

NIS2 requirements and guidance for physical protection and access control

ASSA ABLOY

Enhancing Cyber-Physical Resilience with Digital Access Solutions
Whitepaper - Version 08 / 2025

Experience a safer
and more open world



In this whitepaper,
you will learn about:

The NIS2 Directive	3
Who is impacted by NIS2?	5
NIS2 and the importance of physical security and protection	6
Comprehensive physical protection of your organization and data	7
Kickstart risk management	8
Identifying and closing potential weaknesses in physical access	9
How Digital Access Solutions enhance cyber–physical resilience.....	10
Enhancing protection from the perimeter to the core.....	11
Empower your security model with ASSA ABLOY solutions.....	12
Use case: Physically securing a critical area with digital access control	13
An overview of Digital Access Solutions from ASSA ABLOY	14
Next steps: NIS2 compliance action checklist	17



As of 17 October 2024, compliance with the NIS2 Directive became mandatory, requiring all EU Member States to transpose the directive into national law. This whitepaper is based on the current status of the NIS2 Directive (EU) 2022/2555 and its implementation across EU Member States as of mid-2025. While several countries have enacted national legislation, others are still in the process of transposition, with timelines and requirements subject to change. Readers should be aware that the legal and regulatory landscape may evolve and are advised to consult the latest official sources or legal counsel for up-to-date information. This whitepaper is for informational purposes only and does not constitute legal advice.

The European Commission has estimated that
over 160,000 entities
will fall under its scope

The NIS2 Directive

New demands and challenges have arisen

This EU-wide cyber security law replaces the original NIS Directive on Network and Information Security from 2016. This legislative update tightens the minimum requirements for IT security in critical infrastructure and expands them to include additional sectors. This means that, with the transposition of NIS2 into national laws across Europe, significantly more areas and companies than previously will be affected.

Critical to know: the new cybersecurity directive calls for an **all-hazards approach**. This means that those responsible should not only implement digital security measures, but also take precautions to physically protect their infrastructures.

These are the topics covered in the rest of this whitepaper:

- Which companies are subject to NIS2
- What specific requirements are involved
- How businesses can enhance cyber-physical resilience with Digital Access Solutions



The All-Hazards Approach:
Integrating Cyber and Physical Security




NIS2 is about much more than cyber security compliance. It requires physical security to work together with your cyber protections. It ushers in a new era of **cyber-physical resilience** standards.


Who is impacted by NIS2?


Potential fines


€10 million or 2% of global turnover


ANNEX I Sectors and sub-sectors of high criticality


 **Energy**
Electricity supply, district heating/
cooling, fuel/oil, gas


 **Transport / Traffic**
Air transport, rail transport,
maritime transport,
road transport

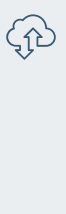
 **Finance / Insurance**
Banks, financial market
infrastructure

 **Healthcare**
Services, reference laboratories,
R&D, pharmaceuticals (NACE C
Division 21), medical devices

 **Water / Wastewater**

 **ICT Service Management
(B2B only)**
Managed service providers
and managed security service
providers

 **Space**
Ground infrastructure

 **Special cases***
Qualified Trust Service Providers
(qTSPs), Top-Level Domain
(TLD) registries, DNS providers,
telecommunications providers,
critical facilities, central
government bodies; Trust Service
Providers (TSPs).


Essential entity


- Has at least 250 employees; or
- Generates more than €50 million in annual turnover; and
- Has a balance sheet total exceeding €43 million


Essential Entity*


NIS2 applies to all companies in these sectors which exceed an annual turnover of €10 million regardless of their size.*


ANNEX II Other critical sectors and sub-sectors


 **Transport / Traffic**
Postal and courier services


 **Chemicals**
Manufacturing, trade, production


 **Research**
Research institutions

 **Manufacturing Sector**
Medical / diagnostics, IT,
electronics, optics (NACE C
Divisions 26 and 27)

 **Mechanical engineering
(NACE C 28)**
Automotive / parts (NACE C 29)
Vehicle manufacturing
(NACE C 30)

 **Digital Services**
Marketplaces, search engines,
social networks

 **Food**
Wholesale, production,
processing

 **Waste Management**
Waste disposal

Important entity


- Has at least 50 employees; or
- Generates more than €10 million in annual turnover and balance sheet total

Whether the NIS2 Directive applies to a company initially depends on its affiliation with one of 18 different sectors. These sectors are outlined in two annexes and divided into “*Sectors of high criticality*” and “*Other critical sectors*”, which follow the classification system of economic sectors in the European Community (NACE).

In addition to these areas of activity, the size and economic performance of an organization are also decisive for its classification. Based on these factors, NIS2 distinguishes between “*essential entities*” and “*important entities*.”

Legal exposure and executive accountability

According to Directive (EU) 2022/2555 (NIS2), entities may face fines of up to €10 million, or 2% of global annual turnover, for non-compliance. Member States must ensure that management bodies can be held liable for breaches due to gross negligence or lack of oversight. Supervisory authorities may also impose temporary bans on individuals in management from exercising leadership roles.

You can read the full legal text on [EUR-Lex](#) .


* Apart from this, smaller businesses may also be affected by NIS2. This applies if their failure would have significant consequences for the economy or public services. This includes, for example, certain digital services regulated by the eIDAS Regulation (EU regulation [No. 910/2014] for electronic IDentification, Authentication and Trust Services).

However, micro-enterprises – those with fewer than nine employees and an annual turnover of less than €2 million – are not affected.

NIS2 and the importance of physical security and protection

In principle, essential and important entities must, according to Article 21 of the NIS2 Directive, “take appropriate and proportionate technical, operational, and organizational measures to manage the risks to the security of network and information systems [...] and to prevent or minimize the impact of security incidents on the recipients of their services and on other services.” These measures must take into account both the state of the art and the specific threat landscape of the organization.

A key aspect is that these protective measures must follow an ‘all hazards approach’. This means not only defending against digital threats to network and information systems, but also protecting the physical environment of these systems from security incidents. The fact that the new directive so clearly emphasizes this aspect is no coincidence.

The European Union Agency for Cybersecurity (ENISA) explicitly highlights in a recent [threat assessment](#)  the rise of so-called **cyber-physical attacks**.

As products become increasingly interconnected through the Internet of Things (IoT), existing vulnerabilities offer potential entry points – for example, to gain access to physically secured high-security areas.

Despite existing hybrid plans for cyber and physical security in many companies, ENISA still considers physical access to be the ‘largest backdoor’, whose importance continues to be underestimated.

Particularly vulnerable in this context are publicly accessible terminals, memory units, or monitors, which can become easy targets for vandalism or sabotage, such as through malicious USB devices.




Physical access is considered the biggest backdoor for cybercriminals. Could your organization be at risk?

Comprehensive physical protection of your organization and data

Whether in industry, public administration, or healthcare, as control and storage hubs for electronic information exchange, modern data centres form the heart of many organizations. Effectively securing the physical and digital assets concentrated there is crucial for maintaining critical business functions and protecting a company's reputation.

The standards and “best practices” already established for securing these sensitive areas provide a solid foundation for implementing appropriate measures across the entire operational infrastructure, as envisioned by the NIS2 Directive.

As an initial point of reference, the European standard series EN 50600 (“*Facilities and Infrastructure of Data Centers*”)  is recommended. It describes a layered security model based on the “onion shell principle”. In this model, various security-relevant classes are built up layer by layer, increasing in protection from the outside in.

*Building cyber-physical resilience:
The layered security model
aligned with NIS2*

INCREASED SECURITY LEVEL AND RESTRICTED ACCESS



Cyber-Physical Resilience

Protecting IT and data security from cyber attacks

Protecting IT, data and infrastructure through physical measures

Protection Class -1

Public space

Protection Class 0

Open areas, semi-public

Protection Class 1

Restricted public access

Building entrance & outer shell of a building with doors / perimeter areas with fencing

Protection Class 2

Regulated access + accompanied access

Office & specialized areas with doors and cabinets

Protection Class 3

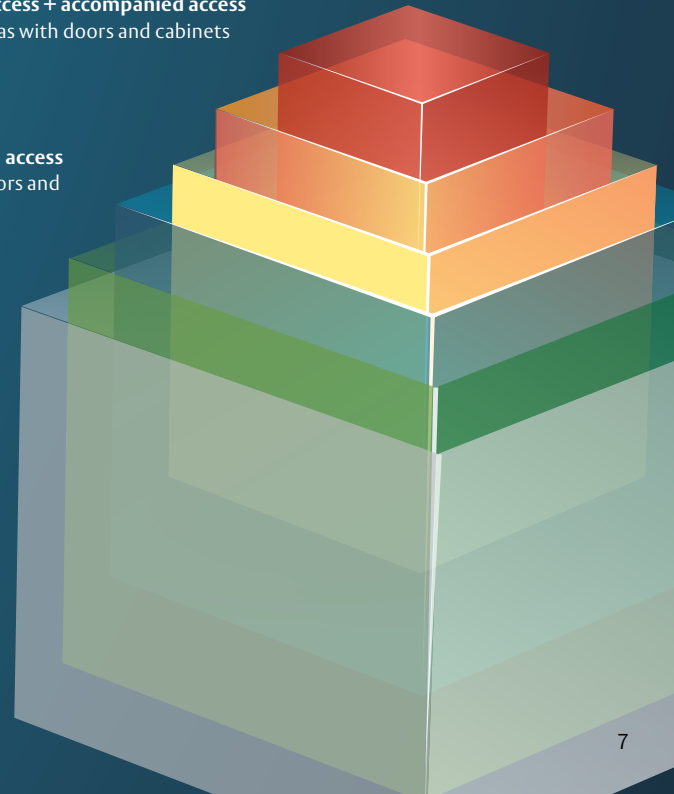
Restricted access + accompanied access

Technical areas with doors and cabinets

Protection Class 4

Strictly regulated access, critical core areas

Server / IT, network with server racks and cabinets



Kickstart risk management: Get everyone on board and take action

Under the NIS2 Directive, organizations are also required to strengthen physical security measures, such as access control

At a minimum, the following requirements must be met:

- Well-developed concepts for risk analysis and IT system security, as well as for managing security incidents
 - Measures to ensure business continuity (Business Continuity Management), including crisis management and backup procedures for data recovery
 - Supply chain security (handling of business partners and service providers, security measures during the acquisition and development of information systems)
 - Security in the procurement, development, and maintenance of IT and network systems, including vulnerability management
 - Guidelines for measuring cyber security and risk mitigation measures
 - Training in IT security and basic cyber hygiene practices (e.g. zero-trust principles, software updates, device configuration, network segmentation, identity and access management, or user awareness; [see NIS2 preamble, 89](#) ↗)
 - Cryptography and data encryption
 - Secure authentication and communication
 - Maintenance of system functionality during power outages, if it is electronic and wired
-
- Personnel security, including **concepts for physical access control** and facility management (ISMS / Information Security Management System)

Identifying and closing potential weaknesses in physical access

The earlier that organizations begin preparing for NIS2, the better – and **measures for the physical protection of facilities play a central role** in this process. During their assessments, security officers should thoroughly evaluate existing security measures, including **access control and locking systems**, to determine their long-term effectiveness.

Older mechanical locking systems can potentially pose significant liability risks for operators, especially if patent protection has expired. In such cases, locksmiths are no longer required to contact the manufacturer, and key copies can be made without verification. This represents a serious security risk. Companies may have to bear the costs of potential service disruptions themselves if they cannot demonstrate adequate protective measures.

Experience shows that the older such locking systems are, the more difficult it becomes to keep track of the number of keys in circulation and to respond quickly to key losses. The checklist opposite can help an organization to determine whether, and where, urgent action is needed.

Businesses **must** demonstrate
adequate physical security measures
are in place

Checklist:

How future-proof is my physical access?



Is a well-developed security concept for physical access in place?



Are access events traceable and documented?



How quickly can key/credential losses be responded to?



Are unauthorized keys/credentials potentially in circulation?



How comprehensive is the key/credential management system?



Is hardware up to date and can critical access points beyond doors be secured (e.g. cabinets, server racks, gates etc.)?



Is continuous operation secured in the event of a power outage (blackout)?



If using a mechanical locking system, does it have valid patent protection?

How Digital Access Solutions enhance cyber-physical resilience

To establish a comprehensive security structure, digital and networked solutions offer clear advantages over mechanical systems. This begins with the simple management of access rights and permissions for individual employees and extends to theft protection and even fire safety.

Especially in the area of physical security – protecting employees, assets, and both analogue and digital data from external threats and incidents – **digital locking systems and electronic access control solutions (Digital Access Solutions)** offer greater convenience and enhanced protection.



Digital access solutions can contribute significantly to achieving compliance with the NIS2 Directive

Enhancing protection from the perimeter to the core

Digital access solutions empower you to secure every layer

Security from the first to the last line of defence: Everything that can be locked should be protected against tampering and intelligent attacks.

Benefits of ASSA ABLOY Digital Access solutions protecting your organization and data:

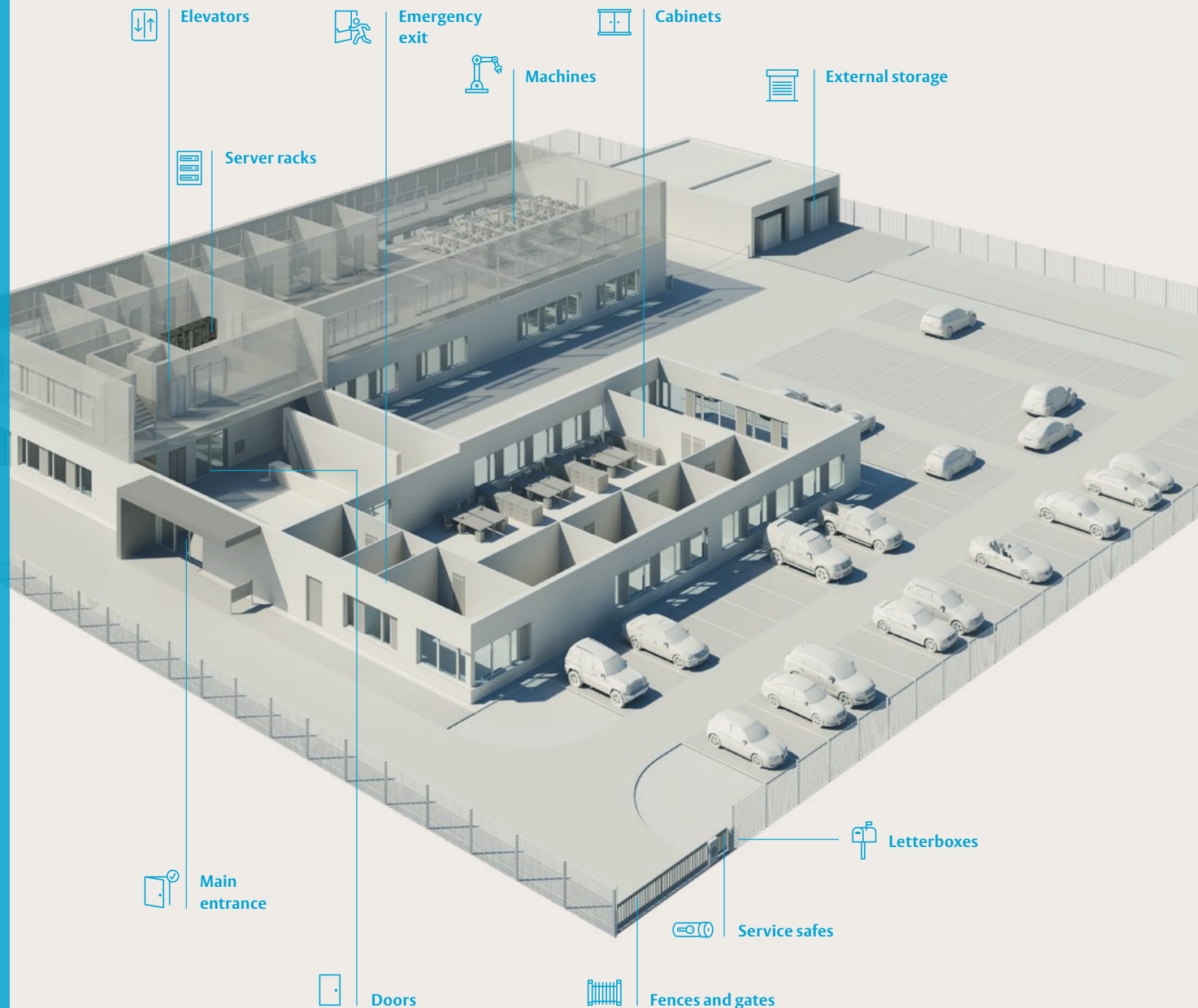
- Control who goes where, and when, for each user or cancel lost credentials with a click
- Online or offline access control and improved workflows through flexible management, remotely or on-site
- Offering provides digital access systems or access hardware to upgrade an existing system
- Access hardware to secure protection classes 1-4
- Gain scalable control over access points that were previously unreachable
- Simple installation of wireless solutions requires no wiring or structural modifications
- Benefit from our in-depth knowledge of regional door and security standards
- Supporting you in achieving NIS2 compliance

Protection Class 4

Protection Class 3

Protection Class 2

Protection Class 1



Empower your security model with ASSA ABLOY solutions

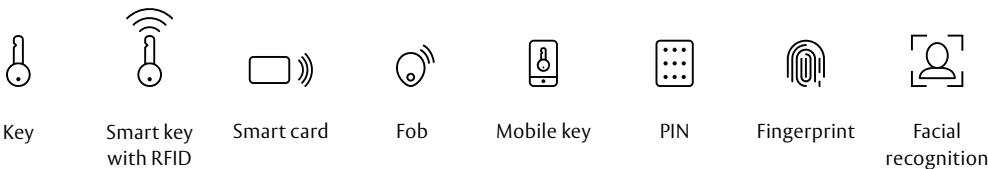
The digital access offering from ASSA ABLOY includes scalable system management, credential types, and hardware designed to achieve NIS2 compliance

Available system management

Access permissions can be flexibly defined by assigning rights with easy-to-use management systems from ASSA ABLOY that can be installed locally, in the cloud, or both. If employees or an entire department relocate, it is not necessary to replace the locks. Lost credentials no longer pose a security risk, as they can simply be deactivated. Time- and location-based access permissions are also possible—for example, to grant technicians individual authorization for a specific task. In large companies, it can be useful to issue time-limited access permissions.

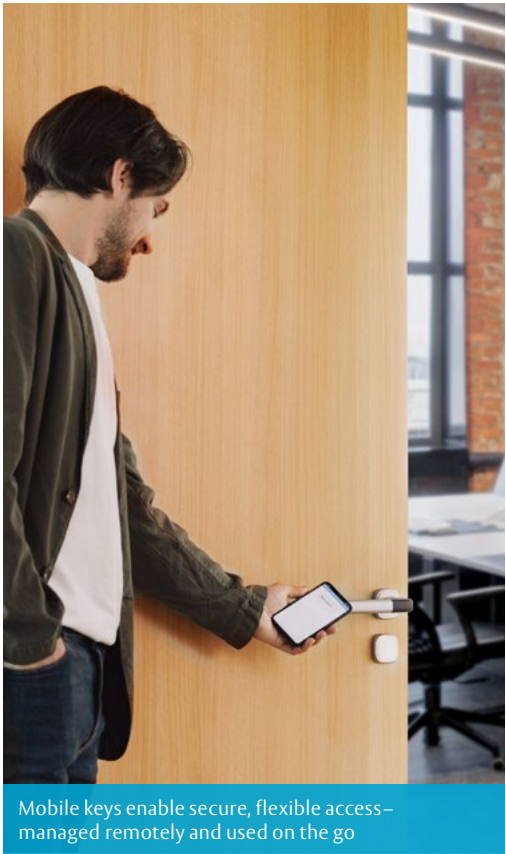
Available credential types

Enhance security by choosing from ASSA ABLOY credentials such as smart keys, smart cards, mobile keys, or even biometrics—and gain the flexibility to combine multiple credentials within a single access solution.



Available access hardware in various types

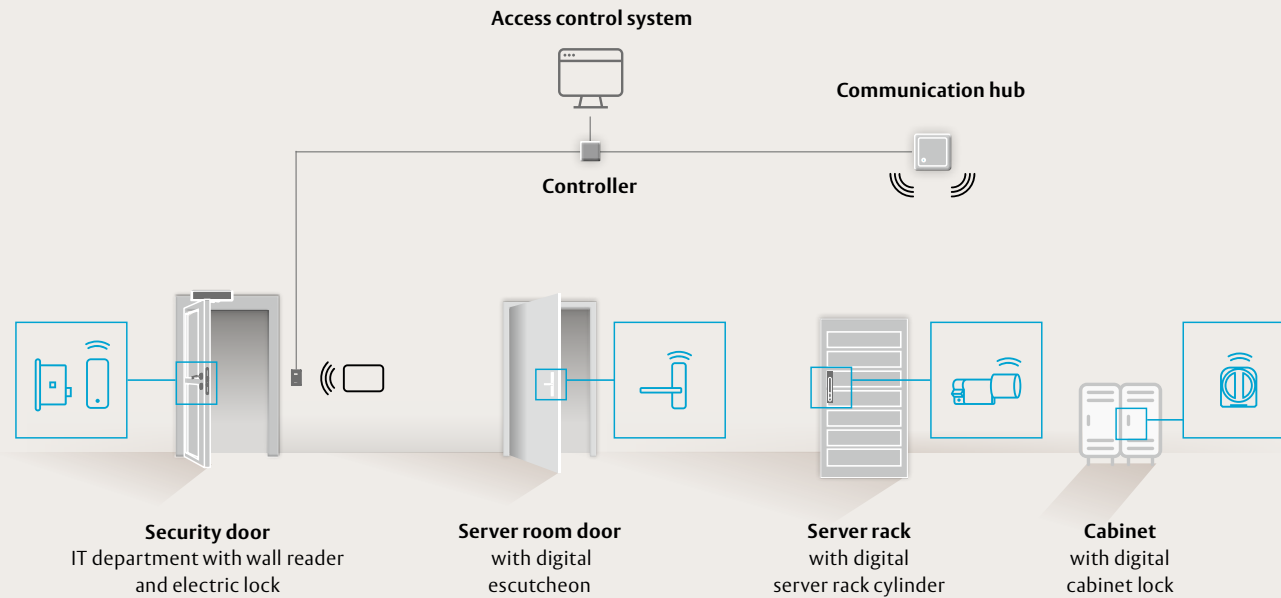
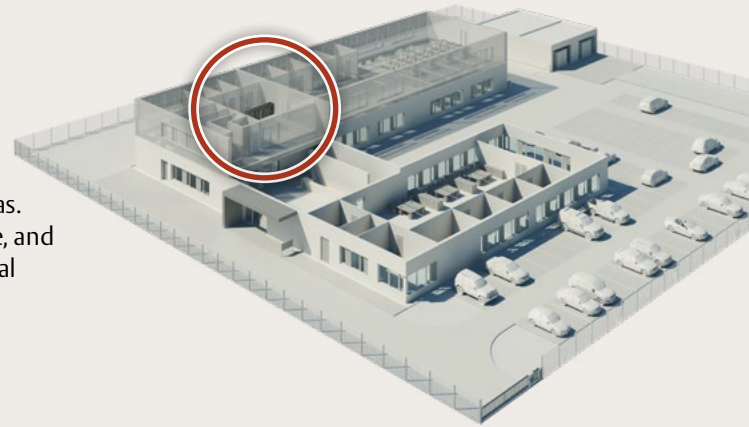
ASSA ABLOY’s wired and wireless access hardware expands flexible control across more entry points within and beyond your building, supporting a layered security approach based on the ‘onion shell principle’.



Use case: Physically securing a critical area with digital access control

IT department and assets **Protection Class 4**












To protect sensitive IT infrastructure and assets, implementing digital access control ensures that only authorized personnel can physically access critical areas. This approach enhances security, supports compliance, and reduces the risk of data breaches by integrating physical safeguards with IT policies.



Secure IT environments—including server racks—with robust physical protection and digital access controls to safeguard sensitive data.

An overview of Digital Access Solutions from ASSA ABLOY









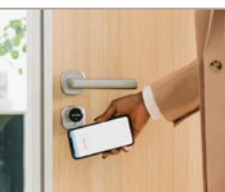
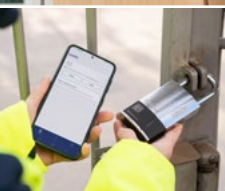
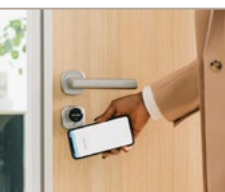
Choose what works best for your environment to enhance protection from the perimeter to the core

<p>Key features of physical access control help safeguard employees, assets and data, both analogue and digital, from external threats and incidents</p> <p>ASSA ABLOY Digital Access Solutions</p>		<p> Access control and identity management ensures only authorized people can access specific systems, spaces, or data</p>	<p> Auditability and traceability ensures that all critical actions and access to systems are logged and can be reviewed – enabling accountability, incident investigation, and compliance verification</p>	<p> Digital credentials deployed to authenticate users, devices, or systems and to control access to sensitive data and services</p>	<p> Revoking or deactivating of credentials ensures access rights are promptly removed when no longer needed, protecting systems from unauthorized use</p>	<p> Secure remote access ensures employees and third parties can access critical systems and data remotely using encrypted connections, strong authentication, and strict access controls to prevent unauthorized access and data breaches</p>	<p> Secure communication/ encryption ensures data exchanged between devices, credentials, and software is protected through strong cryptographic methods, preventing unauthorized access, tampering, or data leaks during transmission</p>	<p> Access hardware and protection classes secure areas based on layered security model</p>
<p>Digital Access Management Systems</p>	 <p>CLIQ Straightforward key-based system which transforms mechanical to high-security digital access management</p>	✓	✓	Smart keys, optional with RFID	✓	✓	✓	<p>More than 60 types of cylinder and padlock Powered by battery in the key Protection classes: 1, 2, 3, 4</p>
	 <p>ABLOY PULSE Unique digital locking and access management system that does not require batteries or cabling</p>	✓	✓	Smart keys	✓	✓	✓	<p>Cylinders and padlocks Powered by energy-harvesting Protection classes: 1, 2, 3</p>
	 <p>SMARTair Modern out-the-box digital access solution which maximizes flexibility and ease of use</p>	✓	✓	Smart cards and fobs, mobile keys, PIN (*CLIQ smart keys available soon)	✓	✓	✓	<p>Locks, escutcheons, cylinders, padlocks and readers Powered by battery in access hardware Protection classes 1, 2, 3, 4</p>
	 <p>ASSA ABLOY Access Smart, scalable digital access management system that unifies smart key, tag and mobile access on a single cloud platform</p>	✓	✓	Smart cards and fobs, mobile keys, smart keys	✓	✓	✓	<p>Cylinders, padlocks, readers, key deposits, swing handles Powered by energy-harvesting or battery Protection classes 1, 2, 3, 4</p>

» continued on the next page »

An overview of Digital Access Solutions from ASSA ABLOY

Choose what works best for your environment to enhance protection from the perimeter to the core

<p>Key features of physical access control help safeguard employees, assets and data, both analogue and digital, from external threats and incidents</p> <p>ASSA ABLOY Digital Access Solutions</p>		<p> Access control and identity management ensures only authorized people can access specific systems, spaces, or data</p>	<p> Auditability and traceability ensures that all critical actions and access to systems are logged and can be reviewed – enabling accountability, incident investigation, and compliance verification</p>	<p> Digital credentials deployed to authenticate users, devices, or systems and to control access to sensitive data and services</p>	<p> Revoking or deactivating of credentials ensures access rights are promptly removed when no longer needed, protecting systems from unauthorized use</p>	<p> Secure remote access ensures employees and third parties can access critical systems and data remotely using encrypted connections, strong authentication, and strict access controls to prevent unauthorized access and data breaches</p>	<p> Secure communication/ encryption ensures data exchanged between devices, credentials, and software is protected through strong cryptographic methods, preventing unauthorized access, tampering, or data leaks during transmission</p>	<p> Access hardware and protection classes secure areas based on layered security model</p>
<p>Digital Access Management Systems</p>	<p> Primo Intelligent digital access solution that seamlessly integrates devices into a unified, scalable system</p>	✓	✓	Smart cards and fobs, mobile keys, PIN, fingerprint, facial recognition	✓	✓	✓	<p>Locks, escutcheons, cylinders, padlocks and readers Powered by battery or wired Protection classes 1, 2, 3, 4</p>
	<p> Aperio The easy way to extend the reach of your access control system</p>	✓	✓	Smart cards and fobs, mobile keys, PIN	✓	✓	✓	<p>Locks, escutcheons, cylinders, padlocks and readers Powered by battery Protection classes 1, 2, 3, 4</p>
<p>Connectable access hardware to increase control and security</p>	<p> ABLOY CUMULUS Cloud platform with easy integration of digital access devices and mobile access</p>	✓	✓	Mobile app with mobile keys	✓	✓	✓	<p>Padlocks, key deposits, swing handles Powered by battery Protection classes 1, 2, 3, 4</p>
	<p> ABLOY CUMULUS Cloud platform with easy integration of digital access devices and mobile access</p>	✓	✓	Mobile app with mobile keys	✓	✓	✓	<p>Padlocks, key deposits, swing handles Powered by battery Protection classes 1, 2, 3, 4</p>

» continued on the next page »

An overview of Digital Access Solutions from ASSA ABLOY

Choose what works best for your environment to enhance protection from the perimeter to the core

Additional connectable access hardware to increase control and security



ABLOY Electric Locks

Combining mechanical strength with advanced control, these electric locks are ideal for critical infrastructure and commercial security.

Trusted worldwide, they integrate with access and alarm systems, drawing power only when needed for energy-efficient, certified protection.



effeff Electric Strikes

Designed for commercial and high-traffic environments, effeff electric strikes offer a reliable combination of mechanical reliability and digital intelligence.

Compact, durable, and digitally connected, they integrate with intercoms and access systems to upgrade mechanical locks without altering door design.



effeff electronic escape route technology

ePED® unite certified safety with smart, integrated control – offering flexible solutions for modern emergency exits.

Modern design, visual cues for intuitive use, and easy installation combine to upgrade escape route technology for 21st-century buildings. Built for critical situations, ePED ensures doors remain locked until authorized release, guiding users safely during emergencies.



Control iD and HID® Signo™ readers

With sleek aesthetics and flexible credential support – from biometrics to mobile and smart cards – these readers enable secure, seamless access control.

Both platforms integrate with cloud-based and local security systems, enabling centralized control and scalable deployment across diverse environments. The door controller or communication hub serves as the interface between the reader and the EAC system, enabling secure data exchange and real-time access decisions

Next steps: NIS2 compliance action checklist

Phase	Action item	Details / enhancements
Classification & Scope	Identify if your organization is an “essential” or “important” entity	Use NACE codes and size thresholds; include subsidiaries and cross-border operations
Governance & Responsibility	Appoint a responsible person or team for NIS2 compliance	Define roles for cyber security, physical security, and legal compliance
Risk Assessment	Conduct a comprehensive cyber-physical risk analysis	Include IT systems, physical access, supply chain, and third-party dependencies
Policy Framework	Develop or update security policies and procedures	Include incident response, business continuity, access control, and vulnerability management
Technical & Organizational Measures	Implement appropriate controls	Examples: MFA, encryption, network segmentation, secure software development, access control
Physical Security Measures	Enhance physical access control and infrastructure security Layer security based on the “onion shell principle”	Ensure physical security by controlling access to critical areas, monitoring activity, protecting infrastructure, and training staff to maintain operational continuity and prevent unauthorized access
Supply Chain Security	Assess and secure third-party relationships	Include contractual clauses, audits, and risk-based segmentation of suppliers
Incident Response & Reporting	Establish procedures for detecting and reporting incidents	Must report significant incidents to CSIRT within 24 hours; maintain logs and evidence
Business Continuity & Recovery	Implement backup and disaster recovery plans	Test regularly; ensure resilience against ransomware and physical sabotage
Staff Training & Awareness	Conduct regular cyber security and physical security training	Include phishing
Compliance Monitoring	Continuously monitor the state of compliance with NIS2 and remediate any instances of non-compliance	Regularly assessing and documenting cyber security and physical security measures, risks, and incident responses to ensure they meet NIS2 requirements and can withstand audits or inspections



Achieve NIS2 compliance with confidence. Our experts are here to help

We invite you to contact us so that we may provide a detailed explanation of how our digital access solutions can assist in achieving compliance with the NIS2 Directive. Our experts are available to guide you through the specific features and benefits that align with the directive's requirements and enhance your organization's cyber-physical security framework.

Regardless of whether your company is affected by the requirements of the NIS2 Directive or not, investing in a modern digital access solution helps enhance the protection of both proprietary and customer-specific information and assets.

Your questions matter – reach out



The ASSA ABLOY Group is the global leader in access solutions. Every day, we help billions of people experience a more open world.

ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions in homes, businesses and institutions. Our offering includes doors, door and window hardware, locks, access control and service.

ASSA ABLOY Opening Solutions EMEA
Digital and Access Solutions
Dukes Court
Duke Street
Woking
GU21 5BH
United Kingdom

assaabloy.com

[ASSA ABLOY country entity Company Name] is committed to complying with the EU NIS2 Directive. We have implemented strong cyber security measures to protect our systems and data. Our approach includes risk management, incident response, and access control. Our alignment with ISO/IEC 27001 and other relevant standards reinforces our commitment to resilience, trust, and regulatory compliance.