AN14601

Ease CRA Compliance with i.MX 93

Rev. 1.1 — 25 June 2025 Application note

Document information

Information	Content
Keywords	AN14601, i.MX 93, CRA requirements
Abstract	This document addresses OEMs who want to understand how i.MX93 can facilitate the implementation of CRA requirements.

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 number of devices and the size of the attack surface increasing, in 2025, there will be an estimated 10.5 trillion dollars in damages from cybercrime[1].

Security is a critical element in the development of products against intentional or unintentional threats. These threats include unauthorized access, installation of malware, ransomware, spyware, or loss of data with the corresponding privacy breach. They can have impact 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 the cyber resilience in the European Union, in 2024, the European Parliament adopted the Cyber Resilience Act[2] (CRA) to ensure the cybersecurity of products and software with digital elements. It covers anything from hard disks and chips to firewalls 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 11, 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 as maritime equipment).

For NXP, the impact is twofold. Firstly, NXP products are digital elements that must comply with CRA. Secondly, NXP products are integrated into OEM devices and machines that must comply with CRA.

Manufacturers of products with digital elements must comply with the essential requirements of the CRA. This requires manufacturers to "own" the product’s cybersecurity risk, 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 noncompliance with the essential requirements of the CRA amount to up to 15 million euros, or 2.5 % of the annual turnover, whichever is higher. Those surveillance-authorized are empowered to issue product recalls or, in extreme circumstances, withdrawal from the European market in cases of nonconformance. Therefore, the consequences of the CRA have a particularly large impact.

2 How to use this document

This document addresses OEMs who want to understand how i.MX 93 can facilitate the implementation of CRA requirements. While the i.MX 93 provides core security capabilities that can be mapped to the cybersecurity requirements of the CRA, the OEM must fill the remaining compliance gap by performing additional actions. This document provides guidance and supporting evidence from the i.MX 93 security capabilities toward the developer’s CRA conformance claims.

Throughout this document, the requirements and text of the CRA is condensed or simplified to summarize the ease of reading or highlight the applicability to the embedded context. For compliance, always consult the full text of the CRA. The applicability of this application note cannot guarantee the legal certainty required by the CRA conformance. Use it only as guidance for manufacturers addressing conformance requirements rather than the attestation of conformance to the CRA.

1 https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
2 https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Therefore, all information in this document 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 is not 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 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 secure or how to use 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[3]:

- Harmonized rules when bringing products or software with digital components to market.
- A framework of cybersecurity requirements governing the planning, design, development, and maintenance of such products, with obligations at every stage of the value chain.
- The obligation to provide a duty of care for the entire life cycle of such products.

The requirements listed throughout the act are as follows:

- **Cybersecurity by design and by default:** cybersecurity must be considered during the product design from the start. The CRA defines what kind of information and documentation to create and gather, as well as, depending on the product's security category, what kind of conformity assessments it must go through.
- **Essential cybersecurity and vulnerability handling requirements, including reporting obligations:** the CRA sets both technical cybersecurity requirements on the products to reduce the attack surface as much as possible and vulnerability handling requirements for vulnerabilities appearing after production.
- **Conformity assessment and compliance:** digital products are subject to a specified conformance assessment, depending on their security category.
- **Fines:** the CRA enforces compliance with the penalty of fines for noncompliant 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 the existing and upcoming legislation, such as the EU Cybersecurity Act.

The i.MX 93 can be of added value in meeting the requirements listed above. The security features of the i.MX 93 can be leveraged by the OEM to implement security countermeasures in an efficient and reliable manner.

Products with Digital Elements (PDEs, also called plain products in this document) are classified into four categories in the Cyber Resilience Act:

- **Nonimportant PDEs**
- **Important PDEs: class I**
- **Important PDEs: class II**
- **Critical PDEs**

Products that are not security-important fall in the nonimportant category. Products that are security-important are classified in the remaining categories based on their functionality, intended use, and optional further criteria. A different standard of assessment/certification applies depending on which category each product has in the CRA Annex III and IV. In the default category, a security self-assessment suffices, whereas critical products require a mandatory EU certification. The intention is that approximately 90 % of digital products will fall into the default category.

3 From: [EU Cyber Resilience Act | Shaping Europe's digital future]

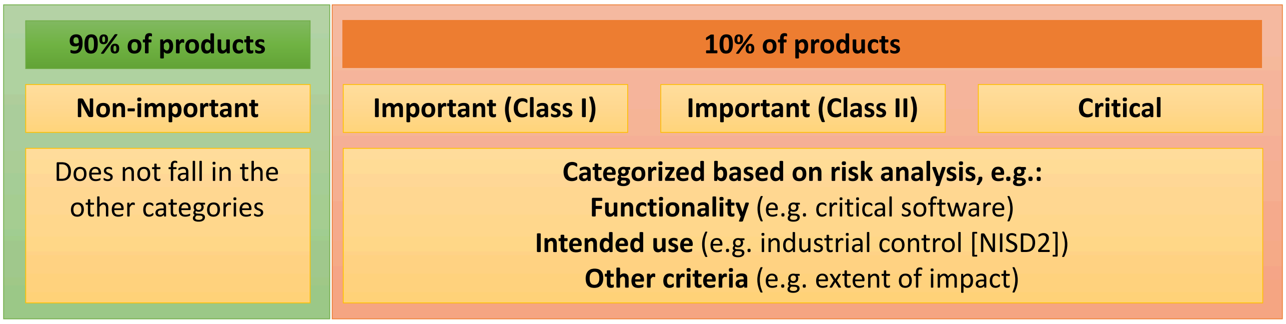

Figure 1. Cyber Resilience Act (CRA)

Examples of each class are shown in Table 1. A more extensive list is in the CRA regulation[4]. Conformance-assessment criteria are in Article 32 of the regulation.

Table 1. Examples

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

4 Leveraging the i.MX 93 to meet Cyber Resilience Act requirements

The clearest contribution of NXP products, such as the i.MX 93, to the CRA compliance of an end-product it integrates into lies in the i.MX 93 security features that can be leveraged by the end-product. Annex I of the CRA lists the Essential Cybersecurity Requirements (ECRs) for products with digital elements (PDEs). This chapter describes how the i.MX 93 can be leveraged to ease compliance with the requirements of Annex I (Part 1 and 2). The last section of this chapter provides additional support for the remaining requirements of the regulation.

Where possible, we use security terminology from the White-Paper Security Primitives: Common Nomenclature to Describe Security Requirements in (I)IoT Systems (see: https://www.nxp.com/securityprimitives).

4 https://eur-lex.europa.eu/eli/reg/2024/2847/oj

4.1 Cyber Resilience Act Annex I, Part 1

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

4.1.1 Requirement 1: Secure manufacturing

The first requirement in Annex I, Part 1, ties to 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, make a risk-based analysis to apply the right level of cybersecurity.

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

The i.MX 93 supports the OEM with security features leveraged by the end-product to get the desired security capability. Independent third parties evaluate and certify those functionalities against EN 17927 (SESIP scheme) and PSA Certified, both at Level 3, equivalent to the AVA_VAN.3 level of assurance under ISO 15408 (common criteria). The SESIP certificate supports the OEM claims of the adequate level of security implementation (proportionality to the risk) by clearly identifying the security functionality provided by the i.MX 93, as well as its level of assurance.

4.1.2 Requirement 2: Cybersecurity requirements

The requirement (2) of Annex I Part 1, 13 lists the cybersecurity measures that a product must comply with. This section explains them one by one. The risk assessment referred to in Article 13(3) of the CRA states that the products with digital elements shall:

a. **Be available on the market without known exploitable vulnerabilities:**
   Security is at the core of the i.MX 93 development cycle. 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.
   As part of the certification process under SESIP, the security evaluation and certification third parties perform a verification against known exploitable vulnerabilities in the i.MX 93.

b. **Be in a secure by default configuration and can reset the product to its original state:**
   The i.MX 93 includes the Advanced High Assurance Boot (AHAB). When enabled by an OEM, AHAB ensures the secure initialization of the device at each power-up and verifies the authenticity and integrity of the firmware.
   To reset to the original state, NXP recommends that OEM implement a secure backup and recovery mechanism. An Over-The-Air (OTA) update mechanism combined with the AHAB verifies the 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 the transmission. For the i.MX 93, see *Enabling SW Update on i.MX 6ULL, i.MX 8M Mini and i.MX 93* (document AN13872) for information about the Secure Over-the-Air Prototype for Linux. The i.MX 93 supports restoring the OEM device to a secure default configuration by ensuring the secure erasing of sensitive data when changing the life cycle state.
   The OEM should leverage the life cycle management of the i.MX 93 to close the JTAG ports after manufacturing. This puts the device into the default state that prevents attacks that utilize the debug functionality of a product on the market.
   The i.MX 93 has been assessed during the SESIP evaluation to a determined level of cybersecurity in a defined context of risks (AVA_VAN). This includes the verification of a secure default configuration and unambiguous identification by the integrator that the certified version is secure to evaluate and verify all guidance to ensure a secure integration.

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. For the i.MX 93, see *Enabling SW Update on i.MX 6ULL, i.MX 8M Mini and i.MX 93* (document AN13872) for information about the Secure Over-the-Air Prototype for Linux. 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 and not altered or corrupted during transmission.

d. **Protects against unauthorized access 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, the 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 i.MX 93 that supports the OEM in their compliance with Requirement (2)(d).

The i.MX 93 contains several mechanisms to ensure that sensitive data and operations can only be accessed by authorized processes. Firstly, the EdgeLock Enclave (ELE) Advanced Profile is an independent security domain that provides security services, which help ensure the key management and execution of cryptographic services. The ELE provides a secure environment that enables applications to execute secure cryptographic services. Secondly, TrustZone (TZ) is enabled on the Cortex-A55 and Cortex-M33 cores of the i.MX 93, which provides the segmentation of memory arrays and peripherals into either Secure (S) or Non-Secure (NS). This allows further protection of sensitive data from unauthorized processes.

The Advanced High Assurance Boot (AHAB) feature is a subcomponent of the ELE Boot ROM. The ELE uses the AHAB library to securely initialize the embedded device. The Root of Trust (RoT) on the i.MX 93 is the core security of the AHAB. It is established during Secure Provisioning, where 4 Super Root Keys (SRK) are generated, and their hashes are stored to the OEMS SRK hash fuses. During boot, the boot image provides four SRKs with an SRK table, which are used to recursively authenticate and validate the boot image. This process prevents the execution of unauthorized software. It should be combined with a secure updating flow for better protection against unauthorized software. Details on this are in Requirement (2)(c).

The i.MX 93 is enabled with a secure JTAG controller (SEC-JTAGC) to allow system debugging and testing. The JTAG can be restricted to the authorized use by symmetric authentication or permanently blocked (CLOSED LOCKED state).

The i.MX 93 offers the OCOTP memory that can be written by the OCOTP Controller in the secure enclave. The ELE can securely store passwords and private keys using the key in the ELE's protected memory. This helps to secure the most sensitive cryptographic data from unauthorized access.

In case any of the authentication mechanisms described above fail, a signal is sent to the System Security Monitor of the Battery-Backed Secure Module (BBSM), which can then take action (automatically notify or record in an audit log).

The i.MX 93 supports the NXP's EdgeLock 2GO (EL2GO) service. This can provision device-unique credentials, such as identity keypairs and certificates, securely into the secure storage of the device after the deployment of the device. Such credentials are then used to verify the identity of the device when the device connects to a cloud or other systems.

The OEM must implement further logging and data protection. The i.MX 93 can support OEM protection with its cryptographic acceleration options. See Requirement (2)(e) for details.

e. **Protect the confidentiality of stored, transmitted, or otherwise processed data (by applying encryption to the 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 i.MX 93 features that can support the OEM in their compliance to (2)(e).

The i.MX 93 has various security features to support confidential (secure, encrypted) data storage. For one, information is securely stored in the Battery-Backed Secure Module (BBSM). It incorporates a security monitor that checks for various security conditions. If it detects a security violation, it zeroizes the secret data and issues an interrupt request.

To support the OEM in securely storing the data at rest in the less secure memory, the i.MX 93 EdgeLock Enclave (ELE) can also encrypt information for secure storage. The On-The-Fly Decryption (OTFAD) can be performed by the FlexSPI interface to store the encrypted application code or data in an external flash device.

For other applications that require encryption (like data in transit), the i.MX 93 ELE supports the acceleration of cryptographic operations. The ELE includes both symmetric and asymmetric crypto accelerators in the ELE to securely process keys and data for encrypted transmission (by TLS). This includes:

- Symmetric cryptography: AES 128/192/256 in supported modes including ECB/CBC/CTR/OFB/CCM/GCM
- Asymmetric cryptography: RSA up to 4096, ECC curves up to P-521
- Hash functionality: SHA 224/256/384/512

For the confidential storage of cryptographic certificates and keys, the i.MX 93 offers the Hardware Security Module (HSM) functionality in the ELE. It can store key attributes, such as the identifier and key type, and both volatile and persistent keys. For nonvolatile memory export, persistent keys are encrypted and encapsulated (with an IV generated by the ELE FW). When required, the encapsulated keys are loaded into the internal ELE memory and decapsulated.

f. **Protect the integrity of stored, transmitted, or otherwise processed data, commands, programs, and configuration against unauthorized modification and report on corruptions:**

After the 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 i.MX 93 aspects that support their compliance with this requirement.

The Advanced High Assurance Boot (AHAB) feature is a subcomponent of the ELE Boot ROM and helps to protect against the bypass of authorized firmware. It works by checking the integrity of the software load to ensure that the software that is going to be executed was not modified to work differently than what was loaded by the manufacturer (either at the factory or as part of software upgrades).

The ELE can also encrypt information for secure storage in the less secure memory. OTFAD can be performed by the FlexSPI interface to store encrypted application code or data in an external flash device and helps to ensure the integrity of that data.

The ELE supports symmetric crypto accelerators that can be used to implement further integrity checks. This includes:

- AES 128/192/256 in supported modes, including ECB/CBC/CTR/OFB/CCM/GCM
- Hash: SHA2 224, 256, 384, 512
- Authentication modes: HMAC, CMAC

If any of the integrity check mechanisms described above fails, a signal is sent to the System Security Monitor of the BBSM, which then can take action (automatically notify or record in an audit log).

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"):**

The minimization of data ensures that a potential attacker has the least attack surface possible. The OEM must realize this requirement for their application data.

When utilizing the i.MX with EL2GO, we support the OEM by minimizing the user data processed in the cloud. EL2GO does not profile on user data, like IP addresses, and does not store this type of data for later use.

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. You can do this by applying software isolation techniques to protect essential processes from external nonessential applications. Both the ELE and TrustZone offer software isolation and thereby mitigate against denial-of-service attacks.

Another method to restrict the data flow in a component is to impose network segmentation. By splitting the communication channels within a component into access-controlled subnetworks, both performance and security can be improved. The i.MX 93 supports data flow restriction requirements through provisions for network segmentation. The application-level network segmentation must be implemented on top of the i.MX 93 platform. The "netconf/YANG" with TLS can be used on the i.MX 93 for the secure remote configuration, which protects the system configuration from tampering. The key storage of the ELE manages the TLS keys.

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 must be controlled in the OEM application.

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 i.MX 93 supports the OEM’s compliance with the CRA through its ability to control access throughout the chip life cycle.

The i.MX 93 is supported by the ELE's trust-provisioning flow of the EdgeLock Enclave (ELE) . During the (secure) provisioning, the Root of Trust (RoT) is established, four Super Root Keys (SRK) are generated, and their hashes are stored in the OEMS SRK hash fuses. During the AHAB secure boot, the boot image provides four SRKs with an SRK table, and they are used to recursively authenticate and validate the boot image. This limits attacks occurring during manufacturing.

The ELE chip life cycle allows for two primary isolated security domains: the EdgeLock secure enclave and the SoC. The life cycle states progress from the NXP manufacturing life cycles to the OEM development and manufacturing states, to the in-field product state, and then to reopen up the chip from fully closed to partially closed to fully open again for silicon analysis in the case of a failure. The life cycle state closes the appropriate test and debug port to limit the attack surface.

In the context of the SESIP certification, the attack surfaces are identified as part of the vulnerability analysis, and any unnecessary external interfaces are reported. At the i.MX 93, this requirement is addressed and verified during the security evaluation.

k. **Be designed, developed, and produced to reduce the impact of an incident:**

While Requirement (2)(j) focuses to reduce the chance of a security incident, Requirement (2)(k) aims to reduce the consequences (if they happen). One main technique on the i.MX 93 that can support the OEM with compliance is the use of software isolation and extensive protection of cryptographic keys and certificates.

Both the ELE and TrustZone offer software isolation and mitigate the impact of attacks on the nonsecure world. See also Requirement (2)(h).

The Battery-Backed Security Module (BBSM) provides features that help the OEM to ensure that the data kept by the device is protected against tamper attacks. It incorporates security logic that checks for various security conditions. If a security violation is detected, it zeroizes the secret data and issues an interrupt request. This reduces the data stolen in case of an attack.

The ELE supports secret key generation, storage, and management. This can diversify the OEM cryptographic key usage and thereby limit the effect of a leaked or recovered key.

Application-level backup and recovery should be implemented on the top of the i.MX 93 platform and it can leverage the i.MX 93 cryptographic capabilities to ensure authenticity and integrity (see Requirements (2)(d) and (2)(f)).

Additionally to the reduction of impacts of incidents caused by the i.MX 93 implementation above, its strength is supported by the vulnerability analysis (which provides an overall security status of the implementation) and verifies it during the SESIP certification.

l. **Provide security-related information by recording and/or monitoring relevant internal activity, with an opt-out mechanism for the user:**

The recording and monitoring on the application level should be implemented by the OEM.

The OEM should use the security services claimed by the i.MX 93 to support this requirement (for instance Root-of-Trust base, secure cryptography, or secure storage, and so on). However, this is determined case by case.

m. **Provide the possibility for users to securely and easily purge all data and settings:**

Upon decommissioning or resale of a device, erase all information in the i.MX 93. The EdgeLock Enclave (ELE) supports secure provisioning. You can implement the erasure of this information in software, but you must undertake an explicit action in the decommissioning. The cryptographic support of the i.MX 93 ELE can be leveraged to port the settings and data to a backup before the decommissioning. The erasure of data is supported by the brick-state in the device life cycle management. This ensures that the device information cannot be read out after decommissioning.

For data encrypted with OTFAD, the erasure of the encryption keys also, in effect, purges the data encrypted with those keys.

4.2 Annex 1, Part 2: Vulnerability handling requirements

The second category in the Cyber Resilience Act requirements surrounds the handling of vulnerabilities. NXP supports the requirements of Annex 1, Part 2 as follows.

The NXP Product Security Incident Response Team (PSIRT) rapidly addresses the material security vulnerabilities in NXP products by responding and documenting the 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 (data sheets and application notes).
- Security-sensitive NXP documents or security-relevant information regarding NXP are in places where they must not be.
- Security-sensitive NXP products are in places where they must 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 1):

- 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 1

Lastly, outside of the product-security-requirement focused Annex 1, there are additional (process) requirements where NXP offers support. We list the most important facets in this section.

5.1 Unique identification

Annex II of the CRA states that all products with digital elements shall be accompanied by their name and type and any additional information enabling the unique identification of the product. In the i.MX 93, the EdgeLock Enclave's Trust Provisioning (TP) flow provides a unique, provable, and attestable identity to each manufactured part. The OEM leverages this to conform to this requirement of the CRA.

5.2 Software Bill of Materials (SBOM)

The Software Bill of Materials (SBOM) of a product lists the components in software and eases the traceability of vulnerabilities. The recital (78) of the CRA states that OEMs should draft an SBOM for their product (it does not have to be public). NXP can help OEMs in sharing the SBOM for the NXP SDK software. It can be used by the OEM to create their own SBOM 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. 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 the 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 i.MX 93 was developed following a secure-by-design process with the in-house NXP EdgeLock Secure Assurance program. The i.MX 93 was evaluated and certified by independent third parties against EN 17927 (SESIP scheme) and PSA-certified. The certificates and the security target, explaining the details of the security claims in the scope of the certification, are public. All this supports 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 Acronyms and abbreviations

Table 2. Acronyms and abbreviations

Term	Definition
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
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
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 Revision history

Table 3. Revision history

Document ID	Release date	Description
AN14601 v.1.1	25 June 2025	• Reformatted Section 4.1.2.
AN14601 v.1.0	14 April 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.

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, μVision, Versatile — are trademarks and/or registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved.

EdgeLock — is a trademark of NXP B.V.

Contents

Date of release: 25 June 2025
Document identifier: AN14601