-range wireless technology that allows devices to communicate with each other.
- **PKI** = Public key infrastructure is an asymmetric encryption method that consists of policies, procedures, hardware and software that are used to create and distribute digital credentials
- **SaaS** = Software as a service delivers cloud-based applications as a service over the internet. The provider of the SaaS runs the application on their servers and manages access and security of the app. For example, ABLOY BEAT is a SaaS.
- **Seos®** = An advanced encryption technology developed by HID Global, an ASSA ABLOY business.
- **Symmetric encryption** = In symmetric encryptionall devices use the same secret key for encryption and decryption.
- **Trust no one** = A TNO model removes the danger of overlooking “trusted” users by requiring all users to be verified and authenticated, always.
- **TSM** = A trusted service manager coordinates technical connections and business agreements with e.g. mobile network operators, service providers and device manufacturers. BEAT TSM’s enables the secure registration of a mobile device.
- **X.509** = An international standard that defines public key certificates. In cryptography these certificates are used in different Internet protocols, like HTTPS and TLS. For example, BEAT has a TLS 1.3 certificate.

The ASSA ABLOY Group is the global leader in access solutions. Every day we help people feel safe, secure and experience a more open world.

ASSA ABLOY
Global Solutions

assaabloyglobalsolutions.com