EVVA
access to security

Whitepaper

The first barrier
Access control for Critical infrastructure

The first barrier
Access control for Critical infrastructure

How modern access control contributes to NIS2 and CER compliance - and enhances sustainable physical security.

Access control as key component for NIS2 and CER compliance

The world and we have changed - especially in the last few years. Geopolitical changes such as wars, political instability, climatic changes and new technologies are shaping our everyday lives and require greater resilience of vital facilities, in particular an increasein physical protection.

With the European NIS2 Directive (2022/2555) and the supplementary CER Directive (2022/2557), the European Union is significantly increasing the safety requirements for operators of critical and important facilities. Both sets of rules aim to centrally strengthen resilienceto digital and physical threats - making access control the focus of modern security architectures. In this white paper, we want to focus on the topic of „Physical protection measures for critical facilities“.

Regulatory framework: NIS2 and CER

Explanation of term

NIS2 and CER are EU directives that require implementation into national law. An overview of the corresponding legal frameworks and designations across European markets is provided on page 15 of this white paper.

NIS2

Cybersecurity for critical and important sectors

- EU Directive (2022/2555)
- **Objective:** Increasing cyber security levels
- through EU-wide minimum standards. Commitment
- organisations to systematically improve their IT and cyber security and report incidents.
- **Applies to:**
  - „Main" facilities: This includes all:
  - Companies with high criticality whose failure would have a significant impact on society, economy or public security, including energy, transport, banking, healthcare, water, telecommunications/IT
  - „Important" sectors: This includes: other critical impacts such as Mail, Waste, Chemicals, Food, Manufacturing of goods (from 50 employees and 10 million EUR turnover)
- **Requirements** for companies that fall under NIS-2 include
  - Cyber security management (risk analysis security concepts, incident response, business continuity)
  - Reporting of Security Incidents
  - Management Responsibility
  - Strict Supervision and Sanctions

CER

Physical resilience of critical infrastructures

- EU Directive (2022/2557)
- **Objective:** Increased physical resilience
- against non-digital threats and
- Hazards (all hazardous approach)
- **Applies to:** Operators of critical infrastructure such as:
  - Energy
  - Traffic
  - Banks
  - Healthcare • Water
  - Telko/IT
  - Food
  - Chemicals
- **Requirements:**
  - Risk-based thinking
  - Emergency and Restart Plans
  - Safety Measures
  - Supply chain and dependency management
  - Serious incident reporting obligation
  - Ensuring the continuityof vital
  - Services

Short and to the point

In summary, this means that organisations affected by NIS2 and CER must, following a systematic threat and risk analysis and assessment, implement measures to ensure effective physical protection. These measures include, in particular, access control, monitoring, and procedures for incident detection. CER further specifies this: Critical plant operators must carry out risk analyses every four years, implement appropriate physical protective measures and effectively prevent unauthorised access.

Cybersecurity also needs physical protection

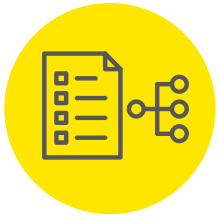
Relevant security features for use in the NIS2 and CER environment

Physical Access Security

- Strict access control to critical areas
- Tamper-proof access media
- State-of-the-art Technician

IT Security & Encryption

- Secure communicatoin using current cryptogrphic standards (TLS, AES, ECDSA)
- No insecure passwords



Logging & Audits

- Comprehensive documentation of all access events and system activities
- Tamper-proof audit logs with export functionality for audit and compliance documentation

Incident Response & Access Protection

- Rapid blocking of compromised access points
- Emergency plans for outages or attacks (offline operation of doors)

Business continuity & data backup

- Automated data backup concept
- Restart strategy after failure, redundancy

Vulnerability management & updates

- Continuous manufacturer monitoring of software Security Vulnerabilities (CVE)
- Timely, signed and verified updates

Data Privacy Policy & data security

- Privacy by Design and GDPR compliance
- Deletion functions for personal data
- Configurable logging
- Four-eyes principle for access to logs

EVVA products and their answers to regulatory requirements

Xesar

Access system for the highest security requirements

Physical & IT Security

- Role-based access rights per person/group
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), system-specific AES keys
- Encrypted Challenge Response communication (no plain text protocols)
- TLS ≥ 1.2 for system communication
- Internal AES256-bit encryption › Passwords hashed (Bcrypt)

Access & system logs

- Complete, tamper-proof event and System Logs
- Audit-proof exports
- Audit and incident evidence possible at any time Incident

Response & Resilience

- Real-time blocking (online), block lists for offline Parts Listing
- Warning mechanisms in the event of an unsafe blocking status
- Independent offline operation at IT or Network failure

Updates & vulnerability management

- Continuous CVE monitoring
- Cryptographically signed updates (RSA/SHA256,
- AES256CCM)
- Verified firmware and software updates

Business Continuity

- Encrypted backups
- Emergency recovery via system safety data sheet
- Multi-user and 24/7 server operation possible

Data Privacy Policy

- Privacy by Design
- No personal data in the app
- Automatic removal of personal identifiers configurable

AirKey

Mobile access solution with the highest standards

Physical & IT Security

- Smartphone & RFID-based access media (JCOP SmartMX3, EAL6+)
- ECDSA256 authentication + AESSessionKeys
- TLS-secured online administration

Access & system logs

- Audit-proof logging
- Audit-proof exports
- Automatic updating of blocklists & logs
- Flexible, data protection-compliant configuration

Incident Response & Resilience

- Real-time locking via the Internet
- Offline door function even in the event of server failure
- Warnings in the event of safety-critical conditions

Updates & Operation

- Central, signed update management
- ISO 27001 certified data centres in Austria
- Redundant EVVA servers, HSM secured keys

Data Privacy Policy

- GDPR-compliant deletion concepts
- Privacyby Design
- Four-eyes principle for viewing logs can be activated

STANDARDS & CERTIFICATION STATUS

Successfully
inspected (TÜV)
EN 18031-1

RED* REQUIREMENTS MET

*RED: Radio Equipment Directive

Practical example 1:

Hospital access control

NIS2/CER-relevant

Initial situation

A hospital is one of the „essential facilities“ according to NIS2 and is subject to strict IT and physical security requirements. Particularly sensitive areas such as server rooms, drug stores or intensive care units must be protected against unauthorised access.

Solution with Xesar

- Role-based access rights for various Employee groups (e.g. IT, maintenance, administration)
- Access media with individual, highly secure Technologies (MIFARE DESFire EV3)
- Complete logging of all access events, Audit-proof logs for audits
- Fast blocking of lost media via Real-time blocklists
- Offline operation of doors in the event of server failure (business Continuity)
- Regular, signed software updates and
- vulnerability management

Added value

The hospital implements risk-based measures, is able to provide a complete audit trail of incidents, and thereby enhances the physical resilience of the facility.

Practical example 2:

Production operation as supplier for critical infrastructure

Supply Chain/ CER-relevant

Initial situation

A medium-sized machine builder supplies energy suppliers and is therefore indirectly covered by the CER directive. The company must demonstrate that its access systems and IT infrastructure are resilient and secure.

Solution with AirKey

- Access rights are managed centrally, including for external service providers (e.g. maintenance personnel)
- Secure cloud-based application
- Access media (smartphones, RFID) with very high Encryption (ECDSA-256, AES-128)
- Logging of all access events, export for audits
- GDPR-compliant deletion functions and Privacy by Design
- Updates and vulnerability management centrally through EVVA

Added value

The company can demonstrate to its customers that it has implemented appropriate access-related measures to ensure security within the supply chain and is optimally prepared for audits and certifications.

Practical example 3:

Emergency management and resilience in a city administration

CER-relevant

Initial situation

A municipality operates critical infrastructure (e.g. water supply and sewage treatment plants) and must ensure that, in an emergency (e.g. cyber attack, power failure) access to critical areas is still possible.

Solution with Xesar

- Functional offline operation in the event of a power failure or cyberattack
- Fast blocking of compromised access media, warnings for open safety tasks
- Backup and restore functions for configuration data

Added value

The city administration remains able to act even in the event of a crisis - the residents and local businesses are not affected by outages and disruptions.

Practical example 4:

Data protection and logging in a research institute

NIS2/CER-relevant

Initial situation

A research institute processes sensitive personal data and must comply with the GDPR and NIS2 requirements.

Solution with Xesar

- Privacy by Design: No Recording of personal data in the backend
- Configurable logging, deletion functions for your personal details
- GDPR-compliant implementation

Added value

The Institute can provide evidence of data protection and transparency to supervisory authorities and partners at any time.

Security Check for Operators of Critical Infrastructure

1. Organisational Security Framework

- Do we have a binding security concept to provide physical security?
- Are roles, rights and Security, IT, Facility Responsibility Structures and CRITIS-relevant areas?
- Are security policies and processes reviewed and updated on a regular basis?
- Compliance with the prescribed reporting obligation secured in a process for security incidents?

2. Risk Analysis & Compliance

- Have we conducted a risk assessment in accordance with the Critical Infrastructure Protection Act (KRITIS Umbrella Act) / CER within the last four years?
- Have we identified all physical and digital vulnerabilities along the process chain?
- Are our access control solutions adequately aligned with NIS2 requirements, particularly regarding secure protocols and protection against tampering?
- Do we use only state-of-the-art systems and technologies (i.e., no unencrypted protocols such as Wiegand)?

3. Access Rights & Identities

- Are all access authorisations role-based and clearly assigned?
- Are access rights regelmäßig recertified or automatically withdrawn when no longer required what's happening?
- Do we have clear onboarding processes, Change of role and offboarding of employees and service providers?

4. Technical Security of Access Control

- Are all access readers, cards and identification media encrypted?
- Are all security-critical doors, server rooms and control stations with electronic access systems secured?
- Are security-relevant data (e.g. logs) made audit-proof saved and protected against manipulation

5. Monitoring, logging & transparency

- Are all access events and access attempts automatically logged?
- Are our access logs audit-proof, tamper-proof and stored for a sufficiently long period?
- Do we use monitoring tools that link physical and digital security events?

6. Protection of critical areas

- Are areas such as server rooms, control centres, energy/utility facilities or switch cabinets subject to special security measures?
- Are there multi-level access zones with increasing levels of security?
- Are sensitive rooms additionally secured by CCTV, door status monitoring or alarm systems?
- Do we have a plan for emergency access (e.g. in the event of a power cut or system failure)?

7. Suppliers & Service Providers

- Do external companies and service providers have only temporary and clearly defined access rights?
- Is access for temporary staff technically restricted and strictly monitored?
- Is the use of external access points regularly audited?

8. Emergency & Recovery Capability

- Is there an emergency and crisis management plan that covers physical security aspects?
- Have procedures been defined for:
  - Immediately blocking access for individual users or groups
  - Rapidly restoring the access infrastructure following an attack
  - Evacuation or incident response scenarios
- Are these plans practised regularly?

9. Training & Awareness

- Are all staff trained in the use of access cards?
- Is there an ongoing awareness programme covering security policies and appropriate behaviour?
- Do staff know how to report suspicious activity?

10. Sustainability & Further Development

- Is our access control solution scalable to accommodate new sites or additional requirements?
- Can we integrate new security standards (NIS2 updates, BSI guidelines, amendments to the KRITIS framework legislation) without any issues?
- Do we have a clear modernisation plan in place in case technologies become obsolete or security vulnerabilities come to light?

NIS2 and CER are implemented in the individual EU Member States under the following national legislative titles

	NIS2	CER
Austria	NISG2026 (Netz- und Informationssicherheitsgesetz 2026)	RKEG (Resilienz kritischer Einrichtungs-Gesetz)
Germany	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Gesetz zur Stärkung der physischen Resilienz kritischer Anlagen)
Belgium	Loi NIS2 (Gesetz vom 26. April 2024 zur Cybersicherheit von Netz- und Informationssystemen)	Loi relative à la résilience des entités critiques (nationales CER-Umsetzungsgesetz, 2025/26
Neterlands	Cyberbeveiligingswet (in parlamentarischer Umsetzung, Stand April 2026)	Wet weerbaarheid kritieke entiteiten (geplantes CER-Gesetz, Stand April 2026)
Sweden	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (CER-Umsetzung in Vorbereitung, Stand April 2026)
Italy	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Czech Republic	Zákon o kybernetické bezpečnosti (Novelle/ Neufassung zur NIS2-Umsetzung)	Zákon o odolnosti kritických subjektů (CER-Umsetzungsgesetz)
Poland	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) – Novelle zur NIS2	Ustawa o odporności podmiotów krytycznych (in Umsetzung)
Slovakia	Zákon o kybernetickej bezpečnosti (NIS2-Novelle)	Zákon o odolnosti kritických subjektov

www.evva.com