KEYFACTOR

EBOOK

Key Requirements Under the NIS2 Directive

Strengthening Cybersecurity Through Robust Certificate Management and PKI Security

Table of contents

Introduction

In today's digital age, cybersecurity has become a top priority for individuals and organizations alike. The increasing reliance on technology and the surge in cyber-attacks have highlighted the need for a comprehensive and robust cybersecurity framework. In 2016, the European Commission proposed the EU Network and Information Security (NIS) directive, the first piece of EU-wide cybersecurity legislation, with the goal of enhancing cybersecurity across the European Union.

However, the 2016 NIS directive lacked accountability and relied heavily on individual member states' discretion. As a response to the growing threats posed by increasing digitalization and cyber-attacks, the European Commission announced plans to replace the NIS directive with a stronger set of security requirements, including harmonized sanctions across the European Union.

On January 16, 2023, the Directive (EU) 2022/2555, known as NIS2, replaced the Directive (EU) 2016/1148.

Under the NIS2 directive, companies must implement a list of key elements as part of their cybersecurity risk management measures, including supply chain security and the use of cryptography and encryption, as outlined in Article 18. Additionally, Article 89 of the directive states that essential and important entities should adopt basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, and identity and access management.

This eBook provides an overview of the NIS2 requirements, how they relate to certificate management and PKI security, and discusses best practices for implementation.

New industries considered critical infrastructure

The definition of critical infrastructure has expanded under the NIS2 Directive, reflecting the increasing interconnectedness of our digital and physical worlds. With the rise of the Internet of Things (IoT) and the integration of digital technologies into all aspects of society, it is more important than ever to ensure the security and resilience of essential services.

The inclusion of industries, such as water supply and waste management, recognizes the critical role these services play in maintaining public health and safety. By requiring these industries to implement cybersecurity measures, the NIS2 Directive aims to mitigate the risk of cyber-attacks that could disrupt essential services and have severe consequences for society.

Furthermore, the inclusion of manufacturing highlights the importance of protecting industrial control systems (ICS) and critical manufacturing processes from cyber threats that could result in production disruptions or even physical damage. Overall, the NIS2 Directive's expanded definition of critical infrastructure reflects the evolving nature of cybersecurity threats and the need for a comprehensive and coordinated approach to cybersecurity across all industries.

The NIS2 Directive recognizes that some sectors may already have their own cybersecurity legal acts in place. In cases where these sector-specific acts provide equivalent or greater cybersecurity measures than those outlined in the NIS2 Directive, the relevant provisions of the directive will not apply to those entities. However, for entities not covered by these sector-specific acts, the provisions of the NIS2 Directive will continue to apply.

Evolution of NIS Industries: From NIS to NIS2

NIS

- Healthcare
- Transport
- Water Supply
- Energy
- Digital Infrastructure
- Digital Service Providers
- Banking and Financial Market Infrastructure

NIS2

- Space
- Food
- Public Administration
- Postal and Courier Services
- Waste water and waste management
- Providers of public electronic communications networks or services
- Digital services such as social networking services platforms and data centre services
- Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals)

Expanded scope to include more sectors and services as either essential or important entities.

Increased cybersecurity requirements for critical infrastructure operators

The NIS2 Directive increases cybersecurity requirements for critical infrastructure operators. Operators are now required to implement advanced security measures, such as intrusion detection systems, security information and event management (SIEM) systems, and vulnerability assessments.

Additionally, critical infrastructure operators are required to report cybersecurity incidents to the competent authority within 24 hours of becoming aware of the incident. Failure to comply with the NIS2 requirements can result in significant financial penalties and damage to the reputation of the organization.

Overall, the NIS2 Directive aims to strengthen cybersecurity and resilience for critical infrastructure and digital service providers in the European Union. Whilst the specific technical requirements will be disclosed over the following months, under NIS2, organizations are held directly responsible and must apply additional “technical and organizational measures” when outsourcing their ICT activities, such as storing and processing data in the cloud.

Cryptography and encryption are essential to enforce these measures, as they require a secret, such as a cryptographic key or digital certificate, to access encrypted data, giving organizations control over their cloud-based assets.

As a result, critical infrastructure operators and digital service providers should take proactive steps to implement these measures to ensure the security and availability of their systems and services.

Use of PKI and certificates under NIS2

Public key infrastructure (PKI) and digital certificates are foundational to establishing trust and secure communications across organizations. Certificates issued from a trusted PKI provide a secure means of verifying the identity of users, devices, and connected "things," and encrypting sensitive data transmitted between them. Everything from websites and applications to Wi-Fi networks and critical infrastructure relies on certificates to run securely.

Under NIS2, critical infrastructure operators are required to implement several security measures, including:

- ✓ Using cryptography and encryption services, such as PKI certificates to secure their networks and systems
- ✓ Implementing multi-factor authentication for all users with access to critical systems
- ✓ Conducting regular risk assessments and security audits
- ✓ Reporting security incidents to the relevant authorities within 24 hours
- ✓ Developing incident response plans and conducting regular drills to test them

The use of PKI and certificates is essential for ensuring the security and resilience of critical infrastructure, as it provides a secure way to verify the identity of users and devices on a network and encrypt and protect sensitive data in transit. By implementing these measures, critical infrastructure operators can better protect their networks and systems from cyber-attacks and other security threats.

Certificate management under the NIS2 directive

Digital certificates are critical components in the secure operation of networks and systems. However, it is not enough to simply issue certificates — every certificate must be managed throughout its lifecycle to ensure it remains trusted, valid, and compliant with policy. As the NIS2 Directive comes into effect and in conjunction with related EU regulations and directives, critical organizations will be required to implement a comprehensive certificate management system (CMS) to manage the lifecycle of digital certificates. This includes tasks such as issuance, revocation, and renewal. To cover these requirements, a CMS must include the following components:

Certificate Policy and Practice Statements:

These are documents that describe the policies and practices for certificate issuance, renewal, and revocation. The policies and practices should align with industry standards and best practices.

Certificate Authority:

A certificate authority (CA) is responsible for issuing digital certificates. The NIS2 Directive requires the implementation of a secure CA, which must be audited and certified by a third-party auditor.

Certificate Repository:

The CMS must provide a secure repository for storing digital certificates. The repository should include access controls and encryption mechanisms to ensure the confidentiality and integrity of stored certificates.

Certificate Revocation List (CRL):

The CMS must include a CRL that lists all revoked certificates. The CRL should be updated regularly and made available to users.

The NIS2 Directive also mandates the use of secure certificate storage and requires that only authorized personnel can issue and manage certificates. To ensure the security and integrity of digital certificates, the NIS2 Directive requires the use of secure hardware for key storage.

PKI security requirements under the NIS2 directive

Provision 98 of the NIS2 Directive states that “In order to safeguard the security of public electronic communications networks and publicly available electronic communications services, the use of encryption technologies, in particular end-to-end encryption as well as data centric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions, should be promoted.”

PKI security controls are critical to protect against cyber threats. These controls are aimed at ensuring the confidentiality, integrity, and availability of digital certificates and keys used in secure communication over networks. These controls include:

Secure key storage:

Private keys used in PKI must be stored in secure hardware devices, such as hardware security modules (HSMs), to prevent unauthorized access. HSMs are specialized devices designed to securely store and manage cryptographic keys, providing a high level of protection against key theft or misuse. Implementing secure key storage measures helps to ensure the integrity of the keys used in PKI.

Backup and recovery:

The NIS2 Directive requires the implementation of secure backup and recovery procedures to ensure the availability of digital certificates and keys in the event of a system failure or disaster. Backup and recovery measures include regular backups of digital certificates and keys, testing backup procedures, and ensuring the availability of backup copies of the keys. Implementing backup and recovery measures helps to ensure the availability of digital certificates and keys, ensuring that secure communication can continue even in the event of a system failure or disaster.

Encryption:

Digital certificates and keys must be encrypted during transmission and storage to ensure confidentiality. Encryption is the process of converting plaintext into ciphertext using an algorithm and a secret key. The ciphertext can only be decrypted using the same key and algorithm, ensuring that only authorized parties can access the data. Implementing encryption measures helps to prevent unauthorized access to digital certificates and keys.

Digital signatures:

Digital signatures must be used to authenticate digital certificates and messages. Digital signatures are mathematical algorithms used to verify the authenticity and integrity of digital documents. They are generated using a private key and verified using a corresponding public key. Implementing digital signature controls helps to prevent tampering with digital certificates and messages, ensuring their authenticity.

Secure communication protocols:

Secure communication protocols, such as Transport Layer Security (TLS), must be used to transmit certificates and keys. TLS is a protocol used to establish secure communication channels over the internet. It uses encryption and authentication mechanisms to ensure the confidentiality and integrity of data transmitted between two endpoints. Implementing secure communication protocols helps to prevent eavesdropping and data tampering during transmission.

In summary, the NIS2 Directive requires critical infrastructure operators and digital service providers to implement robust PKI security controls to protect against cyber threats. By implementing these controls, organizations can ensure the confidentiality, integrity, and availability of digital certificates and keys used in secure communication over networks.

Compliance and auditing requirements

Compliance and auditing requirements are essential components of the NIS2 Directive. In addition to mandating that critical infrastructure operators and digital service providers comply with its requirements related to certificate management and PKI security, the Directive requires regular auditing and risk assessments of these practices to ensure compliance. Failure to comply with these requirements can lead to severe financial and reputational consequences for organizations.

To ensure compliance with the NIS2 Directive, organizations must establish clear policies and procedures for certificate management and PKI security. These policies and procedures should include the identification of risks related to certificate management and PKI security, as well as controls to mitigate these risks. Organizations should also establish roles and responsibilities related to certificate management and PKI security, including the appointment of individuals responsible for overseeing these functions.

The NIS2 Directive requires regular auditing of certificate management practices to ensure compliance. These audits should be conducted by independent third-party auditors who have the necessary expertise to assess certificate management and PKI security controls effectively. The auditors should assess the effectiveness of controls related to certificate management, such as issuance, revocation, and renewal of certificates. They should also evaluate the effectiveness of controls related to PKI security, such as key management, encryption, and digital signature verification.

In addition to regular auditing, organizations must conduct risk assessments of their certificate management and PKI security practices. These risk assessments should identify potential threats and vulnerabilities to certificate management and PKI security and evaluate the likelihood and impact of these risks. Based on the results of the risk assessment, organizations should implement controls to mitigate identified risks.

Penalties for non-compliance

Failure to comply with the Directive's requirements related to certificate management and PKI security can result in significant financial penalties, loss of reputation, and legal liability for organizations.

Provision 23 of the Network and Information Systems Directive (NIS2), which outlines the requirements for Member States to establish penalties and sanctions for non-compliance with the Directive's provisions. The NIS2 Directive requires Member States to establish penalties and sanctions for non-compliance with the Directive's provisions. These penalties and sanctions must be effective, proportionate, and dissuasive. Member States have the flexibility to determine the specific penalties and sanctions for non-compliance with the NIS2 Directive, but these penalties must be in line with the Directive's overall objective of improving cybersecurity and resilience.

The penalties for non-compliance with the NIS2 Directive can vary depending on the severity and impact of the violation. For minor violations, penalties may include warnings or fines. For more serious violations, penalties may include suspension or revocation of licenses, temporary or permanent closure of the business, or criminal sanctions.

One of the most significant penalties for non-compliance is the capacity for "the competent authorities should be empowered to suspend temporarily or to request the temporary suspension of a certification or authorisation concerning part or all of the relevant services provided or activities carried out by an essential entity."

Conclusion

The NIS2 Directive is a significant piece of EU-wide cybersecurity legislation that sets out stringent requirements for organizations operating in critical sectors. The directive emphasizes the importance of supply chain security and introduces mandatory requirements for encryption and key management systems. Specifically, Article 18 of the directive calls for appropriate and proportionate technical and organizational measures, including supply chain security and the use of cryptography and encryption. Additionally, Article 89 emphasizes the adoption of basic cyber hygiene practices.

With the implementation of the NIS2 Directive, organizations must be prepared to manage the lifecycle of digital certificates and take on greater responsibility for their ICT activities, including those outsourced to third-party providers. These measures are necessary to enhance cybersecurity across the European Union and protect against the growing threats posed by increasing digitalization and cyber-attacks.

PKI and certificate automation powered by Keyfactor

Keyfactor Command and Keyfactor EJBCA can help organizations comply with the NIS2 Directive's requirements. By providing centralized issuance, visibility, and control over digital certificates and keys, Command and EJBCA enable organizations to enforce strong security practices, maintain compliance with regulations, and mitigate cyber risks. Both solutions support auditing and reporting, making it easy for organizations to demonstrate compliance with the NIS2 Directive's requirements.

Overall, implementing a robust certificate management solution like Keyfactor Command or a PKI like EJBCA can help organizations effectively manage their digital certificates and keys, ensuring compliance with the NIS2 Directive and protecting against cyber threats.

Keyfactor
Command

Learn more ↗

Keyfactor
EJBCA

Learn more ↗

Deploy your PKI, your way

MANAGED

PKI as a Service

Available as a service

24/7 managed zero-touch PKI with an offline, air-gapped root.

SAAS

EJBCA SaaS

Available in AWS

Turnkey SaaS PKI deployed and managed by Keyfactor.

CLOUD

EJBCA Cloud

Available in AWS & Azure

Self-managed PKI deployed in your cloud environment.

SOFTWARE

EJBCA Software

Available as a virtual appliance

Deploy within your own datacenter and integrate with your HSM provider.

HARDWARE

EJBCA Hardware

Available in turnkey hardware

Deploy turnkey PKI with a full hardware and software stack and HSM.

Manage every machine identity

ENTERPRISE SECURITY

Keyfactor Command

Available on-prem, hybrid or SaaS

Prevent outages and enable crypto-agility with complete visibility, control and automation for keys and certificates.

PRODUCT SECURITY

Keyfactor Command for IoT

Available on-prem, hybrid or SaaS

Secure IoT products by design with end-to-end identity management for devices and manufacturing supply chains.

Prepare your organization for the NIS2 Directive

Whether your organization is prepared today or just beginning to plan, NIS2 Directive requirements are on the horizon. When it comes to PKI and certificate management, the message is clear — every business must modernize their strategy, tools, and processes to protect critical infrastructure and maintain trust across their IT and IoT environment.

GET IN TOUCH

Get started on your journey to modernize PKI and certificate management. Request a demo from a Keyfactor expert.

Request a demo ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +46 873 561 00