AN15177

Ease CRA compliance with EdgeLock 2GO

Rev. 1.0 — 8 September 2026 Application note

Document information

Information	Content
Keywords	CRA, EdgeLock 2GO, Industrial IoT
Abstract	This application note describes how NXP EdgeLock 2GO can support manufacturers in addressing cybersecurity requirements of the European Union Cyber Resilience Act (CRA). The document maps EdgeLock 2GO capabilities to the CRA Annex I Part I Section 2 requirements and provides guidance for referencing the service in cybersecurity risk assessments and technical documentation.

1 Introduction

The EU Cyber Resilience Act (CRA) requires manufacturers of products with digital elements to assess cybersecurity risks, implement appropriate controls, manage vulnerabilities throughout the product lifecycle, and maintain supporting technical documentation. For connected products, this includes demonstrating how device identity, secure provisioning, software integrity, update management, access control, monitoring, and incident response are addressed.

NXP EdgeLock 2GO supports CRA readiness by providing cloud-based security capabilities for connected devices. It helps customers manage device identities, cryptographic credentials, certificates, secure provisioning flows, code signing and encryption operations, OTA update campaigns, user access rights, project separation, and audit logs. These capabilities contribute to reducing risks such as device impersonation, credential compromise, insecure provisioning, unauthorized software installation, firmware manipulation, delayed vulnerability remediation, and lack of traceability.

EdgeLock 2GO is especially relevant to CRA Annex I Part I Section 2, where it can support secure-by-design, secure-by-default, lifecycle security, and auditability objectives. By enabling controlled provisioning, certificate-based authentication, credential lifecycle management, authenticated software signing, secure update orchestration, access governance, and operational logging, EdgeLock 2GO provides important building blocks for a CRA-aligned cybersecurity risk treatment plan.

EdgeLock 2GO does not replace the manufacturer’s own CRA cybersecurity risk assessment or conformity responsibilities. The manufacturer remains responsible for assessing the complete product, including hardware, embedded software, cloud services, applications, secure boot and device-side verification, vulnerability handling, SBOM management, user documentation, incident response, and product support obligations. EdgeLock 2GO should therefore be documented as a supporting security control within the broader product security architecture.

Customers can use this document to understand where EdgeLock 2GO contributes to CRA readiness, how to reference the service in their cybersecurity risk assessment, and how to map its capabilities to CRA Annex I Part I Section 2 requirements.

2 CRA

The European Union Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, establishes a horizontal cybersecurity framework for products with digital elements placed on the EU market. Its objective is to improve the cybersecurity of connected hardware and software products by ensuring that cybersecurity is considered from design and development through production, maintenance, vulnerability handling, and end of support. The CRA responds to the increasing dependence on connected products and to the security risks created when devices, applications, software components, or embedded systems are placed on the market without adequate protection or timely security updates.

The CRA applies broadly to “products with digital elements,” meaning hardware or software products whose intended or reasonably foreseeable use includes a direct or indirect data connection to a device or network. This includes many connected devices, embedded systems, IoT products, software applications, and components that may be integrated into other products. Some products are subject to specific sectoral legislation and may be excluded or treated differently, while products considered important or critical for cybersecurity may be subject to stricter conformity assessment requirements.

For manufacturers, the CRA introduces obligations before and after a product is placed on the market. Before market placement, manufacturers must perform a cybersecurity risk assessment, design and develop the product according to applicable essential cybersecurity requirements, prepare technical documentation, perform the relevant conformity assessment, issue an EU declaration of conformity, and affix the CE marking where applicable. The product must be designed with security-by-design and security-by-default principles, including appropriate controls for authentication, access management, data protection, software integrity, secure updates, logging, and reduction of attack surfaces.

After placing a product on the market, manufacturers must maintain cybersecurity throughout the indicated support period. This includes monitoring and addressing vulnerabilities, making security updates available, providing relevant information and instructions to users, and reporting actively exploited vulnerabilities and severe incidents affecting the security of the product. The CRA therefore moves cybersecurity from a one-time product design activity to an ongoing lifecycle responsibility that must be supported by processes, evidence, and operational controls.

The CRA main obligations apply from 11 December 2027, while vulnerability and incident reporting obligations apply earlier, from 11 September 2026. This transition period gives manufacturers time to assess product scope, define support periods, update development and vulnerability management processes, prepare technical documentation, and align product architectures with the essential cybersecurity requirements.

In this context, EdgeLock 2GO can be considered a supporting security service that helps manufacturers implement and operate selected CRA-relevant controls. Its capabilities for device identity, credential and certificate management, secure provisioning, code signing, OTA update management, access control, monitoring, and auditability can contribute to a manufacturer’s cybersecurity risk treatment plan. However, the manufacturer remains responsible for the complete product-level CRA assessment, implementation of all applicable requirements, conformity assessment, technical documentation, vulnerability handling, and declaration of conformity.

3 EdgeLock 2GO

EdgeLock 2GO is NXP's cloud-based security service for protecting connected devices across their lifecycle: during development, at manufacturing and provisioning, and after deployment in the field. The service helps device manufacturers centralize the management of device identities, cryptographic credentials, firmware signing keys, and secure update campaigns through a web portal and REST APIs.

For device manufacturers preparing for the EU Cyber Resilience Act (CRA), EdgeLock 2GO provides security capabilities that are directly relevant to the protection, provisioning, maintenance, and update of connected products. It helps reduce the complexity of implementing security controls by providing managed PKI and credential lifecycle management, secure device provisioning, code signing and encryption, OTA update orchestration, access control, monitoring, and audit-ready logs. EdgeLock 2GO can be used with any devices and provides extended security capabilities when used in conjunction with NXP devices.

3.1 PKI, key and certificate management

Public Key Infrastructure (PKI), keys, and certificates are foundational security elements for connected products. They enable device authentication, secure communication, protection of sensitive data in transit, and trusted interactions between devices, cloud services, mobile applications, and backend systems. Under the CRA, manufacturers are expected to design products with appropriate cybersecurity measures and to reduce the risk of unauthorized access, data compromise, impersonation, and manipulation.

EdgeLock 2GO supports centralized PKI and credential management for IoT devices. EdgeLock 2GO users can configure Certificate Authorities (CA), use an NXP-managed Root CA or link to an existing third-party Root CA, create intermediate CAs, define X.509 certificate templates, and issue device certificates. The service can also support ecosystem-specific certificate models, such as Matter or Qi wireless charging.

From a CRA perspective, managed PKI and credential lifecycle capabilities help manufacturers implement stronger device identity, encrypted communication, and controlled access to services. They also support operational security over time by enabling credential updates, revocation, and renewal processes. Centralized management and auditability are important because manufacturers must be able to demonstrate that security controls are consistently applied and maintained throughout the product lifecycle.

3.2 Device provisioning

Device provisioning is the process of securely installing the initial credentials, keys, certificates, software configuration, and security material required for a device to operate as a trusted product. This step is critical because the security posture of a connected product is often established during manufacturing or first commissioning. Weak provisioning processes can expose secrets, allow device cloning, create inconsistent configurations, or leave products without a reliable identity.

EdgeLock 2GO provides several provisioning options to support different manufacturing and deployment models. Devices can be provisioned at manufacturing through REST APIs or programming stations, provisioned in the field through a device connection over TLS, or supported through programming partners.

From a CRA perspective, secure provisioning helps ensure that every device leaves manufacturing with the intended security configuration and a unique, trusted identity. This contributes to protection against unauthorized access, product cloning, and uncontrolled production. Provisioning records, monitoring, and audit logs can also help manufacturers provide evidence that security measures were applied consistently across production batches and device groups.

3.3 Code signing

Code signing is a key mechanism for protecting firmware and software integrity. It allows a device or system to verify that software originates from an authorized source and has not been modified before installation or

execution. This is especially important for connected products because attackers frequently attempt to install modified firmware, exploit update mechanisms, or bypass secure boot and software verification controls.

EdgeLock 2GO provides secure code signing and encryption capabilities using managed keysets. EdgeLock 2GO users can configure production or test keysets, use signing and encryption keys, integrate signing operations into build pipelines through REST APIs, and control access to signing operations with permissions and API keys. Signing events are logged to support traceability and compliance evidence. The service supports strong cryptography and is designed to evolve with future cryptographic requirements.

From a CRA perspective, code signing helps manufacturers demonstrate that only authenticated and authorized software can be deployed to a product. It supports secure-by-design principles by protecting the integrity of firmware, applications, data packages, and other software assets. When combined with secure boot and device-side verification, code signing reduces the risk of malicious software installation and strengthens the manufacturer's ability to maintain product security throughout the lifecycle.

3.4 OTA update

Over-the-air (OTA) update capability is essential for maintaining the cybersecurity of connected products after they are placed on the market. Vulnerabilities may be discovered after deployment, cryptographic requirements may evolve, and manufacturers may need to deliver security fixes or configuration updates across large device fleets. The CRA emphasizes the need to manage vulnerabilities and provide security updates during the product support period.

EdgeLock 2GO supports secure OTA update management by allowing manufacturers to organize devices into groups, upload firmware or other update packages, define rollout strategies, and monitor deployment status. Update campaigns can be controlled using rules such as start and end dates, limits on the number of devices updated, update rate limits, and device properties. Devices or local servers can authenticate to the service, retrieve applicable packages, and report status information. The OTA update capability is not limited to firmware and can also support other updateable assets such as data or AI models, depending on the device implementation.

From a CRA perspective, OTA update management helps manufacturers maintain products securely after deployment. It supports the ability to distribute authenticated updates, fix vulnerabilities in the field, stage rollouts to reduce operational risk, and monitor whether updates have been successfully deployed. Combined with code signing and device authentication, OTA update capability provides an important foundation for vulnerability remediation, lifecycle security, and audit-ready evidence of maintenance activities.

3.5 Other features important for CRA

3.5.1 Audit logs and event traceability

EdgeLock 2GO records security-relevant events to help device manufacturers monitor activity, investigate changes, and maintain evidence of how security controls are applied over time. Audit logs can support traceability for actions such as provisioning, certificate issuance, signing operations, update campaign management, and user administration.

- Provides visibility into security-sensitive operations and administrative actions.
- Helps manufacturers demonstrate that security processes are controlled and consistently executed.
- Supports incident investigation, compliance evidence collection, and lifecycle security governance.

3.5.2 Separation of users, roles, and projects

EdgeLock 2GO helps device manufacturers organize security operations by separating users, roles, and projects. This separation supports a clearer governance model, where users only receive access to the projects and functions required for their responsibilities. It also helps reduce the risk of unintended changes,

unauthorized access, or accidental misuse of sensitive security functions such as provisioning, certificate management, code signing, and OTA update management.

From a CRA perspective, this capability supports controlled access to cybersecurity-related functions and helps manufacturers demonstrate that security operations are managed through defined responsibilities and access boundaries. Project separation is especially useful when different product lines, customer programs, manufacturing flows, or development environments must be managed independently.

Key benefits include:

- Limiting access to sensitive security functions based on user responsibilities.
- Separating production, test, and development environments to reduce operational risk.
- Supporting governance across multiple products, customers, or manufacturing programs.
- Helping manufacturers demonstrate controlled administration of cybersecurity-relevant processes.
- Reducing the risk that an incorrect configuration, certificate, signing key, or update campaign is applied to the wrong device population.

4 Using EdgeLock 2GO in CRA cybersecurity risk assessment and documentation

The CRA requires manufacturers to ensure that products are designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I of CRA.

In particular, manufacturers shall undertake an assessment of the cybersecurity risks associated with their product and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with a view to minimizing cybersecurity risks, preventing incidents and minimizing their impact.

That cybersecurity risk assessment shall be documented and comprise an analysis of cybersecurity risks based on the intended purpose of the product. It shall indicate whether and how the security requirements are applicable to the product and how those requirements are implemented.

The section “CRA Annex I Part I Section 2 mapping to EdgeLock 2GO” explains how EdgeLock 2GO can contribute to the cybersecurity risk management to implement the security requirements of CRA.

Note: *The document “EdgeLock 2GO Security Architecture Overview” details the security controls implemented by EdgeLock 2GO. You can use or refer to this document as evidence of the security mechanisms involved for minimizing the cybersecurity risks associated with your product. This document can be found in your EdgeLock 2GO account.*

4.1 CRA Annex I Part I Section 2 mapping to EdgeLock 2GO

The following sections map each requirement of CRA Annex I Part I Section 2 to the way EdgeLock 2GO can contribute to the manufacturer’s cybersecurity risk management. This mapping is intended as supporting guidance only. The manufacturer remains responsible for the complete product-level CRA assessment, implementation, verification, technical documentation, and declaration of conformity.

2(a) Products with digital elements shall be made available on the market without known exploitable vulnerabilities.

EdgeLock 2GO does not replace the manufacturer’s vulnerability assessment for the complete product. However, it supports secure lifecycle management by enabling controlled provisioning, managed credentials, code signing, OTA update campaigns, access governance, and audit logs. These capabilities help customers reduce the likelihood that products are released with weak identity, uncontrolled credentials, unsigned software, or unmanaged update mechanisms.

2(b) Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.

EdgeLock 2GO helps manufacturers define and apply secure provisioning profiles, certificate templates, device identities, and project-level configurations. By using controlled provisioning flows and separating production, test, and development environments, customers can reduce the risk of insecure default credentials, inconsistent device identity configuration, or accidental use of test material in production. The final secure-by-default product configuration and reset behavior remain the responsibility of the manufacturer.

Device manufacturers using the EdgeLock 2GO service for provisioning their devices can use such statement in their CRA documentation:

The product uses NXP EdgeLock 2GO to support controlled provisioning of device identities, certificates, credentials, and security configuration. This helps reduce the risk of insecure default credentials, inconsistent device identity configuration, or accidental use of test material in production. Details about the EdgeLock 2GO service can be found in the document "EdgeLock 2GO Security Architecture Overview".

2(c) Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.

EdgeLock 2GO contributes through secure OTA update management. Device manufacturers can create update campaigns, target device groups, control rollout timing, limit update rates, monitor deployment status, and distribute firmware or other update packages. When combined with code signing and device-side update verification, this helps manufacturers deliver authenticated updates and remediate vulnerabilities after deployment. User notification, opt-out, postponement behavior, update installation logic, and device-side enforcement must be implemented by the manufacturer.

Device manufacturers using the EdgeLock 2GO OTA Update service can use such statement in their CRA documentation:

The product uses the NXP EdgeLock 2GO service for delivering software updates to the devices over-the-air. The communication between the devices and the update server is protected through TLS with mutual authentication. Details about the EdgeLock 2GO service can be found in the document "EdgeLock 2GO Security Architecture Overview".

2(d) Products with digital elements shall ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.

EdgeLock 2GO supports protection from unauthorized access by enabling unique device identities, certificate-based authentication, credential lifecycle management, role-based user access, API key management, and project separation. These capabilities help ensure that only authorized devices, users, and systems can access relevant security functions. Audit logs and event records can support investigation and reporting of security-relevant activity. Product-level access control, runtime authorization, and user-facing reporting remain customer responsibilities.

Device manufacturers using the EdgeLock 2GO service for provisioning the devices can use such statement in their CRA documentation:

The product uses NXP EdgeLock 2GO to install device identities, certificates and credentials into the product. Details about the EdgeLock 2GO service can be found in the document "EdgeLock 2GO Security Architecture Overview".

2(e) Products with digital elements shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means.

EdgeLock 2GO contributes by supporting certificate-based authentication, secure credential provisioning, and cryptographic material management that can be used to establish trusted and encrypted communication channels. It can help manufacturers provision device certificates and keys needed for TLS or other secure communication mechanisms. Confidentiality of data stored or processed on the device, in customer applications, or in customer backend systems remains the responsibility of the manufacturer and system operator.

Device manufacturers using the EdgeLock 2GO service for provisioning client certificates on the devices can use such statement in their CRA documentation:

The product uses TLS client certificates provisioned through NXP EdgeLock 2GO to establish mutually authenticated and encrypted communication channels. Details about the EdgeLock 2GO service can be found in the document "EdgeLock 2GO Security Architecture Overview".

2(f) Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions.

EdgeLock 2GO contributes to software and data integrity through code signing and encryption capabilities, secure provisioning of credentials, authenticated update distribution, and auditability of signing and update operations. Manufacturers can use EdgeLock 2GO to sign firmware, applications, configuration packages, or other updateable assets, then rely on device-side verification to detect unauthorized modification. Device-side integrity checks, secure boot, corruption reporting, and runtime protection remain customer responsibilities.

Device manufacturers using the EdgeLock 2GO code signing service can use such statement in their CRA documentation:

The product uses NXP EdgeLock 2GO to sign the firmware of the device. The product verifies the signature before installation or execution to help prevent unauthorized or modified software from being deployed. Details about the EdgeLock 2GO service can be found in the document "EdgeLock 2GO Security Architecture Overview".

2(g) Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements.

EdgeLock 2GO can support data minimization by enabling customers to define the security credentials, certificate attributes, device metadata, and operational data needed for provisioning and lifecycle management. The manufacturer should configure the service to provision only the data required for the intended security functions. The broader product data model, application telemetry, personal data handling, and privacy documentation remain the responsibility of the manufacturer.

2(h) Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.

EdgeLock 2GO supports availability-related risk treatment by enabling controlled update rollout, campaign monitoring, device grouping, rate limiting, and lifecycle management of credentials and updates. These capabilities can reduce operational disruption when deploying security fixes or recovering from incidents. Availability of the complete product, device fallback behavior, local resilience, denial-of-service protection, and continuity measures remain the responsibility of the manufacturer and system operator.

2(i) Products with digital elements shall minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks.

EdgeLock 2GO can help reduce negative operational impact by supporting staged OTA deployments, update rate limits, device grouping, and controlled campaign execution. These mechanisms help avoid uncontrolled update storms or simultaneous device behavior that could overload backend systems or networks. The manufacturer remains responsible for device behavior, network usage, retry logic, traffic shaping, and ensuring that the product does not adversely affect other devices or services.

2(j) Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces.

EdgeLock 2GO contributes by centralizing selected security operations, reducing the need for customers to build and expose custom provisioning, credential management, signing, or update-management infrastructure. Role-based access control, project separation, API credential management, and managed security workflows can help reduce unnecessary operational interfaces. The manufacturer remains responsible for limiting the product’s own device, application, cloud, API, debug, and maintenance interfaces.

Device manufacturers using the EdgeLock 2GO service can use such statement in their CRA documentation:

The product uses NXP EdgeLock 2GO as a managed service for selected security lifecycle functions, including provisioning, certificate management, code signing, and OTA update management. This reduces the need for the manufacturer to build and expose custom infrastructure for these functions. Details about the EdgeLock 2GO service can be found in the document "EdgeLock 2GO Security Architecture Overview".

2(k) Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.

EdgeLock 2GO helps reduce the impact of incidents by supporting credential lifecycle operations, controlled update campaigns, code signing, project separation, access governance, and audit logs. These capabilities can help manufacturers revoke or rotate credentials, deploy fixes, separate affected projects or product lines, and investigate security-relevant actions. Device-side exploit mitigation, containment, recovery behavior, and incident response processes remain customer responsibilities.

2(l) Products with digital elements shall provide security-related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.

EdgeLock 2GO records security-relevant events related to provisioning, certificate management, signing operations, update campaigns, user administration, and other operational activities. These logs can support traceability, compliance evidence, and incident investigation. Internal product telemetry, device-side logging, user opt-out behavior, retention policy, and customer-facing reporting remain the responsibility of the manufacturer.

Device manufacturers using the EdgeLock 2GO service can use such statement in their CRA documentation:

The product uses NXP EdgeLock 2GO to record security-relevant events related to provisioning, certificate management, signing operations, OTA update campaigns, user administration, and API usage. These logs can support traceability, compliance evidence, and incident investigation. Details about the EdgeLock 2GO service can be found in the document "EdgeLock 2GO Security Architecture Overview".

2(m) Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

EdgeLock 2GO may support lifecycle operations related to credentials, device records, projects, and security material managed in the service. However, secure deletion of user data, product settings, local credentials, application data, and transferable data on the device or in customer systems remains primarily the responsibility of the manufacturer. Manufacturers should document how EdgeLock 2GO-managed credentials and device identities are handled during decommissioning, reset, ownership transfer, or product end-of-life.

4.2 EdgeLock 2GO Security Architecture Overview

The document "EdgeLock 2GO Security Architecture Overview" describes the security architecture and security controls of EdgeLock 2GO for protecting the different assets. You can use or refer to this document as evidence of the security mechanisms in place for minimizing the cybersecurity risks associated with your product.

This document can be found in your EdgeLock 2GO account.

5 Revision history

Table 1. Revision history

Document ID	Release date	Description
AN15177 v.1.0	8 September 2026	• 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.

Tables

Contents