AN15228

Ease CRA compliance with EdgeVerse™ NFC Reader Portfolio

Rev. 1.0 — 3 November 2026 Application note

Document information

Information	Content
Keywords	CRA, NFC Reader, PN7642, PN5190, PN716x, PN722x, PN76AC, CLRC663 plus family, Cybersecurity
Abstract	This document outlines how the NXP EdgeVerse NFC Reader portfolio can support OEMs in addressing selected Cyber Resilience Act requirements through trusted reader security capabilities, firmware life cycle support, and vulnerability-management processes. It also reinforces that final CRA classification, conformity assessment, and product-level compliance remain the responsibility of the OEM.

1 Introduction

The potential risk from cyberattacks increases as the number of connected devices, machines, devices, and sensors keeps growing. By 2033, the number of IoT devices worldwide is expected to double, surpassing 40 billion ref. [16]. With growing number of devices and size of attack surface increasing, in 2031, there will be an estimated $12.2 trillion in damages from cybercrime ref. [17].

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 Cyber Resilience Act (CRA) ref. [1] to ensure the cybersecurity of products and software with digital elements. In essence, it covers anything from hardware components and connected devices 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 11, 2027. Article 14 reporting obligations apply from September 11, 2026, and Chapter IV applies from June 11, 2026. Products operating in markets and applications covered by sector-specific Union legislation with equivalent cybersecurity requirements may be excluded as specified in the 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, document the measures taken and communicate relevant information to users. Only when the applicable conformity requirements are met may the manufacturer affix the CE mark to products covered by the regulation.

Penalties for non-compliance with the essential requirements of the CRA can amount to up to 15 million euros, or 2.5 % of the total worldwide annual turnover for the preceding financial year, whichever is higher. Market surveillance authorities are also empowered to require corrective measures and, where appropriate, product recalls or withdrawal from the Union market.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

2 How to use this document

This document is addressed to OEMs and manufacturers (hereafter referred to as OEMs) interested in understanding how products from the NXP NFC reader portfolio can be used to facilitate CRA compliance for their device implementation. While selected reader products provide security capabilities that can be mapped to certain cybersecurity requirements of the CRA, the available contribution differs significantly between pure NFC frontends, firmware-based frontends, NFC controllers with integrated firmware, and the programmable PN7642 NFC open controller. 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 selected product capabilities towards the developer's CRA conformance claims.

Note that throughout this document the requirements and text of the CRA are condensed or simplified to summarize for ease of reading or highlight applicability to the embedded context. For compliance, the full text of the CRA and applicable implementing acts should always be consulted. The application of this document cannot guarantee the legal certainty required by CRA conformance and it should be used only as 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.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

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 products are secure or how to utilize them securely. The main CRA document consists of 8 chapters and 8 annexes providing additional details. The CRA's goal is to guarantee:

- 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 to be met 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 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 to create and gather, as well as depending on the product's security category, what kind of conformity-assessment 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.

OEMs can leverage selected capabilities of the NXP NFC reader portfolio to support implementation of specific CRA requirements. Reader-specific features such as secure firmware handling, cryptographic support, key management, RF robustness, protected interfaces and life cycle controls can help OEMs implement security countermeasures more efficiently. The level of contribution depends on the chosen reader architecture and on how the reader is integrated with the host, credential technology, application software and overall product life cycle.

Products with digital elements are classified into four categories in the CRA:

- Default PDEs.
- Important PDEs: Class I.
- Important PDEs: Class II.
- Critical PDEs.

Approximately 10% of all PDEs 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 critical products may become subject to mandatory European cybersecurity certification. Where that requirement does not apply, the conformity assessment procedures specified in Article 32 CRA apply, which may require third-party assessment.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

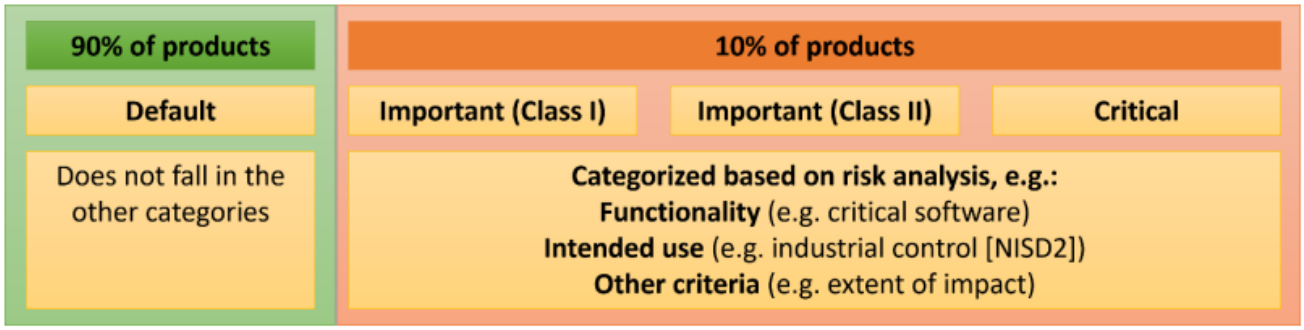


Figure 1. CRA products

Examples of each class are listed below. A more extensive list can be found in the CRA regulation ref. [1]. Commission Implementing Regulation (EU) 2025/2392 provides the current technical descriptions of the Annex III and Annex IV categories ref. [2]. Conformity assessment criteria can be found in Article 32 of the CRA.

Note: *The information below reflects the current understanding of CRA and its implementing act at the time of writing. Future delegated or implementing acts, harmonized standards and guidance can add further detail. Readers should verify authoritative sources for the applicable product and use case.*

Table 1. Examples of products with digital elements

See ref. [18].

Category	Examples
Default	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 Smart cards or similar devices, including secure elements

3.1 Reader products and CRA category

CRA classification should be determined based on the core functionality and intended purpose of the product with digital elements that is placed on the market. Under Article 7, integrating a product that itself has the core functionality of an Annex III category does not, by itself, automatically make the integrating end product subject to the same Article 32 conformity-assessment procedure ref. [1]. Therefore, the use of an NXP NFC reader IC in an OEM product does not automatically determine the CRA category of that OEM end product. The OEM must assess the final product in its own context, considering its core functionality, intended use, system architecture and applicable Annex III or Annex IV category descriptions.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

Reader products require careful CRA classification because Annex III Class I includes authentication and access control readers. This classification is relevant when authentication or access control is the core functionality of the product placed on the market. It should not be interpreted as automatically applying to every NFC reader IC or controller capable of communicating with a card, tag or NFC device.

PN7642 has been assessed by NXP as an Important Product with Digital Elements, Class II, under the CRA classification framework. This classification is based on NXP's product-specific CRA assessment and should not be understood as a claim that PN7642 provides hardware attack-prevention or tamper-resistant protection equivalent to a secure element, smart card or tamper-resistant microcontroller.

PN7642 is GlobalPlatform SESIP Level 2 certified and integrates a Cortex-M33 MCU with a security subsystem. SESIP Level 2 provides useful independent assurance evidence within its certification scope, but CRA classification and security certification are separate concepts. OEMs remain responsible for assessing the CRA category, conformity route and cybersecurity requirements of their final product based on its intended purpose, core functionality and system architecture.

Table 2. NXP EdgeVerse NFC Reader product CRA classification considerations

NXP reader product / family	Reader type	NXP CRA classification view	Customer note
CLRC663 plus family	NFC frontend	Default Product with Digital Elements	OEM host owns most security, update, credential and final-product CRA responsibilities.
PN5190	Firmware-based NFC frontend	Default Product with Digital Elements	Provides NXP-managed reader firmware and security-relevant life cycle support; OEM remains responsible for host/application security.
PN7160 / PN7161	NFC controller	Default Product with Digital Elements	Integrated NFC controller firmware; final authentication, policy and product classification remain OEM responsibilities.
PN7220 / PN7221	NFC controller	Default Product with Digital Elements	Integrated controller firmware with security-relevant life cycle support; OEM assesses final product context.
PN76AC	NFC controller for smart access	Default Product with Digital Elements	Integrated controller firmware component for access-related use cases; OEM owns credential policy and end-product CRA assessment.
PN7642	Programmable NFC controller with security subsystem	Important PDE, Class II	Assessed by NXP as Class II. This does not imply hardware attack-prevention or tamper-resistant protection equivalent to a secure element or smart card.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

4 Leveraging the NXP NFC reader portfolio to meet Cyber Resilience Act requirements

As mentioned in the introduction, the clearest contribution of the NXP NFC reader products considered in this application note to CRA compliance of an end product in which they are integrated lies in product-specific security and life cycle features that can be leveraged by the end product. These contributions differ materially between NFC frontends, firmware-based frontends, NCI controllers and a programmable secure reader controller. Additional contributions are discussed in Section 5 "Beyond Annex I".

In Annex I of the CRA, the Essential Cybersecurity Requirements (ECRs) are listed for products with digital elements. In this chapter, we expand on how selected NXP NFC reader products can be leveraged to ease compliance with Section 4.2.1 "Annex I, Part I. Security requirements" and Section 4.2.2 "Annex I, Part II. Vulnerability handling requirements".

4.1 Reader architectures and security responsibility

The reader architecture determines where security functions are implemented and where cybersecurity responsibility is concentrated. A pure frontend transfers RF frames and protocol support to a host that owns most application security. An NFC controller with integrated NXP firmware moves the low-level NFC and NCI functionality into the controller, while the host still owns authorization policy and application data. Programmable NFC controllers move part of the application logic into the reader IC. The specific security responsibility split depends on the product architecture. PN7642 extends this model with an integrated Cortex-M33 MCU and security subsystem, enabling more security functions to be implemented inside the reader IC.

Table 3. Reader architecture and security responsibility split

Architecture	Representative products	NXP reader responsibility	OEM system responsibility
NFC frontend	CLRC663 plus family	Provides RF and protocol interface; no OEM application runs inside the reader IC.	The host owns application security, credentials, update mechanism, logging, and CRA evidence.
Firmware-based NFC frontend	PN5190	NXP firmware handles reader functions and component firmware life cycle.	The host owns application logic, authorization policy, credential handling, and end-product updates.
NCI controller with integrated firmware	PN7160 / PN7161 PN7220 / PN7221 PN76AC	The controller owns NFC/NCI execution and reader firmware behavior.	The host owns access-control policy, application data, backend interaction, and final-product security claims.
Programmable NFC open controller	PN7642	Provides NXP secure firmware, programmable MCU environment, secure key store, crypto and secure update support.	OEM owns user application security, provisioning, life cycle configuration, update policy, and integration with the final product.

4.2 Cyber Resilience Act

4.2.1 Annex I, Part I. Security requirements

This part of the document covers security requirements relating to the properties of products with digital elements.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

4.2.1.1 Requirement (1): Secure manufacturing

The first requirement in Annex I, Part I, 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 life cycle. 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.

PN7642 supports OEMs with security features that can be leveraged by the end product to achieve selected cybersecurity objectives. Its GlobalPlatform SESIP Level 2 certification provides independent component-level assurance evidence for the security functionality covered by the certificate scope. This evidence can support the OEM’s CRA technical documentation, but it does not replace the OEM’s end-product risk assessment, CRA classification or conformity assessment.

For Default-category NFC frontend products, NXP provides component documentation, configuration guidance, and PSIRT support that can help OEMs integrate the reader securely. Security controls such as credential protection, application logic, updates, and vulnerability handling are mainly implemented at the host or system level.

For Class I NXP reader products, integrated firmware and life cycle features can provide stronger component-level support for selected CRA requirements. Depending on the product, this may include NXP-managed firmware, version traceability, controlled configuration, secure update support, and PSIRT-based vulnerability handling. These capabilities support the OEM’s technical documentation but do not replace the OEM’s end-product risk assessment, CRA classification, or conformity assessment.

4.2.1.2 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:

4.2.1.3 a) be made available on the market without known exploitable vulnerabilities

NXP EdgeVerse NFC Reader products support this requirement through NXP’s security-by-design practices, PSIRT-led vulnerability handling, firmware release governance, and product/firmware traceability. For reader products with embedded firmware, the OEM should track the exact product, silicon revision, and firmware version, monitor NXP release notes and security communications, and assess whether any disclosed issue creates an exploitable path in the final product. Where secure update mechanisms are available, they can support remediation of relevant component vulnerabilities; however, the OEM remains responsible for vulnerability assessment, software quality, secure integration, and final-product compliance.

For a programmable reader product, PN7642, the OEM must additionally manage the security quality, software composition, testing, and vulnerability handling of the customer application code running on the device.

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

To reset the product to its original state, NXP recommends that the OEM implement a secure backup and recovery mechanism at the end-product level. For the CLRC663 plus family, the OEM host is responsible for restoring the approved reader register/EEPROM configuration, RF settings, access policy, and any related SAM provisioning state where a SAM is used. For PN5190, the OEM should restore the approved reader firmware and configuration baseline using NXP-supported firmware-update mechanisms, where applicable, and track the deployed firmware/configuration version as part of the product maintenance process.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

For PN716x and PN722x, which include integrated NXP firmware and NCI-based host control, the OEM should maintain the approved controller firmware/configuration baseline and apply NXP-provided firmware or configuration updates according to the product recovery and maintenance policy.

For PN7642, the OEM can use the documented security capabilities, including secure boot support, secure key storage, cryptographic functions and secure firmware-update support, to strengthen the recovery architecture. In all cases, restoring the reader IC or reader configuration alone does not reset the complete product; the OEM remains responsible for host software state, user data, credentials, access policy, and any backend-linked authorization state.

4.2.1.5 (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. NXP recommends that OEM OTA mechanisms implement independent validity and/or conformity checks for any newly downloaded firmware. Such checks should already be part of the OEM's OTA implementation to ensure that the update was from a trusted source and not altered or corrupted during transmission.

NFC reader architectures differ significantly in their update model and in the level of security assurance they can provide for security updates.

For CLRC663 plus family frontends, vulnerability remediation is mainly implemented at host software, middleware, configuration, or system level, because the OEM application and update mechanism reside outside the reader IC.

For PN5190, PN722x, PN7642, PN716x, the NXP firmware binary is protected using RSA signature and AES encryption, helping ensure that firmware updates originate from a trusted source and have not been altered during distribution or installation. This provides a stronger component-level contribution to the CRA requirement that vulnerabilities can be addressed through security updates.

In all cases, secure update of the reader component does not replace secure update of the complete OEM product; the OEM remains responsible for update distribution, conformity checks, rollback strategy, host software, customer application code, credentials, backend dependencies, and final-product CRA compliance.

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.

4.2.1.6 (d) protect against unauthorized access by using mechanisms such as authentication, identity, or access management systems and report 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 features of the EdgeVerse NFC Reader portfolio that supports the OEM in their compliance with requirement (d).

The level of NXP support depends on the selected reader architecture. CLRC663 plus family frontends provide the RF/protocol interface, while authentication, access policy and reporting are implemented by the host and, where used, a SAM for protected key storage and cryptographic operations. PN5190, PN716x, and PN722x

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

provide NXP-managed reader/controller firmware for the NFC communication path, while credential validation, access decisions, logging, and backend integration remain under OEM control.

PN7642 incorporates several hardware-based mechanisms that ensure that sensitive data and cryptographic operations are only accessible to authorized processes. PN7642 features a secure key store and a key transfer unit, which together prevent keys from ever being exposed to CPU-accessible memory by moving them directly into the cryptographic engines. This ensures secure key management and protected execution of cryptographic services.

PN7642 enforces firmware integrity through secure boot, which verifies the authenticity and integrity of the bootloader and application firmware before execution, preventing unauthorized or tampered code from running. Reporting of possible unauthorized access remains an end-product function and shall be implemented by OEMs through the host software or user application.

4.2.1.7 (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 (d), the protection of confidentiality also relates to many security paradigms. The focus is on the most important EdgeVerse NFC Reader features that can support the OEM in their compliance with requirements (e).

Confidentiality must be considered across the complete data path, including the NFC air interface, reader IC, reader-to-host interface, host software, network connection and backend. NFC communication should not be considered confidential merely because it is contactless; confidentiality of application data requires the selected credential or card protocol to encrypt the relevant messages, and any exposed reader-to-host path must be protected by the OEM system architecture.

NXP EdgeVerse NFC Reader products support this requirement at component level, depending on the selected architecture. CLRC663 plus family, PN5190, and NCI controllers such as PN716x and PN722x provide the RF, protocol or controller communication path, but do not automatically encrypt arbitrary OEM application data.

PN7642 has various security features to support the OEM in securely storing data. PN7642 can also encrypt information for secure storage using the same cryptographic schemes as available for NXP firmware. The keys for signing and encryption shall be provisioned by the customer.

For other applications that require encryption, like data in transit, the PN7642 supports the acceleration of cryptographic operations. Both symmetric and asymmetric crypto accelerators are included to securely process keys and data for encrypted transmission (for example, by TLS). This includes:

- Symmetric cryptography: AES 128/256 in supported modes incl. CCM/CBC/ECB/CTR/GMAC
- Asymmetric cryptography: RSA, ECC P-256/384 curve, Ed25519, ECC key generation, Sign/Verify
- Hash functionality: SHA 256

The OEM remains responsible for end-to-end confidentiality, including credential selection, key provisioning, host protection, backend security, and final-product compliance.

4.2.1.8 (f) protect the integrity of stored, transmitted, or otherwise processed data, commands, programs, and configuration against unauthorized modification, and report on corruptions

After authenticity in requirement (d) and confidentiality in requirement (e), requirement (f) focuses on the integrity of data on the product. Again, the focus is on the most important EdgeVerse NFC Readers' aspects that support their compliance with this requirement.

Integrity protection must cover reader firmware, configuration, application commands, contactless data, and host/backend interactions. RF framing, CRC and protocol error checks can detect transmission errors, but they should not be treated as protection against intentional modification. For security-relevant data, commands or configuration, the OEM should use cryptographic integrity mechanisms such as secure messaging, MACs,

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

signatures, authenticated configuration handling, or secure firmware-update processes, depending on the product risk assessment.

NXP EdgeVerse NFC Reader products support this requirement at different levels. CLRC663 plus family frontends rely mainly on the host, middleware and, where used, a SAM to protect configuration, commands, and credential-related data. PN5190, PN722x, and PN7642 provide secure firmware-update mechanisms that help protect updateable firmware against unauthorized replacement. PN716x provides integrated controller firmware and NCI-based host control, while integrity of host commands and application data remains under OEM control.

PN7642 adds secure boot support, protected key storage and cryptographic functions that can help the OEM application authenticate data, commands, and security-relevant configuration.

PN7642 supports crypto accelerators that can be used to implement integrity checks. This includes:

- Symmetric cryptography: AES 128/256 in supported modes incl. CCM/CBC/ECB/CTR/GMAC
- Asymmetric cryptography: RSA, ECC P-256/384 curve, Ed25519, ECC key generation, Sign/Verify
- Hash functionality: SHA 256

Reporting corruptions, such as failed verification, invalid secure messages, unexpected configuration changes or rejected updates, remains an end-product function implemented by OEM.

4.2.1.9 (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”)

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

The reader ICs covered by this document do not determine which application data are retained by the host, backend or cloud service. The OEM should minimize data at the point of collection, avoid unnecessary logging of raw identifiers, apply suitable retention limits, and use pseudonymous, tokenized or backend-resolved identifiers where appropriate.

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

Requirement (h) aims to mitigate attacks that attempt to make the product unavailable. NFC readers ICs covered in this document operate on an externally accessible RF interface and may be subject to malformed payloads, mass/repeated polling, or RF jamming.

NXP reader products include RF and protocol robustness features, depending on the product, such as dynamic power control, adaptive waveshape control, EMD/error handling, and receiver configuration options. These features can improve reliable NFC operation in difficult RF environments, but they should be treated only as robustness support, not as complete cybersecurity denial-of-service protection.

The OEM remains responsible for end-product availability and DoS mitigation. This includes bounding polling, retry rates, and timeouts; validating host commands and NFC input; defining fallback or safe-state behavior when NFC communication is unavailable; and ensuring that essential product functions are not degraded by reader-related faults.

4.2.1.11 (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 application.

NFC reader polling and RF-control functions can help simplify host timing implementation, while the OEM remains responsible for defining reader activation policy, timeout handling and application-level recovery. Data

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

received through the contactless interface should be validated by the protocol stack and application before it is trusted or used for security-relevant decisions.

4.2.1.12 (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.

In NFC reader-based products, the relevant attack surface includes the RF interface, host interface, enabled protocols, firmware or application update paths, debug/programming access, configuration mechanisms and, where applicable, OEM application software running on the reader controller.

The selected reader architecture influences where this attack surface is located. CLRC663 plus family frontends expose the RF and host interfaces but do not host OEM application code. PN5190 and NCI controllers such as PN716x and PN722x add NXP-managed secure firmware and command interfaces that should be configured and maintained according to NXP guidance. PN7642 adds a programmable controller environment, creating additional trust boundaries for OEM application code, provisioning, update policy and debug access. PN7642 also provides managed secure firmware updates and further provides secure boot, protected key storage, and cryptographic functions support that can help maintain a trusted software baseline and protect security-sensitive assets when correctly integrated.

The OEM should enable only required RF protocols and host interfaces, restrict debug and production programming access, validate all data crossing RF and host boundaries, and prevent untrusted NFC input from being passed directly into privileged host or application functions.

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

While requirement (j) focuses on reducing the chance of a security incident, requirement (k) aims to reduce the consequences if it does happen.

In NFC reader-based products, the impact can be reduced by limiting credential exposure, separating trust boundaries, avoiding unnecessary sharing of long-term keys across devices or fleets, and defining recovery actions such as credential revocation, firmware update, or backend deny-listing.

NXP EdgeVerse NFC Reader products can support this objective at component level. For CLRC663 plus family designs, use of a SAM can help isolate credential keys and cryptographic operations from the host MCU. Secure firmware-update mechanisms on PN5190, PN722x and PN7642 can also support incident response where the issue can be remediated in updateable firmware.

For PN7642, protected key storage and key-transfer mechanisms can reduce exposure of symmetric keys to application software and support separation between different key roles, when combined with appropriate provisioning, key diversification and revocation policy.

The OEM remains responsible for defining the complete incident-response strategy of the final product, including credential rollover, revocation, recovery, service procedures, backend controls and final-product compliance.

4.2.1.14 (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 at the application or system level by the OEM.

NXP EdgeVerse NFC Readers can support this requirement at component level, but they are not complete security logging systems. For frontends, such as CLRC663 plus family, PN5190, and NCI-controllers of the

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

PN716x or PN722x architectures, the external host is generally responsible for event collection, correlation, storage, and reporting.

For programmable controllers of the PN7642-based designs, the OEM user application can monitor reader-specific events locally and forward relevant security information to the connected host (if any), backend, or access-management system. Logging should be proportionate, privacy-aware, and aligned with data-minimization principles.

The OEM remains responsible for defining which events are recorded, how long they are retained, how they are reported, and how any applicable user opt-out mechanism is implemented in the final product.

4.2.1.15 (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 device.

Data purge is a system-life cycle requirement. Reader ICs may contain firmware, nonvolatile RF configuration, key material, or application data whose life cycle differs from user data stored by the host.

For PN7642, the OEM should define how customer-provisioned keys, user-application data, and configuration are invalidated or reprovisioned during decommissioning, service, or resale, using only product-supported life cycle mechanisms. Secure key storage prevents ordinary application reusing of key material, but key protection is not the same as satisfying the complete end-product purge requirement. Host memory, backend records, and credentials outside the reader must be handled separately.

For PN5190 and NCI controllers PN716x and PN722x, the OEM should restore or remove mutable reader configuration as supported and separately purge host-side application data. For a pure frontend, purge obligations are normally concentrated in the host and external secure-storage components.

4.2.2 Annex I, Part II. Vulnerability handling requirements

The second category of CRA requirements focuses on the handling of vulnerabilities. NXP can support the requirements of Annex I, Part II as follows:

NXP Product Security Incident Response Team (PSIRT) is committed to rapidly addressing material security vulnerabilities in NXP products by responding to and documenting reported material vulnerabilities and, where feasible and appropriate, providing customers with clear guidance on impact, severity and, if available, mitigation (ref. [14]).

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 (find 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.

The OEM remains responsible for vulnerability management of the finished product.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

5 Beyond Annex I

Lastly, outside of the product-security-requirement focused Annex I, 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 are accompanied by the product name, type, and any additional information enabling the unique identification of the product. NFC reader products can provide a unique identification (die ID or product ID) for each manufactured part. OEMs can make use of this information to conform to this CRA requirement.

Component identification should not automatically be equated with legal identification of the complete OEM product. The OEM remains responsible for the name, type, manufacturer information, serialization and traceability of the product placed on the market.

5.2 Software bill of materials

The CRA's vulnerability-handling requirements require manufacturers to draw up an SBOM in a commonly used, machine-readable format covering at least the product's top-level dependencies. NXP may provide relevant product-level SBOM with top-level dependencies, where available and appropriate, as an input to the OEM's SBOM. The OEM remains responsible for the completeness and maintenance of the SBOM for its final product. The SBOM does not generally have to be made public, but it forms part of the manufacturer's technical documentation and may need to be provided to a market surveillance authority upon a reasoned request.

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 smart cards, 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 serves as the first step toward the supply chain security of the OEM product.

5.4 Manufacturer obligations on due diligence for integrated components

The OEM remains responsible for due diligence on integrated third-party components and for ensuring that those components do not compromise the cybersecurity of the finished product. NXP product datasheets, security guidance, certification evidence, firmware release notes, provisioning records and PSIRT communications can provide evidence inputs for the OEM technical documentation.

The CRA category of the final OEM product is not inherited from the integrated reader component. The OEM must assess the final product's core functionality and intended purpose, determine the applicable conformity-assessment route, and document how the selected reader contributes to risk controls. Similarly, the CRA category of an NXP reader product placed on the market cannot be inferred solely from labels such as "frontend", "controller", firmware programmability or SESIP certification.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

6 Abbreviations

Table 4. Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
CC	Common Criteria
CRA	Cyber Resilience Act
DPC	Dynamic Power Control
ECC	Elliptic-curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EMD	Electromagnetic Disturbance
ECR	Essential Cybersecurity Requirement
FW	Firmware
GPIO	General-purpose input/output
HMAC	Hash-based Message Authentication Code
I²C	Inter-Integrated Circuit
MCU	Microcontroller Unit
NCI	NFC Controller Interface
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
PDE	Product with Digital Elements
PSIRT	Product Security Incident Response Team
RF	Radio Frequency
RNG	Random Number Generator
SAM	Secure Access Module
SBOM	Software Bill of Materials
SESIP	Security Evaluation Standard for IoT Platforms
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
SWD	Serial Wire Debug
TRNG	True Random Number Generator
UID	Unique Identifier

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

7 References

1. 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 (Cyber Resilience Act), EUR-Lex (link)
2. Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 laying down technical descriptions of the categories of important and critical products with digital elements under Regulation (EU) 2024/2847, EUR-Lex (link)
3. NXP white paper - Security Primitives: Common Nomenclature to Describe Security Requirements in (I)IoT Systems (link)
4. Data sheet – PN7642: Single-chip solution with high-performance NFC reader, customizable MCU, and security toolbox (link)
5. Application note – AN13720 – PN7642 Secure Key Mode demo application (link)
6. Application note – AN14060 – How to use the PN76 family cryptographic features (link)
7. Application note – AN14540 – Firmware update on PN7642 (link)
8. Data sheet – PN5190B2: NFC Frontend (link)
9. Data sheet – PN7160/PN7161: Near Field Communication (NFC) controller (link)
10. Data sheet – PN7220: NFC controller with NCI interface supporting EMV and NFC Forum applications (link)
11. Short data sheet – PN76AC: NFC controller with NCI interface for Smart Access solution (link)
12. Data sheet – CLRC661 plus: High performance NFC frontend (link)
13. Data sheet – CLRC663 plus: High performance multi-protocol NFC frontend (link)
14. NXP Product Security Program / Product Security Incident Response Team (PSIRT) (link)
15. Web page – EdgeLock Assurance Program – Process and product security criteria (link)
16. Web page – IoT in 2026: Edge AI, growing complexity, and the demand for smarter updates (link)
17. Web page – Cybercrime Statistics Worldwide: The 2026 Global Picture (link)
18. Web page – Cyber Resilience Act, Classification Finder (link)

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

8 Revision history

Table 5. Revision history

Document ID	Release date	Description
AN15228 v.1.0	3 November 2026	Initial version.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

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.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

Licenses

Purchase of NXP ICs with NFC technology — Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

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.

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

Tables

Tab. 1. Examples of products with digital elements 5
Tab. 2. NXP EdgeVerse NFC Reader product CRA classification considerations 6
Tab. 3. Reader architecture and security responsibility split 7
Tab. 4. Abbreviations 15
Tab. 5. Revision history 17

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

Figures

Fig. 1. CRA products 5

All information provided in this document is subject to legal disclaimers.

© 2026 NXP B.V. All rights reserved.

Contents

1 Introduction 2
2 How to use this document 3
3 Cyber Resilience Act overview 4
3.1 Reader products and CRA category 5
4 Leveraging the NXP NFC reader portfolio to meet Cyber Resilience Act requirements 7
4.1 Reader architectures and security responsibility 7
4.2 Cyber Resilience Act 7
4.2.1 Annex I, Part I. Security requirements 7
4.2.1.1 Requirement (1): Secure manufacturing 8
4.2.1.2 Requirement (2): Cybersecurity requirements 8
4.2.1.3 a) be made available on the market without known exploitable vulnerabilities 8
4.2.1.4 b) be in a secure by default configuration and can reset the product to its original state 8
4.2.1.5 (c) ensure that vulnerabilities can be addressed through security updates 9
4.2.1.6 (d) protect against unauthorized access by using mechanisms such as authentication, identity, or access management systems and report possible unauthorized access 9
4.2.1.7 (e) protect the confidentiality of stored, transmitted, or otherwise processed data by, e.g., applying encryption to data at rest or in transit 10
4.2.1.8 (f) protect the integrity of stored, transmitted, or otherwise processed data, commands, programs, and configuration against unauthorized modification, and report on corruptions 10
4.2.1.9 (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”) 11
4.2.1.10 (h) protect the availability of essential and basic functions, and be resilient against and able to mitigate denial-of-service attacks 11
4.2.1.11 (i) minimize the negative impact of by-products on the availability of services of others 11
4.2.1.12 (j) be designed, developed, and produced to limit attack surfaces, including external interfaces 12
4.2.1.13 (k) be designed, developed, and produced to reduce the impact of an incident 12
4.2.1.14 (l) provide security-related information by recording and/or monitoring relevant internal activity, with an opt-out mechanism for the user 12
4.2.1.15 (m) provide the possibility for users to securely and easily purge all data and settings 13
4.2.2 Annex I, Part II. Vulnerability handling requirements 13
5 Beyond Annex I 14
5.1 Unique identification 14
5.2 Software bill of materials 14
5.3 Security of the supply chain 14
5.4 Manufacturer obligations on due diligence for integrated components 14
6 Abbreviations 15
7 References 16
8 Revision history 17
Legal information 18

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© 2026 NXP B.V. **All rights reserved.**