ALCEA
ASSA ABLOY

cybersecurity in keyless access management.

alceaglobal.com

contents.

4 Introduction.
5 Why is cybersecurity important?
6 Cybersecurity worries and challenges of critical infrastructure today.
7 Wireless access management: What are mobile credentials?
8 Implementing essential cybersecurity layers.
9 What is encryption?
11 What are cybersecurity risks and attacks?
12 Digital locking solutions in the market now.
14 Introducing ABLOY CUMULUS.
16 CUMULUS security aspects.
18 How does ABLOY CUMULUS work?
20 Playbook: is the CUMULUS solution right for you?
21 Why your safety matters to us: our security policy
22 Glossary.

introduction.

Digitalization is changing how critical infrastructure is operated and secured. Across industries, organizations are introducing connected technologies to simplify daily operations, improve visibility, and better control access to sites and assets.

As access control moves from mechanical to digital and wireless solutions, cybersecurity becomes a central concern. Wireless devices and mobile credentials create new opportunities for flexibility and efficiency, but they also require a different approach to security. Protection is no longer limited to the lock itself - it extends to software, communication, user behavior, and system architecture.

In this white paper, we explain how wireless access solutions can be deployed securely, and what cybersecurity principles matter most in access management.

Protecting data through encryption

For many employees, the smartphone is already a key work tool. It is used to communicate, plan, authenticate, and support daily tasks, often across multiple locations.

Using a smartphone as a digital key builds on this reality. Digital credentials allow authorized users to access sites and premises without physical keys, whether those locations are nearby or remote. Access rights can be managed centrally, updated quickly, and adapted to changing operational needs, while maintaining control and traceability.

Understanding access environments and connectivity needs

Not all sites are the same. Some are connected, others operate with limited or no network access. Some require real-time control, while others prioritize availability and resilience.

Before deploying digital access solutions, organizations need a clear understanding of their current situation: how access is managed today, where connectivity exists, and where secure communication between devices and systems is required. Gateways play an important role in this context by enabling controlled data exchange, system monitoring, and secure management of access points. A clear assessment helps ensure that security, usability, and operational requirements are balanced from the start.

Cybersecurity built on trust, people, and responsibility

Cybersecurity is not only about technology. It also involves people and everyday practices. Even the most advanced system depends on correct use and clear responsibility.

Trust sits at the center of digital access management, trust in the devices that control access, in the systems that manage permissions, and in the people who use them. When cybersecurity is built into solutions from the beginning, wireless access can make critical infrastructure safer, more efficient, and easier to manage.

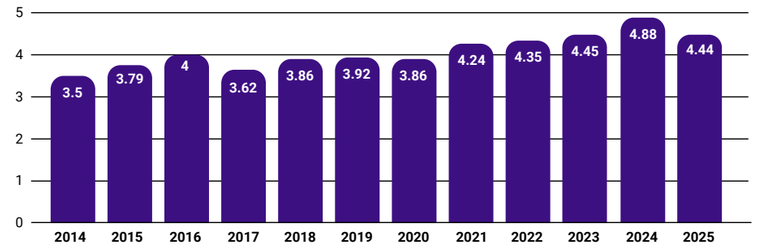
why is cybersecurity important?

Everything today is interconnected and digital. Organizations rely on online networks and connected devices to operate efficiently — but this connectivity also exposes them to growing cybersecurity risks. Threats that compromise individual safety or disrupt company operations and public infrastructure remain constant, even as technology advances. That's why cybersecurity measures must be built into every solution to protect integrity, continuity, and trust.

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 disrupt infrastructure and critical operations. The global average cost of data breaches has changed direction for the first time in five years. In 2025, it dropped to USD 4.44 million, as security teams used AI and automation to detect and contain breaches faster — even while attackers began using generative AI to launch more convincing phishing and deepfake attacks. Despite the global decrease, costs reached a record high in the United States. (Source: IBM)

Average cost of a data breach worldwide, 2014-2025
(in million U.S. dollars)



Source: IBM, Cost of a Data Breach Report 2025, ibm.com/reports/data-breach

cybersecurity realities in today's critical infrastructure.

Security, safety, and operations managers in critical infrastructure environments oversee complex, interconnected operations. Many services must run continuously, which makes resilience, availability, and protection of assets and personnel essential.

Infrastructure systems rely on connected devices for monitoring, tracking, and access management, all while complying with local laws and regulations. Any disruption — whether physical or digital — can have serious operational and safety consequences.

From an information security perspective, evaluating cybersecurity is often challenging. Comparing solutions and understanding the real impact of different security mechanisms is not always straightforward, particularly as threats and technologies continue to evolve. Increasing computing power places growing demands on encryption and other protective measures, making long-term security a critical consideration.

This white paper highlights key cybersecurity aspects of keyless access management to support informed decision-making in critical infrastructure environments.

keyless solutions: securing data from end to end.

Cryptography is the foundation of cybersecurity in digital access management. It is used to protect data, verify identities, and ensure that communication between devices and systems cannot be read or manipulated by unauthorized parties. In wireless access solutions, cryptography ensures that commands, credentials, and system updates remain confidential and trustworthy, even when transmitted over public or shared networks. Without strong cryptographic mechanisms, digital access control would be vulnerable to interception, duplication, or manipulation.

Rather than being a complex or abstract concept, cryptography is the first foundational layer of security in wireless access management. It creates a trusted digital environment where data is protected by design. On top of this secure foundation, additional security layers such as authentication and authorization ensure that only verified users and devices can request access, and that permissions are strictly controlled. Together, these layers enable wireless access systems to operate safely, reliably, and at scale in critical environments.

Protecting data through encryption

Encryption protects data by transforming it into an unreadable format for anyone who does not have the correct authorization to access it. In wireless access systems, encryption is used to secure communication between access devices, gateways, mobile devices, and management platforms.

This means that access credentials, commands, and status information cannot be interpreted even if data traffic were intercepted. Strong encryption ensures confidentiality and integrity: data cannot be read, altered, or replayed without detection. For critical infrastructure, this protection is essential to prevent unauthorized access and to maintain trust in digital access systems operating in exposed or remote environments.

Secure firmware updates of access devices

Cryptography also plays a critical role in keeping access devices secure over time. Wireless locks, padlocks, and controllers rely on firmware, embedded software that controls how the device functions.

Secure firmware update mechanisms ensure that only authorized and verified software can be installed on a device. Cryptographic verification prevents tampered or malicious firmware from being loaded, protecting devices from compromise. Regular updates allow vulnerabilities to be addressed, security mechanisms to be strengthened, and devices to remain compliant with evolving cybersecurity requirements.

By combining strong encryption with secure firmware update processes, wireless access solutions can maintain a high level of security throughout their lifecycle, from initial deployment to long-term operation in critical environments.

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 verifies the identity of both the user and the access management system before access rights are granted or used. This ensures that communication only takes place between trusted parties. User authentication may include identification within the access application, device-level security such as passwords or PINs, and biometric methods including fingerprint or facial recognition. The access management system validates the received data, and if authentication fails or invalid information is detected, access is denied.

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.

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.

In ALCEA keyless access solutions, asymmetric encryption is used to protect access right data. This means that data is uniquely encrypted from point to point, so that only the intended devices and systems can read it. Communication between the access management system, gateways, access devices, and mobile credentials takes place through end-to-end encrypted channels, with encryption applied at multiple stages.

Each access device is protected with its own unique cryptographic keys. As a result, data encrypted for one device cannot be decrypted by another. If a single device were ever compromised, the impact would be contained to that device alone, while the rest of the system remains protected. This device-level isolation is a key principle for securing distributed access systems used in critical infrastructure environments.

what are cybersecurity risks and attacks?

Brute-force attacks

In a brute-force attack, an attacker attempts to gain access by systematically guessing passwords or credentials. In well-designed access systems, this risk is mitigated through strong encryption and credential protection. Encrypted credentials cannot be meaningfully exploited through guessing alone. While such attacks are theoretically possible, overcoming modern encryption would require an impractical level of time and resources, making them ineffective in real-world scenarios.

Stolen devices: locks, phones, and credentials

Loss or theft of devices is a realistic risk in operational environments. Wireless access systems are designed to limit the impact of such events. Each device uses unique cryptographic keys, meaning a compromised lock cannot affect other devices or the wider system.

Mobile devices follow the same principle. Smartphones rely on built-in security features such as PIN codes, passwords, and biometrics. Access rights are time-limited and can be remotely revoked if a device is lost or compromised. This ensures that risks remain contained and manageable across distributed environments.

Social engineering and human factors

Some attacks target people rather than technology. Social engineering attempts to manipulate users into revealing credentials or bypassing procedures, making it one of the most common real-world risks.

Access systems reduce this exposure by limiting reliance on shared secrets and manual processes. Strong authentication, controlled authorization, and centralized access management help prevent misuse. Combined with clear procedures and user awareness, these measures significantly reduce the impact of human error.

Software vulnerabilities and open-source components

Modern access solutions rely on software, including open-source components. While these enable flexibility and innovation, vulnerabilities can arise if not actively managed.

Effective cybersecurity depends on continuous monitoring, secure development practices, and the ability to deploy updates quickly. Controlled connectivity and robust system architecture ensure that vulnerabilities can be addressed efficiently, maintaining long-term security and trust.

digital locking solutions on the market now.

Digital locking solutions are widely used to secure critical infrastructure, offering improved control, traceability, and protection of sensitive assets. These solutions can be deployed in both wired and wireless environments, depending on site conditions, operational requirements, and security needs.

In critical infrastructure, physical conditions and connectivity vary significantly. Some sites are connected, others are remote or operate with limited network access. Wired solutions can provide continuous connectivity, but they are often constrained by installation requirements, fixed locations, and infrastructure availability. Wireless solutions address many of these limitations by enabling flexible deployment across dispersed environments.

Battery-powered Bluetooth® locks are commonly used in keyless access solutions because they combine wireless flexibility with reliable power autonomy. Designed specifically for digital access, they support secure credential handling, scalable deployment, and long-term operation in demanding environments. When access devices are purpose-built for keyless use, they deliver better usability, security, and endurance compared to solutions adapted from traditional locking concepts. At the same time, modern keyless solutions are designed to work seamlessly alongside trusted mechanical locking systems, enabling organizations to transition at their own pace without compromising security or operational continuity.

Creating a connected digital locking ecosystem

Modern digital locking solutions operate as part of a connected access ecosystem, where locks, mobile credentials, secure connectivity components, and management software work together.

These components enable secure communication between access devices and central systems, supporting monitoring, credential updates, and access management across multiple sites, even in environments with limited or intermittent connectivity.

By combining Bluetooth® access devices with gateway-enabled connectivity, organizations gain improved visibility and faster response to events such as unauthorized access or tampering, reducing the need for physical site visits and strengthening overall situational awareness.

Designed for the realities of critical infrastructure

Keyless access solutions must be designed with the complexity of critical infrastructure in mind. This includes long operational lifecycles, harsh environments, remote locations, and strict security requirements.

Access devices are built to operate for years on battery power, supporting thousands of access cycles without compromising performance. At the same time, systems are designed to function both online and offline, allowing access rights to be used securely even outside network coverage. When connectivity is available, gateways enable synchronization, monitoring, and system updates, supporting future-ready and connected security operations.

Together, these capabilities enable organizations to deploy digital locking solutions that are flexible, resilient, and scalable, supporting secure access today while remaining adaptable to future operational and security needs.

introducing
ALCEA keyless solutions.

ALCEA keyless solutions are designed to protect critical infrastructure environments where access must be secure, flexible, and reliable, often across remote, distributed, and demanding sites.

The ALCEA keyless portfolio includes solutions such as ABLOY CUMULUS, built specifically for wireless access management in critical infrastructure. These solutions use mobile credentials and Bluetooth® connectivity to enable secure, keyless access to locks and assets, while supporting both online and offline operation depending on site conditions.

From the outset, ALCEA keyless solutions are designed with cybersecurity in mind. Multiple security layers are implemented to protect access rights, communication, and devices, ensuring that solutions remain secure not only today, but also as technologies and threats evolve.

Why is ALCEA keyless solutions secure to use?

Cybersecurity in ALCEA keyless solutions is based on a combination of encryption, authentication, and controlled authorization.

Encryption protects all data exchanged between system components by rendering it unreadable to unauthorized parties. Communication between access devices, mobile credentials, connectivity components, and management systems is secured using strong, industry-standard cryptographic methods. This ensures that access rights, commands, and device data remain confidential and cannot be altered in transit.

Authentication ensures that only trusted users and devices can participate in the system. Each lock, client, and system component has a unique, verified identity, and all interactions are validated before access is granted. Access rights are issued for limited time periods and can be revoked centrally if a device is lost, stolen, or suspected to be compromised.

Together, these mechanisms ensure that access is granted only to authorized users, data remains protected end to end, and the impact of compromised devices is contained, supporting secure and resilient keyless access management across critical infrastructure environments.

Firmware updates for known vulnerabilities
Potential vulnerabilities are identified through ongoing security research and testing. When updates are required, firmware fixes can be deployed securely to supported devices.

Firmware updates are applied when connectivity is available, without disrupting normal operation. This ensures that devices remain protected over time, while maintaining reliable access even in environments with intermittent or limited network coverage.

ALCEA keyless solutions 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 communication

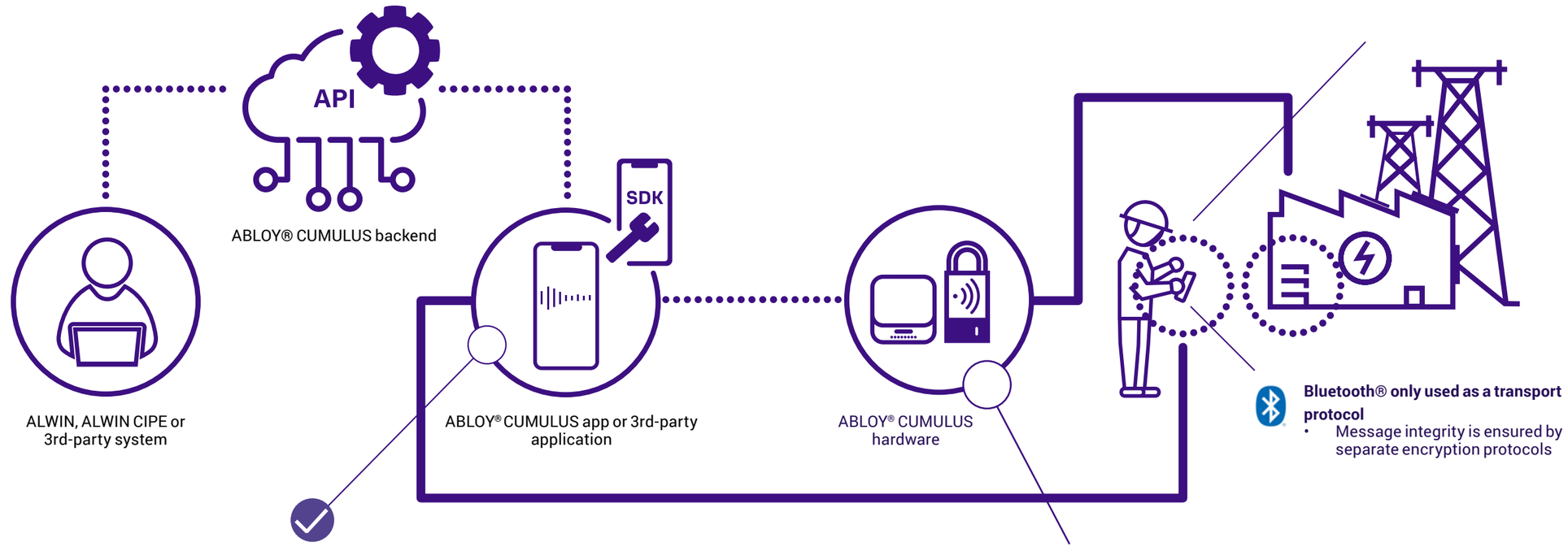
Global PKI as the modern IoT approach for authentication

Reviewed by 3rd party security institutes

how does ABLOY CUMULUS 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
- Message integrity is ensured by separate encryption protocols

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

playbook: is the ALCEA keyless solutions right for you?

Our evolving keyless solutions portfolio has future-proof products that offer security and connectivity. These questions can help you decide if a keyless solution is the right choice for your organization:

- Would you like to get real time information of your most valuable assets?
- 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

why your safety matters to us: our security policy

Responsible disclosure of vulnerabilities ensures that security access infrastructure is continuously tested and proven reliable. That's why ALCEA, as part of the ASSA ABLOY Group, takes cybersecurity and responsible disclosure seriously. We value the insight and commitment of security researchers and vulnerability investigators who help strengthen the security of critical access infrastructure.

Our security teams work closely across the ASSA ABLOY Group, combining expertise from physical security, digital access, and cybersecurity domains. ALCEA also actively contributes to industry collaboration and standardization efforts, helping to shape secure and trusted access technologies for the future.

For us, responsible disclosure is essential to improving the quality of our products and services, and to protecting the customers who rely on them. We have established a security policy for responsible disclosure, which includes the following principles:

ALCEA discloses known vulnerabilities and their fixes to customers in a responsible manner that protects both ALCEA and its customers.

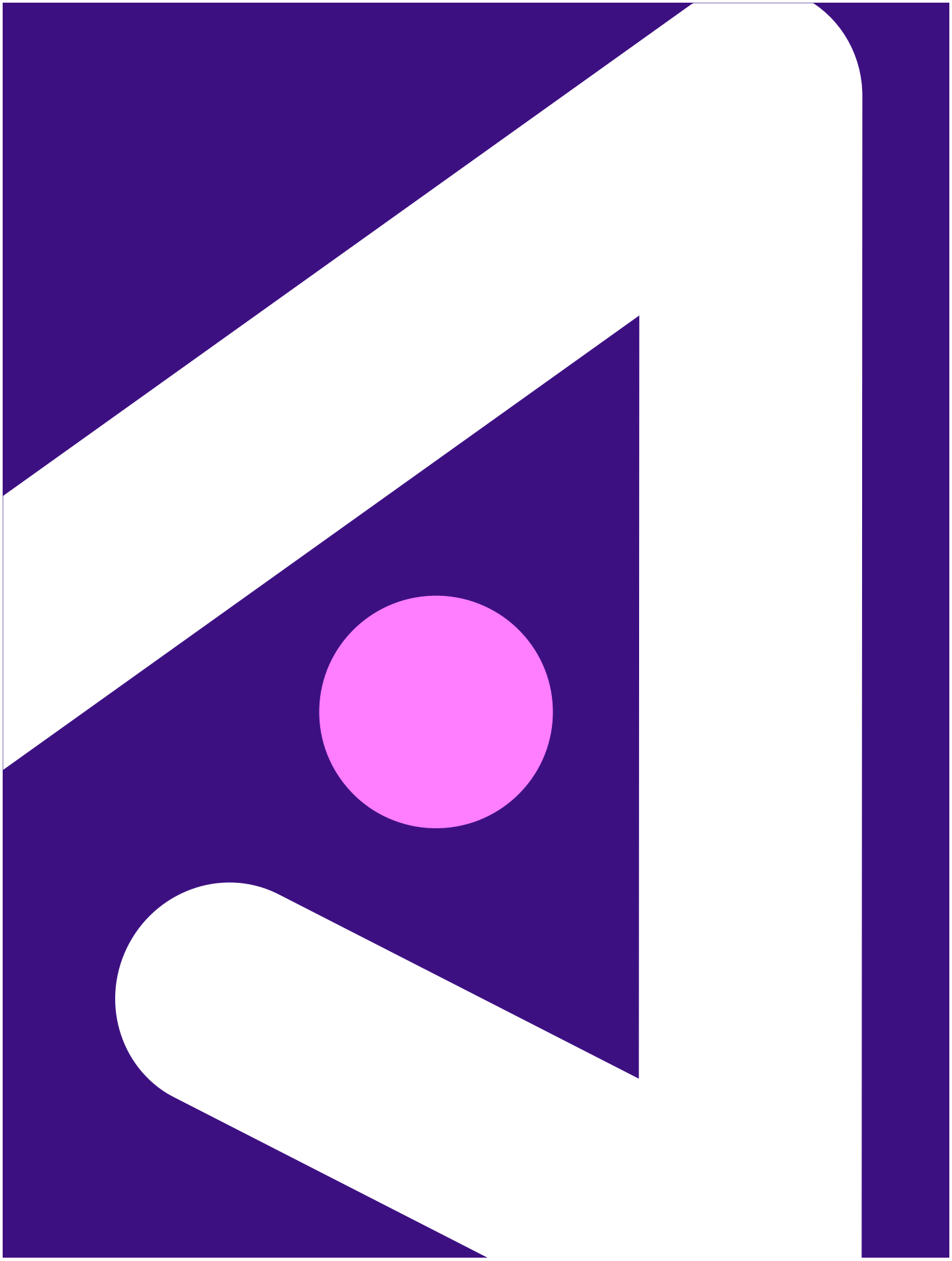
ALCEA is open to communication and collaboration with security researchers who share a common goal of improving security and coordinating the responsible distribution of vulnerability information and corresponding mitigations.

Read our full security policy.

Explore the NIS2 ebook

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.
- **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 CUMULUS is a SaaS.
- **Symmetric encryption** = In symmetric encryptionall devices use the same secret key for encryption and decryption.
- **TSM** = A trusted service manager coordinates technical connections and business agreements with e.g. mobile network operators, service providers and device manufacturers. CUMULUS 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, CUMULUS has a TLS 1.3 certificate.



ALCEA specializes in protecting critical infrastructure globally, including energy, water, telecom, transportation, mining, oil, and gas. We provide comprehensive security solutions tailored to your unique needs, from access control and intrusion detection to key and video management. Our experienced specialists deliver customized, digitalized solutions that enhance efficiency, ensure compliance, and offer peace of mind.

alceaglobal.com