# AN14671

## Ease CRA compliance with EdgeLock Discrete Portfolio

Rev. 1.0 — 13 October 2025 Application note

**Document information**

| Information | Content |
|---|---|
| Keywords | CRA, EdgeLock, SE05x, A30, EdgeLock Discrete, Cybersecurity, Industrial IoT |
| Abstract | This document elaborates on the use of EdgeLock Discrete portfolio features to reduce implementation complexity and to ease the compliance to the requirements mandated by the CRA. |

# 1 Introduction

The potential risk from cyberattacks increases as the number of connected devices, machines, devices, and sensors keeps growing. It is predicted that in 2025, there will be 75 billion connected devices worldwide. With the increasing number of devices, as does the size of the attack surface, in 2025, there will be an estimated 10.5 trillion dollars in damages from cybercrime (ref.[1]).

As such, (cyber)security proves itself as a critical element in the development of products against intentional or unintentional threats. These threats may include unauthorized access, installation of malware, ransomware, spyware, or loss of data with the corresponding privacy breach. They can also have impacts of a secondary nature, such as personal injury, equipment damage, supply chain downtime, environmental impact, loss of production, or violation of regulatory requirements.

To improve cyber resilience in the European Union, in 2024, the European Parliament adopted the Cybersecurity Resilience Act (CRA) (ref.[2]) to ensure the cybersecurity of products and software with digital elements. In essence, it covers anything from hard disks and chips to software and robots. The CRA describes the requirements (technical and process) and obligations of manufacturers, importers, distributors, and third parties that supply their products to the European market.

The CRA was published in the European Official Journal as Regulation (EU) 2024/2847. It will be fully enforced from December 11th, 2027. From that date, all products with digital elements introduced in the European market must comply with the regulation. Products operating on markets and applications with similar security requirements are not required to comply with the CRA. For example certain vehicle types, medical, aeronautic equipment and planes, as well maritime equipment are segments with already existing regulations.

Manufacturers of products with digital elements, must comply with the essential requirements of the CRA. This requires for manufacturers to “own” the product’s cybersecurity risk, the obligation to mitigate such risk and communicate it to the users. Only when compliant, a manufacturer is allowed to affix the CE mark to its products. This mark is mandatory for access to the EU market.

Penalties for non-compliance with the essential requirements of the CRA can amount to up to 15 million euros, or 2.5% of the annual turnover, whichever is higher. Additionally, surveillance authorized have been empowered to issue product recalls or in extreme circumstances, withdrawal from the European market in cases of non-conformance. Therefore, the consequences of the CRA are of particularly large impact.

## 2 How to use this document

This document is addressed to OEMs and manufacturers (hereafter referred to a OEMs) interested in understanding how the products of the NXP EdgeLock Discrete portfolio can be used to facilitate the CRA compliance for their device implementation. While the products provide core security capabilities that can be mapped to the cybersecurity requirements of the CRA, the OEM will need to fill the remaining compliance gap by performing additional actions. This document is developed in that spirit, looking to provide guidance and supporting evidence from the EdgeLock Discrete Portfolio security capabilities towards the developer's CRA conformance claims.

Note that throughout this document the requirements and text of the CRA is condensed or simplified to summarize for ease of reading or highlight the applicability to the embedded context. For compliance, the full text of the CRA should always be consulted. The applicability of this Application Note cannot guarantee the legal certainty required by the CRA conformance and it should be used only as a guidance for manufacturers addressing conformance requirements rather than attestation of conformance to the CRA.

Therefore, all information provided hereunder is provided "AS IS" and NXP makes no representation or warranty, express or implied, of accuracy, completeness, that products will be suitable for any specified use, or that the information, test results, analysis or assessments are reliable without further testing or modification by the customer.  NXP will not be liable for any damage or loss arising from, in connection with or incident to any information or assistance provided by NXP. Customers are responsible for the design and operation of their applications and products and are responsible to provide appropriate design and operating safeguards to minimize risks associated with their applications and products.

# 3 Cyber Resilience Act overview

The Cyber Resilience Act (CRA) sets common security requirements for products with digital elements sold in the EU. This addresses the issue that many products on the market are currently not secure and that it is difficult to ascertain which of the products are, in fact, secure or how to utilize them securely. The main CRA document consists of 8 chapters and another 8 annexes to provide additional details. The CRA's goal is to guarantee[1]:

- harmonized rules when bringing to market products or software with digital components;
- a framework of cybersecurity requirements governing the planning, design, development, and maintenance of such products, with obligations to be met at every stage of the value chain;
- the obligation to provide a duty of care for the entire lifecycle of such products.

The requirements listed throughout the act can be grouped as follows:

- **Cybersecurity by design and by default:** cybersecurity should be considered during product design from the start. The CRA defines what kind of information and documentation should be created and gathered as well as, depending on the product's security category, what kind of conformity assessments it is required to go through.
- **Essential cybersecurity and vulnerability handling requirements, including reporting obligations:** the CRA sets both technical cybersecurity requirements on manufactured products to reduce the attack surface as much as possible and vulnerability handling requirements for vulnerabilities found after production and introduction to the market.
- **Conformity assessment and compliance:** digital products have to be subjected to a specified conformance assessment, depending on their security category.
- **Fines:** the CRA enforces compliance with the penalty of fines for non-compliant manufacturers, importers, or distributors.
- **The interplay between the conformity assessment procedure and existing or upcoming cybersecurity legislation:** the CRA aims to complement and harmonize with existing and upcoming legislation, such as the EU Cybersecurity Act.

OEMs may find the EdgeLock Discrete portfolio can be of added value in meeting the requirements listed above. Its security features can be leveraged by the OEM to implement security countermeasures in an efficient and reliable manner.

Products with digital elements (PDEs, also referred to as plain products in the remainder of this document) are classified into four categories in the Cyber Resilience Act.

- **Default PDEs.**
- **Important PDEs: class I.**
- **Important PDEs: class II.**
- **Critical PDEs.**

Approximately 10% of all PDE are classified as security-important and further subcategorized based on their functionality, intended use, and optional further criteria. The remaining products are classified as the default category. A different standard of assessment/certification applies depending on which category each product is listed in the CRA Annex III and IV: in the default category, a security self-assessment suffices, whereas, for critical products, a mandatory EU certification is required. The intention is that approximately 90% of digital products will fall into the default category.

1 From: EU Cyber Resilience Act | Shaping Europe's digital future

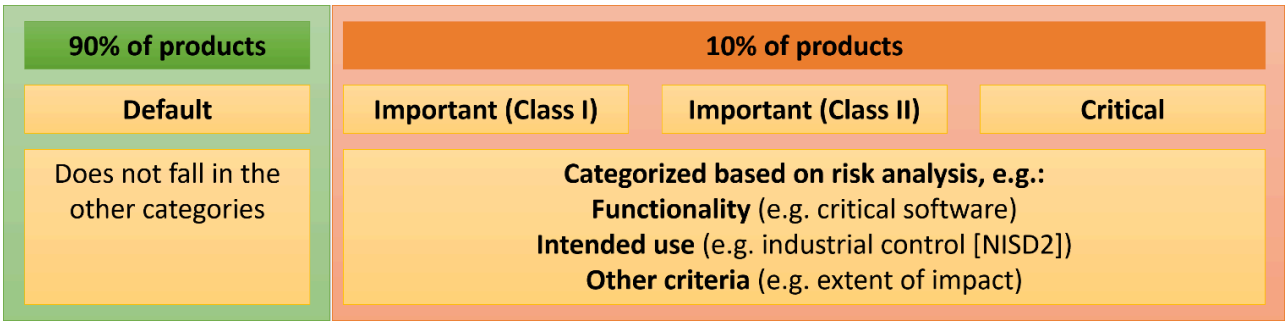


**Figure 1. Products with digital elements**

Examples of each class are listed below. A more extensive list can be found in the CRA regulation (ref.[2]). **Note that future EU Delegated and Implementing Acts can add additional clarity to these product types.** Conformance assessment criteria can be found in Article 32 of the regulation.

***Note:*** *The information provided in the table reflects the current understanding of the CRA at the time of writing this document. However, CRA regulation may be subject to updates or interpretation changes. Readers are encouraged to verify the original source documents or consult authoritative references to ensure accurate and up-to-date guidance.*

**Table 1. Examples of products with digital elements**

| Category | Examples[1] |
|---|---|
| Default | Hard drives<br>Smart speakers<br>Robot vacuum<br>Games and toys |
| Important (Class I) | Identity/network management systems<br>Microprocessors/controllers with security-related functionalities<br>Smart home products with security functionalities<br>Personal wearables for health monitoring |
| Important (Class II) | Hypervisors and container runtime systems<br>Firewalls, intrusion detection and prevention systems<br>Tamper-resistant microprocessors<br>Tamper-resistant microcontrollers |
| Critical | Hardware devices with security boxes<br>Smart meter gateways within smart metering systems<br>Devices for advanced security purposes, including for secure crypto processing<br>Smartcards or similar devices, including secure elements[2] |

[1] List is not exhaustive.
[2] Including secure authenticators such as the EdgeLock A30 and A5000 Secure Authenticators

# 4 Leveraging the EdgeLock® Discrete portfolio to meet Cyber Resilience Act requirements

As mentioned in the introduction, the clearest contribution of NXP products to the CRA compliance of an end-product it's integrated into, lies in their security features that can be leveraged by the end-product. Additional contributions are discussed in the next section of this document.

In Annex I of the CRA, the Essential Cybersecurity Requirements (ECRs) are listed for products with digital elements (PDEs). In this chapter, we will first expand on how the EdgeLock A30, A5000, and SE05x products of the EdgeLock Discrete portfolio can be leveraged to ease compliance with the requirements of Annex I (Part 1 and 2). In the last section of this chapter, we expand on additional support for the remaining requirements of the regulation.

Where possible, we use security terminology as outlined in the White-Paper Security Primitives: Common Nomenclature to Describe Security Requirements in (I)IoT Systems (ref.[3]).

Note that adding components from the critical category, like a secure element within a product with digital elements, does not make the final product part of the critical category. For example, a wearable device integrating a secure element will be in Class I, as per the CRA, even if the integrated secure element is in the Critical Category. The secure element will have to demonstrate conformance using the mechanism from the Critical Category, like a certification scheme from the Cyber Security Act. The wearable in a Class I product can demonstrate conformance by a self-assessment following the adequate harmonized standard. However, for the purpose of the risk assessment, the Class I product manufacturer can leverage the integrated critical secure element. The mapping will be detailed out in the following sections.

## 4.1 Cyber Resilience Act

### 4.1.1 Annex I, Part 1. Security requirements

This part of the document covers security requirements relating to the properties of PDEs.

#### 4.1.1.1 Requirement (1): Secure manufacturing

The first requirement in Annex I, Part 1, concerns the development process of the product: "Products with digital elements shall be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks." Starting from the design of a product to its production, at each level, a risk-based analysis should be made to apply the right level of cyber security.

At NXP, security is integral to the entire product lifecycle. Product development is supported by a dedicated team of security experts to reduce the risk of critical vulnerabilities. The NXP Secure Manufacturing Process is supported by the in-house EdgeLock Secure Assurance program, as well as certifications like ISO/SAE 21434 and IEC 62443-4-1.

Additionally, the products in the EdgeLock Discrete portfolio support the OEM with security features that can be leveraged by the end-product to get the desired security capability. Those functionalities have been evaluated and certified by independent third parties against CC (Common Criteria) EAL 6+ with AVA_VAN.5 level of assurance under ISO 15408. Additionally the portfolio offering includes an SE050 variant available which is FIPS 140-2 certified, and an SE052F variant as first FIPS 140-3 Level 3 certified secure element. The applet-updatable SE051 gains additional assurance in its security capabilities since it has achieved the IEC 62443 4-2 certification.

#### 4.1.1.2 Requirement (2): Cybersecurity requirements

In requirement (2) of Annex I Part 1, 13 cybersecurity measures are listed that a product should comply with. In this section, we will go through them one by one. Based on the risk assessment referred to in Article 13(3) of the CRA, it states that products with digital elements shall:

#### 4.1.1.3 a) be made available on the market without known exploitable vulnerabilities;

Security is at the core of the development cycle of the EdgeLock Discrete portfolio. Security-by-design is an integral part of the NXP (certified) cybersecurity engineering processes. The process increases the security maturity level of the device by having security experts perform reviews and assessments of the device's security concept, architecture, design, and implementation.

Additionally, as part of the certification process under the Common Criteria scheme, the security evaluation and certification third parties perform a verification against known exploitable vulnerabilities in EdgeLock Discrete products.

#### 4.1.1.4 b) be in a secure by default configuration and can reset the product to its original state;

To reset to the original state of the device, NXP recommends that OEMs implement a secure backup and recovery mechanism. An over-the-air (OTA) update mechanism combined with the cryptography capabilities of the EdgeLock Discrete products can verify independent validity and/or conformity checks for any newly downloaded images. Such checks should already be part of the OEM OTA implementation to ensure that the update was from a trusted source and not altered or corrupted during transmission.

The products can also support the security of the MCU/MPU boot sequence. The EdgeLock A30, A5000 and SE05x supports the storage of public keys (RSA, ECC) that can be used to verify a signed digest of a software component before it is loaded and executed. In this way only applications that have been signed by the OEM with the corresponding private key will be accepted as valid by the system. This feature can be used to check the authenticity and integrity of boot loaders, firmware and OS applications before they are executed. For more information on how EdgeLock SE05x can be leveraged to support a secure boot, you can refer to ref.[4] and ref.[5].

The A30, A5000 and SE05x products have been assessed during the CC evaluation to have reached a determined level of cybersecurity in a defined context of risks (AVA_VAN5). This includes the verification of a secure default configuration, unambiguous identification by the integrator, that the certified version is secured and all guidance to ensure a secure integration are also evaluated and verified.

#### 4.1.1.5 (c) ensure that vulnerabilities can be addressed through security updates;

Even when carefully designed, unknown exploits can appear after a product enters the market. A secure update mechanism ensures that a product can be patched if it is within the physical capabilities of the device.

The EdgeLock Discrete portfolio provides support for cryptographic signature algorithms that can be used to sign and then verify the digest of an update or patch in order to ensure the integrity and authenticity of the firmware before installation. All products support the NIST Brainpool and Koblitz ECC (ECDSA signature algorithms for this purpose. Additional curves and RSA-based authentication can be found on the SE05x. The backup digests can be generated by EdgeLock Discrete supported hash functions (SHA-224 to SHA-512). The EdgeLock Discrete tamper-resistant hardware ensures that signing keys and encryption keys are protected.

On the EdgeLock SE051 series, the NXP IoT applet can be updated through an integrated update mechanism (SEMSLite). NXP recommends that OEM OTA mechanisms implement independent validity and/or conformity checks for any newly downloaded images. Such checks should already be part of the OEM OTA implementation to ensure that the update was from a trusted source, not altered or corrupted during transmission.

When customers embed NXP products into their solutions, they benefit from the support of the NXP PSIRT. This dedicated team is committed to:

- rapidly addressing security vulnerabilities in NXP products;
- providing clear guidance to customers regarding the impact and severity of identified vulnerabilities to NXP products, and recommending mitigation strategies.

NXP PSIRT ensures that customers can confidently deploy NXP products with the assurance of a proactive and transparent security response process.

#### 4.1.1.6 (d) protects against unauthorized access by using mechanisms such as authentication, identity, or access management systems and reports possible unauthorized access;

Authentication and access control mechanisms relate to many cryptography and security functionalities. The software on the device should be from an authenticated source, access to data and functionality on the device should be access controlled, and cryptographic protocols should be available for the OEM to implement their own (PKI-based) access management systems. We focus on the most important features of the EdgeLock Discrete portfolio that supports the OEM in their compliance with Requirement (2)(d).

EdgeLock Discrete portfolio is pre-provisioned for ease of use in NXP's secure facilities with a set of device-unique key-pairs, certificates and identifiers that can be used to establish the initial Root of Trust (RoT) of the IoT device. Customers are therefore not required to inject additional credentials. Pre-provisioned credentials can be used to support the main use cases, including device-to-device authentication. The EdgeLock Discrete products are further supported by NXP's EdgeLock 2GO service. This can provision device-unique credentials such as identity keypairs and certificates securely into the secure storage of the device after deployment of the device. Such credentials are then used to verify the identity of the device when the device connects to cloud or other systems.

The EdgeLock secure authenticators and secure elements offer secure memory that can only be written by authorized processes through the secure Host-SE channel. The memory can securely store passwords and private keys and helps secure the most sensitive cryptographic data from unauthorized access.

For authentication mechanisms on the MCU/MPU, EdgeLock Discrete products support symmetric encryption algorithms (AES), public-key encryption algorithms using ECC with support for Brainpool curves, public-key signing algorithms (ECDSA), key agreement algorithms (ECDH, ECDHE) and hashing and MAC algorithms (SHA, HMAC, CMAC). Additional curves and algorithms, e.g. NIST curves, DES, RSA signing, EdDSA, may be supported by specific products of the portfolio.

Further logging and data protection should be implemented by the OEM. The Edgelock Discrete portfolio can support OEM protection with its cryptographic acceleration options listed above.

#### 4.1.1.7 (e) protect the confidentiality of stored, transmitted, or otherwise processed data by, e.g., applying encryption to data at rest or in transit;

As with Requirement (2)(d), the protection of confidentiality also relates to many security paradigms. We focus on the most important EdgeLock Discrete features that can support the OEM in their compliance to (2)(e).

The EdgeLock Discrete products have various security features to support confidential (secure, encrypted) data storage. For one, they provide a secure, tamper-resistant hardware secure memory for the secure storage of device credentials such as keys, identifiers and certificates. To support the OEM in securely storing at rest data in less secure memory, the supports both asymmetric (ECC, optionally RSA) and symmetric (AES) cryptographic algorithms that can be used to encrypt data at rest in the IoT device.

For other applications that require encryption, like data in transit, the EdgeLock Discrete products support the acceleration of cryptographic operations. Both symmetric and asymmetric crypto accelerators are included to securely process keys and data for encrypted transmission (e.g., by TLS). This includes:

- Symmetric cryptography: AES 128/256 in supported modes incl. ECB/CBC/CTR/CCM/GCM
- Asymmetric cryptography: ECC P-256 curve (more curves, e.g. NIST, Brainpool, BN, available on SE05x devices)
- Hash functionality: SHA 224/256/384/512

#### 4.1.1.8 (f) protect the integrity of stored, transmitted, or otherwise processed data, commands, programs, and configuration against un-authorized modification, and report on corruptions;

After authenticity in Requirement (2)(d) and confidentiality in (2)(e), Requirement (2)(f) focuses on the integrity of data on the product. Again, we focus on the most important aspects of the EdgeLock Discrete portfolio that support their compliance with this requirement.

As mentioned before, the EdgeLock Discrete products support the encryption of information for secure storage in less secure memory. They also support symmetric crypto accelerators that can be used to implement further integrity checks. This includes:

- Symmetric cryptography: AES 128/256 in supported modes incl. ECB/CBC/CTR/CCM/GCM
- Hash functionality: SHA 224/256/384/512
- Authentication modes HMAC, CMAC

In case of a failure of any of the integrity check mechanisms described above, a verify result (ok/failed) is sent by the secure element or authenticator to the host, which can then take action, e.g., automatically notify or record in an audit log.

#### 4.1.1.9 (g) process only data that are adequate, relevant, and limited to what is necessary in relation to the intended use of the product ('minimization of data');

Minimization of data ensures that a potential attacker has the least attack surface possible. This requirement needs to be realized by the OEM for its application data.

When utilizing the EdgeLock Discrete products with EdgeLock2GO, NXP supports the OEM by minimizing the user data that is processed in the cloud. E.g., EdgeLock2GO does not profile on user data like IP addresses and does not store this type of data for later use.

#### 4.1.1.10 (h) protect the availability of essential and basic functions, and be resilient against and able to mitigate denial-of-service attacks

Requirement (2)(h) aims to mitigate attacks that attempt to make the product unavailable. This can be done by applying software isolation techniques to protect essential processes from external non-essential applications.

Application-level network segmentation must be implemented on the main processor. EdgeLock Discrete products can be leveraged to offload communication protocols cryptographic operations while keeping the cryptographic keys secure inside the SE/SA. They have built-in support for the widely used TLS protocol to secure and isolate upper layer communication protocols such as OPC-UA, HTTP and MQTT. More information regarding EdgeLock Discrete TLS support can be found in, for example, ref.[6].

#### 4.1.1.11 (i) minimize the negative impact of by-products on the availability of services of others;

The impact of an OEM's product on other devices should be controlled in the OEM applications.

The availability of the SE/SA services is aided by its feature that different parties can independent operate within SE/SA. For instance, one cloud entity can conduct diagnostics while another cloud agent performs data analytics, ensuring that both entities remain distinct and separate.

#### 4.1.1.12 (j) be designed, developed, and produced to limit attack surfaces, including external interfaces;

Limiting the attack surface gives malicious actors the least possibility to mount an attack. As was the case with the confidentiality, authenticity, and integrity of data, the attack surface of a device is reduced by the collaboration of many security components. The main feature of the EdgeLock Discrete products that supports the OEM's compliance with the CRA through its ability to control access to sensitive key material throughout the chip lifecycle.

EdgeLock Discrete portfolio is pre-provisioned for ease of use in NXP's secure facilities with a set of device-unique key-pairs, certificates and identifiers that can be used to establish the initial Root of Trust (RoT) of the IoT device. This RoT can then be leveraged by the secure boot of the main processor, and used to authenticate and validate the boot image. This limits attacks occurring during manufacturing.

The EdgeLock Discrete Portfolio natively supports Secure Channel Protocol (SCP), including GlobalPlatform SCP03, FastSCP and Sigma-I (for A30). The SCP protocols allows to protect the integrity of local (Platform SCP) and ensure end-to-end (Applet level SCP) encrypted communication to protect from local spoofing and eavesdropping.

In the context of the CC certification, the attack surfaces are identified as part of the vulnerability analysis, and any unnecessary external interfaces reported. As a result, for the EdgeLock Discrete portfolio this requirement is addressed and verified during the security evaluation.

#### 4.1.1.13 (k) be designed, developed, and produced to reduce the impact of an incident;

While Requirement (2)(j) focuses on reducing the chance of a security incident, Requirement (2)(k) aims to reduce the consequences if it does happen. One main technique on the products of the EdgeLock Discrete portfolio that can support the OEM with compliance is through extensive protection of cryptographic keys and certificates. Additionally, the products offer software protocol isolation and mitigate the impact of attacks on the non-secure world. See also Requirement (2)(h).

The EdgeLock Discrete products allow you to securely generate and store credentials as secure objects inside its secure tamper-resistant hardware. Cryptographic operations involving secure objects are always performed inside the secure element or authenticator protected environment using the built-in cryptographic functions and algorithms. This can be utilized to diversify OEM cryptographic key usage and thereby limit the effect of a leaked or recovered key.

The products also support access management to credentials in the form of policies that can be used to specify the operations allowed on a given credential. Policies can be used, for example, to define if a key can be used for encryption, for signing or both and if a key is read-only or if it can be exported or deleted. This allows keys to be protected from export by malicious processes.

Application-level backup and recovery must be implemented on host-MCU platform and can leverage EdgeLock Discrete products' cryptographic capabilities to ensure authenticity and integrity (see Requirements (2)(d) and (2)(f)).

Lastly, to the reduction of impacts of incidents, its strength is supported by the vulnerability analysis which provide an overall security status of the implementation, and verified during the CC and FIPS (where applicable) certifications.

#### 4.1.1.14 (l) provide security-related information by recording and/or monitoring relevant internal activity, with an opt-out mechanism for the user;

Recording and monitoring must be implemented on the application level by the OEM.

The OEM may use security services claimed by the EdgeLock Discrete portfolio to support this requirement, for instance where a Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.

#### 4.1.1.15 (m) provide the possibility for users to securely and easily purge all data and settings

Upon decommissioning or re-sale of a device, all information should be erased on the EdgeLock product. The EdgeLock Discrete portfolio allows you to securely decommission your IoT device. Thanks to its strong tamper-resistance capabilities, it protects keys from extraction even after the device has been decommissioned. Moreover, policies can be set to restrict or disable the usage of stored credentials. For additional security, explicit delete of created credentials (excluding some pre-provisioned credentials) is supported.

The erasure of this information through a host-MCU can be implemented in software, but an explicit action must be undertaken in the decommissioning.

### 4.1.2 Annex I, Part 2. Vulnerability handling requirements

The second category in the Cyber Resilience Act requirements are surrounding the handling of vulnerabilities.

Related security primitives for Annex I, Part 2. Vulnerability Handling Requirements:

- Security Process Primitive 3: Vulnerability and Incident Management

The NXP Product Security Incident Response Team (PSIRT) is committed to rapidly addressing material security vulnerabilities in NXP products by responding and documenting reported material vulnerabilities and, if feasible and appropriate, by providing customers with clear guidance on the impact, severity, and, if available, mitigation.

This goes beyond mere software vulnerabilities and covers:

- Security incidents in NXP products (hardware or software).
- Flaws in NXP documents regarding security information or recommendations (e.g., datasheets and application notes).
- Security-sensitive NXP documents or security-relevant information regarding NXP are found in places where they should not be.
- Security-sensitive NXP products are found in places where they should not be.

The security vulnerabilities in NXP products are actively and carefully managed through a reporting, evaluation, and communication process.

This facilitates NXP customers in their compliance with requirements such as (see the full text in Annex I):

- Facilitating the sharing of information about potential vulnerabilities in third-party components contained in their product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;
- Ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay.

# 5 Beyond Annex I

## 5.1 Unique identification

In Annex II of the CRA, it is stated that all products with digital elements shall be accompanied by name and type and any additional information enabling the unique identification of the product. Products in the EdgeLock Discrete portfolio are pre-injected in NXP's secure facilities with a device-unique, read-only 7-byte UID that can be used to identify the whole IoT device. If the use case requires it, a custom identifier can also be injected in the product and protected against deletion and overwriting using the appropriate policies.

## 5.2 Software bill of materials

The software bill of material (SBOM) of a product lists the components in software and eases the traceability of vulnerabilities. In the recital (78) of the CRA, it is stated that OEMs should draft an SBOM for their product (it does not have to be public). NXP can aid OEMs in sharing the SBOM for NXP SDK software. This can be utilized by the OEM for their own SBOM creation and conform to this requirement of the CRA.

## 5.3 Security of the supply chain

The CRA emphasizes that the end product is more secure if its components and the supply chain are also well-protected. At its core, NXP has extensive security expertise and addresses the security demands of its products by leveraging its heritage in highly advanced secure elements for smartcards, government e-passports, and automotive applications. The company rigorously tests its sites, systems, and processes. In addition to ensuring the integrity of its secure components, NXP has a security-conscious culture within its organization, making security part of its DNA. Choosing an NXP product to design takes the first step toward the supply chain security of the OEM product.

## 5.4 Manufacturer’s obligations on due diligence for integrated components

The EdgeLock Discrete portfolio has been developed following a secure by design process, with the in-house NXP EdgeLock Secure Assurance program. Its products have been evaluated and certified by independent third parties against CC (Common Criteria) EAL 6+ with AVA_VAN.5 level of assurance under ISO 15408. Additionally there is an SE050 variant available which is FIPS 140-2 certified, and an SE052F variant as first FIPS 140-3 Level 3 certified secure element. The applet-updatable SE051 gains additional assurance in its security capabilities from its IEC 62443 4-2 certification. The certificates and Security Target explaining the details of the security claims in the scope of the certification are public. All this to support OEMs with their CRA obligations managing the risk of their supply chain, due diligence of integrated components, conformance of these components to the essential requirements, vulnerability management of the components and integration of technology functionality proportional to the specific OEM’s risk and use cases.

# 6 Abbreviations

**Table 2. Abbreviations**

| Abbreviation | Description |
|---|---|
| AES | Advanced Encryption Standard |
| CR | Component Requirement |
| DES | Data Encryption Standard |
| ECC | Elliptic-curve Cryptography |
| ECDH | Elliptic-curve Diffie-Hellman |
| ECDHE | Elliptic-curve Diffie-Hellman Ephemeral |
| EDR | Embedded Device Requirement |
| FR | Foundational Requirement |
| HDR | Host Device Requirement |
| HTTP | Hypertext Transfer Protocol |
| IoT | Internet of Things |
| KDF | Key Derivation Function |
| MAC | Message Authentication Code |
| MQTT | Message Queuing Telemetry Transport |
| NDR | Network Device Requirement |
| OEM | Original Equipment Manufacturer |
| OS | Operating System |
| PCR | Platform Configuration Register |
| PDE | Products with digital elements |
| PKI | Public Key Infrastructure |
| PRNG | Pseudo Random Number Generator |
| SA | Secure Authenticator |
| SAR | Software Application Requirement |
| SCP | Secure Channel Protocol |
| SE | Secure Element |
| SHA | Secure Hash Algorithm |
| SL | Security Level |
| SP | Security Primitive |
| TLS | Transport Layer Security |
| TRNG | True Random Number Generator |

# 7 References

[1] Webpage - Cybercrime Magazine: "Cybercrime To Cost The World $10.5 Trillion Annually By 2025" (link)

[2] Document - Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance) (link)

[3] White paper - NXP: SECURITY PRIMITIVES: COMMON NOMENCLATURE TO DESCRIBE SECURITY REQUIREMENTS IN (I)IoT SYSTEMS (link)

[4] Application note - AN12662 - Binding a host device to EdgeLock SE05x (link)

[5] Application note - AN13086 - EdgeLock™ SE05x to enhance the MCU boot sequence security (link)

[6] Application note - AN12400 - EdgeLock™ SE05x for secure connection to OEM cloud (link)

# 8 Revision history

**Table 3. Revision history**

| Document ID | Release date | Description |
|---|---|---|
| AN14671 v.1.0 | 13 October 2025 | • Initial version |

# Legal information

## Definitions

**Draft** — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

## Disclaimers

**Limited warranty and liability** — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

**Right to make changes** — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

**Suitability for use** — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

**Applications** — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**Export control** — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

**Suitability for use in non-automotive qualified products** — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

**HTML publications** — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

**Translations** — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

**Security** — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

**NXP B.V.** — NXP B.V. is not an operating company and it does not distribute or sell products.

## Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

**NXP** — wordmark and logo are trademarks of NXP B.V.

**EdgeLock** — is a trademark of NXP B.V.

# Tables

# Figures

# Contents