AN14544

EdgeLock 2GO Services for MPU and MCU

Rev. 1.1 — 27 March 2025 Application note

Document information

Information	Content
Keywords	AN14544, EdgeLock 2Go, EdgeLock, security, secure provisioning, i.MX, i.MX RT, MCX
Abstract	This application note introduces various methods that the EdgeLock 2GO service can be used with MCU and MPU devices and the features available for each method.

1 Introduction

EdgeLock 2GO is the service platform of NXP for provisioning and managing IoT devices. It lets you securely install keys and certificates into your devices, either during manufacturing or in the field, and then keep credentials up to date during the device life cycle. EdgeLock 2GO uses the security capability of each device, for optimal levels of security across your entire IoT fleet.

The service has been available for secure elements for years and is rolling out to NXP processors and microcontrollers that contain an EdgeLock secure enclave. This includes devices in the i.MX, i.MX RT, MCX, and wireless connectivity families.

This application note introduces various methods that the EdgeLock 2GO service can be used with MCU and MPU devices and the features available for each method.

2 EdgeLock 2GO introduction

EdgeLock 2GO is a fully managed cloud platform operated by NXP, which provides secure provisioning services for easy deployment and maintenance of IoT devices using supported NXP products. The service allows you to create and manage secure objects, such as symmetric keys, key-pairs and certificates, which are then securely provisioned into your NXP MCU or MPU.

Secure objects and certificates created through EdgeLock 2GO can be used for a wide variety of use cases, including secure cloud onboarding of IoT devices to your preferred cloud service (for example, AWS IoT Core or Azure IoT Hub), data encryption or decryption, and access control.

EdgeLock 2GO abstracts the complexity of key and certificate management so you do not need to invest in a PKI infrastructure. The security of EdgeLock 2GO relies on roots of trust that are injected into the device during their manufacturing and then uploaded to the platform. These roots of trust allow EdgeLock 2GO to customize the devices and provision them with your device-specific certificates and keys. The whole process is encrypted end-to-end from the service directly into the device, so special security on the production line is not required to handle the credentials.

3 EdgeLock 2GO provisioning methods

EdgeLock 2GO is a flexible service that can be used in different ways depending on your provisioning needs and where the provisioning occurs. Figure 1 shows the high-level EdgeLock 2GO provisioning method/flow options that are available for NXP MCUs and MPUs.

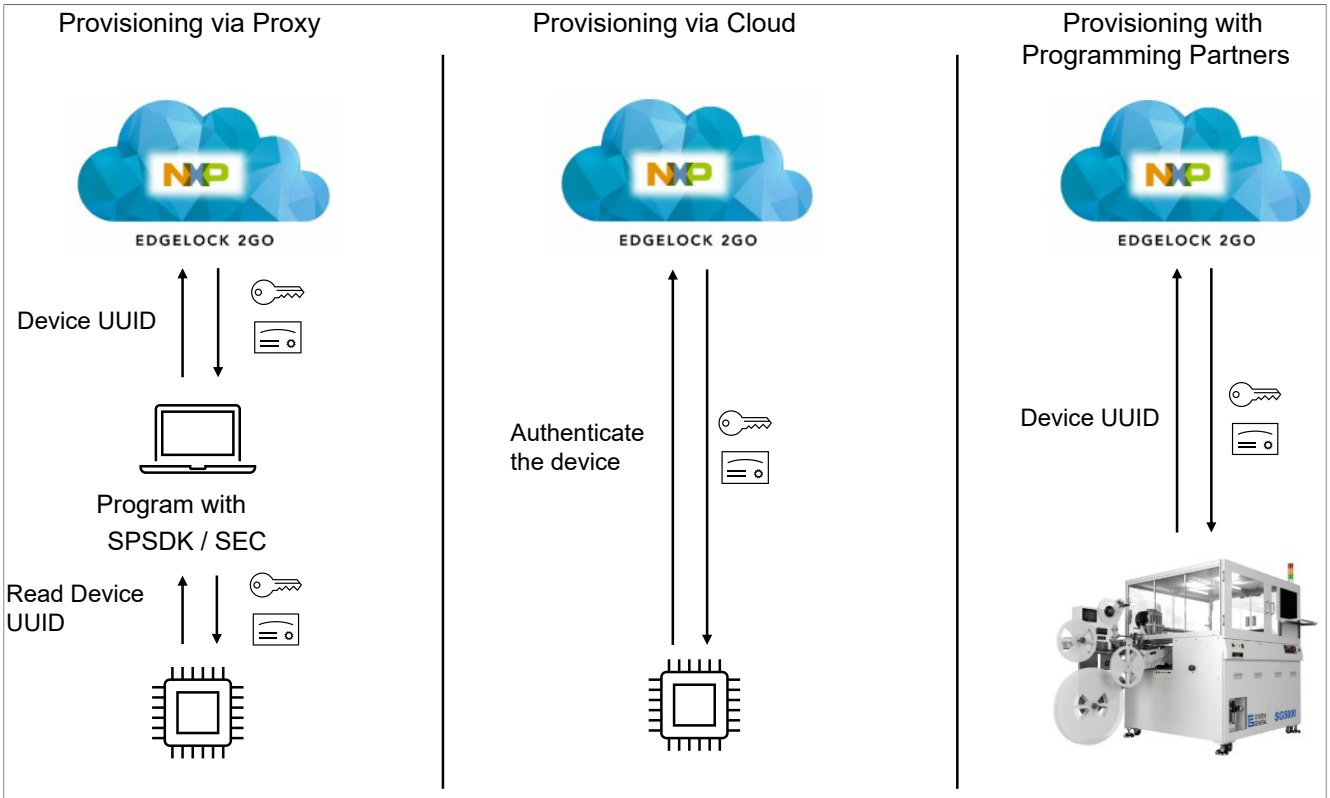

Figure 1. EdgeLock 2GO provisioning flows

- Provisioning via Proxy flow – A host running SPSDK/SEC tools is used to facilitate provisioning.
- Provisioning via Cloud flow – A device communicates directly with the EdgeLock 2GO server using a TLS stack.
- Provisioning with Programming Partners flow – A programming partner uses EdgeLock 2GO to provision devices before they are sent to manufacturing.

The flows supported vary with devices. Check EdgeLock 2GO supported products for a list of supported devices including the flows supported for each.

You don't need to select a single flow. Multiple EdgeLock 2GO flows can be used together. For example, the Provisioning via Proxy flow could be used for initial device provisioning at manufacturing, and then later the Provisioning via Cloud flow could be used to add, update, or rotate keys while the device is deployed in the field. EdgeLock 2GO can also be used alongside other trust provisioning methods, such as the Device HSM provisioning available on many NXP MCUs.

3.1 Provisioning via Proxy flow

When using the Provisioning via Proxy flow, a host running SPSDK or SEC is used to facilitate provisioning. The secure objects to be provisioned are loaded from the EdgeLock 2GO server to the host. Then they are moved from the host to the device.

This flow is intended to be used for initial provisioning of the device during manufacturing and supports provisioning of device internal secure objects which are stored in fuses and/or flash implicit-protected flash region (IFR):

- OEM firmware authentication key hash (ROTKH/SRKH)
- OEM firmware decryption key (CUST_MK_SK/OTFAD keys)
- General configuration of the device using fuse/IFR (secure boot settings, device configuration, and so on)

- Advancement of device life cycle state

The Provisioning via Proxy flow also supports provisioning of external secure objects which are rewrapped and stored in flash for use by the application. External secure objects include any secure objects that are not stored in the fuses or IFR. Typically these are keys and certificates which have an application usage, but are not used by the device ROM. Examples of external secure objects are:

- Certificates and key pairs used for cloud on-boarding including intermediate certificates if needed
- Matter certificates and key pairs
- Data encryption/decryption key

3.1.1 Provisioning via Proxy flow steps

Figure 2 shows the steps used in the Provisioning via Proxy flow.

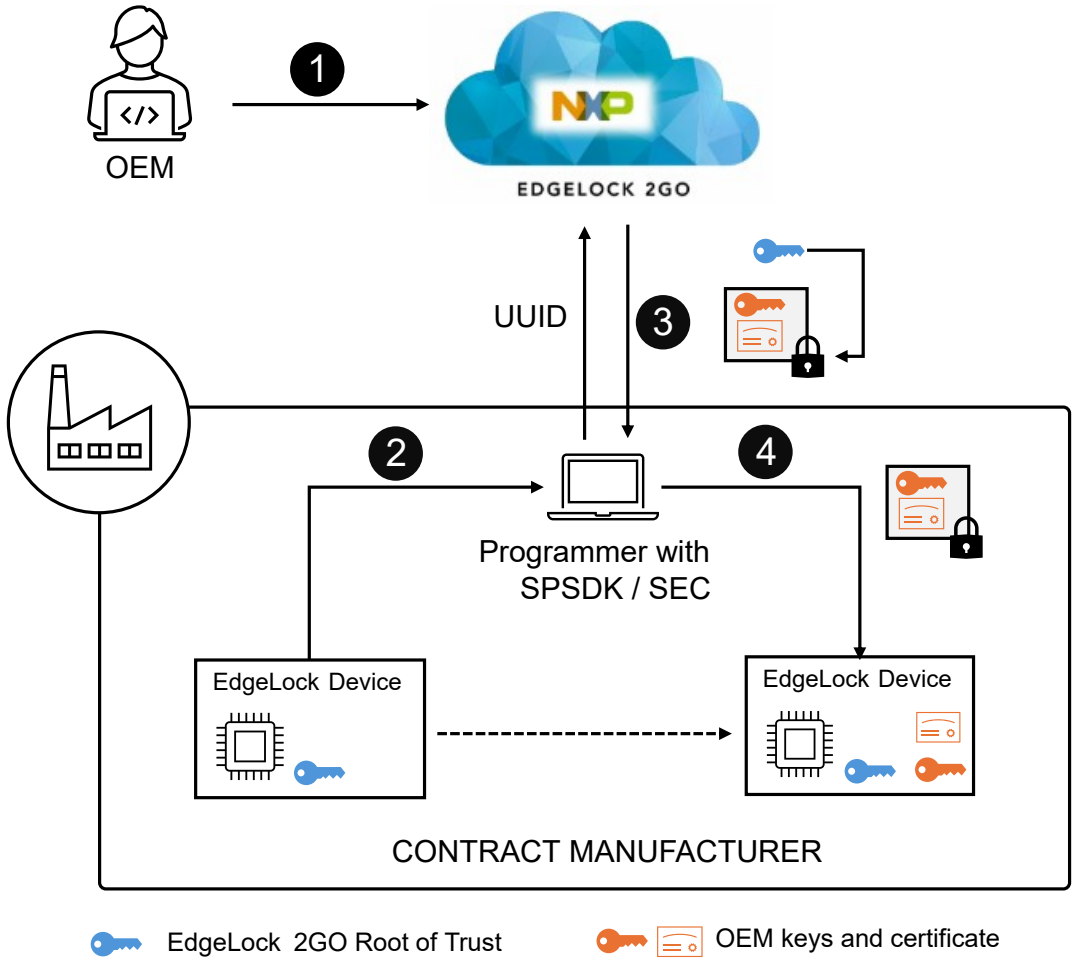

Figure 2. Provisioning via Proxy flow

1. OEM configures secure objects via the EdgeLock 2GO portal or API.
2. At device manufacturing, readout device UUIDs (one by one or by batch) and send the UUID or list of UUIDs to EdgeLock 2GO over API.
3. EdgeLock 2GO generates the secure objects configured in Step 1 and encrypts with EdgeLock 2GO root of trust. The encrypted secure objects are downloaded to the host.

4. The host loads the encrypted secure objects to the device where EdgeLock 2GO provisioning firmware passes the encrypted credentials to the EdgeLock secure enclave to unwrap them. Internal secure objects are installed into fuses/IFR. External secure objects are rewrapped and written to flash.

3.1.2 Why use Provisioning via Proxy flow?

Below lists some reasons to use the Provisioning via Proxy flow:

- Need to provision fuse/IFR keys (internal secure objects).
- Target-end product doesn't have direct Internet connectivity available.
- Manufacturing network topology makes direct connection of end product difficult and/or slow.

Keep in mind that the Provisioning via Proxy flow can be combined with other flows as needed. For example, the Provisioning via Cloud flow could be used by the application for in-field management.

3.2 Provisioning via Cloud flow

When using the Provisioning via Cloud flow, the target board communicates directly with the EdgeLock 2GO server over a TLS connection. The TLS channel can be using connectivity within the device (ex: on-chip Ethernet controller) or through an attached Ethernet or Wi-Fi controller included on the target board.

This flow can be used for provisioning of the device during manufacturing and/or in-field management of keys and certificates. The `el2go_agent` software provided by NXP can be used as a standalone project, typically used for manufacturing, and can also be integrated as part of the end application to provide in-the-field downloading and updating of keys.

The Provisioning via Cloud flow does not support provisioning of internal secure objects to be stored in fuses or IFR (ex: ROTKH/SRKH, secure boot settings, and life cycle). Another flow or trust provisioning method (ex: Provisioning via Proxy or Device HSM provisioning) can be used with the Provisioning via Cloud flow to support complete device provisioning.

The Provisioning via Cloud flow supports provisioning of external secure objects which are rewrapped by the EdgeLock secure enclave in the device and written to flash for long-term storage. The secure objects can be unwrapped by the secure enclave when the application uses them. External secure objects include any secure objects that are not stored in the fuses or flash IFR. Typically, these are keys which have an application usage, but are not used by the device ROM. Examples of external secure objects are:

- Certificates and key pairs used for cloud on-boarding including intermediate certificates if needed
- Matter certificates and key pairs
- Data encryption/decryption keys

3.2.1 Provisioning via Cloud flow steps

Figure 3 shows the steps used in the Provisioning via Cloud flow.

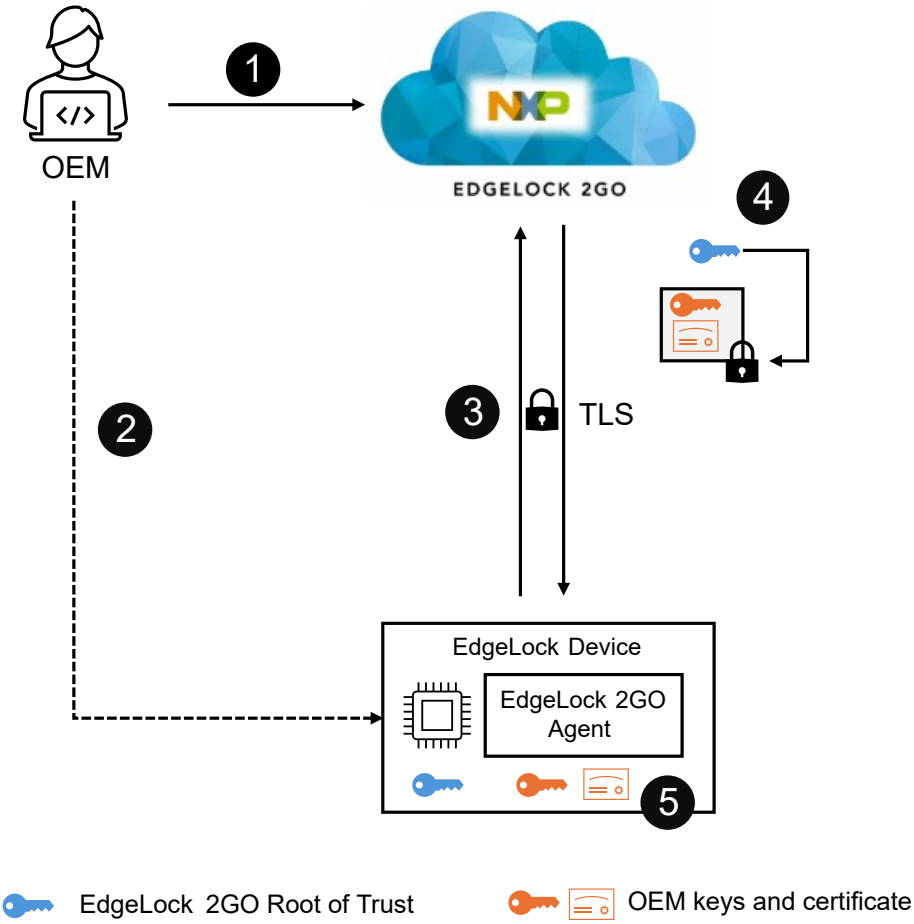

Figure 3. Provisioning via Cloud Flow

1. OEM configures secure objects via the EdgeLock 2GO portal or API.
2. **(Optional)** User administrator generates a claim code and installs the claim code on the devices (the same claim code is used on many devices).
3. On the device, the application calls the EdgeLock 2GO agent to connect to the EdgeLock 2GO server. The device is authenticated thanks to EdgeLock root of trust.
4. EdgeLock 2GO generates the secure objects configured in Step 1 and encrypts with EdgeLock 2GO root of trust. The encrypted secure objects are sent to the device through the TLS channel.
5. The EdgeLock 2GO Agent passes the encrypted secure objects to the EdgeLock secure enclave to rewrap them, and then writes them to flash.

3.2.2 Using claim codes

The Provisioning via Cloud flow supports using a claim code instead of the device UUID to validate a device. Claim codes allow for provisioning many devices without knowing the UUIDs ahead of time, but still having control and notifications of the total number of devices that get provisioned.

A claim code is a random base64-encoded string of 16 to 255 characters, which is generated for a particular device group on the EdgeLock 2GO server. Multiple devices use the same claim code to authenticate to the server, but the number of activations per claim code can be limited.

Figure 4 shows the steps used to add a device to a device group using a claim code.

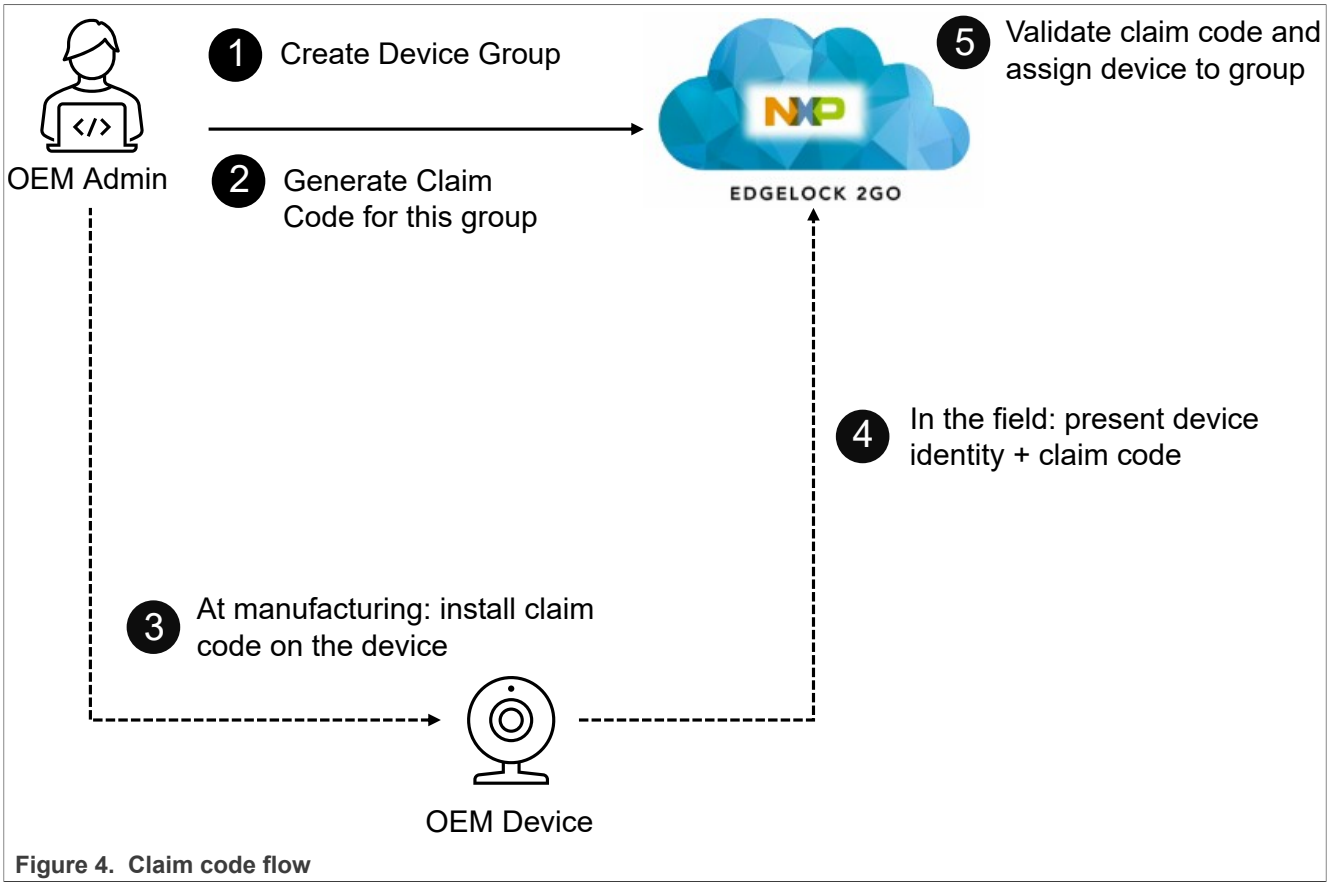

Figure 4. Claim code flow

1. Create a device group on the EdgeLock 2GO server.
2. Generate a claim code for this device group.
3. Load the claim code into the devices before deploying to the field.
4. The device sends its UUID and the claim code to the EdgeLock 2GO server.
5. EdgeLock 2GO server validates the claim code and assigns the device to the corresponding device group.

3.2.3 Why use Provisioning via Cloud flow?

Below lists some reasons to use the Provisioning via Cloud flow:

- In-field key management is required.
- Want to use claim codes instead of UUIDs.
- Need to monitor the provisioning state of each device. This can be seen in the EdgeLock 2GO server when Provisioning via Cloud is used.

Keep in mind that the Provisioning via Cloud flow can be combined with other flows as needed. For example, the Provisioning via Proxy flow could be used for initial provisioning.

3.3 Provisioning with Programming Partners flow

Our programming partners offer secure provisioning services based on the EdgeLock 2GO service for various devices including MCU and MPU products. Check the EdgeLock 2GO programming partners for the complete list of programming partners supporting EdgeLock 2GO provisioning.

The Provisioning with Programming Partners flow is used for pre-provisioning of devices before they are shipped to manufacturing. The flow supports provisioning of device internal secure objects which are stored in fuses and/or flash implicit-protected flash region (IFR):

- OEM firmware authentication key hash (ROTKH/SRKH)
- OEM firmware decryption key (CUST_MK_SK/OTFAD keys)
- General configuration of the device using fuse/IFR (secure boot settings, device configuration, and so on)
- Advancement of device life cycle state

For MCUs with internal flash, Provisioning with Programming Partners can also support provisioning of the application image and external secure objects which are rewrapped and stored in flash for use by the application. External secure objects include any secure objects that are not stored in the fuses or flash IFR. Typically, these are keys which have an application usage, but are not used by the device ROM. Examples of external secure objects are:

- Certificates and key pairs used for cloud on-boarding including intermediate certificates if needed
- Matter certificates and key pairs
- Data encryption/decryption key

3.3.1 Provisioning with Programming Partners flow steps

Figure 5 shows the steps used in the Provisioning with Programming Partners flow.

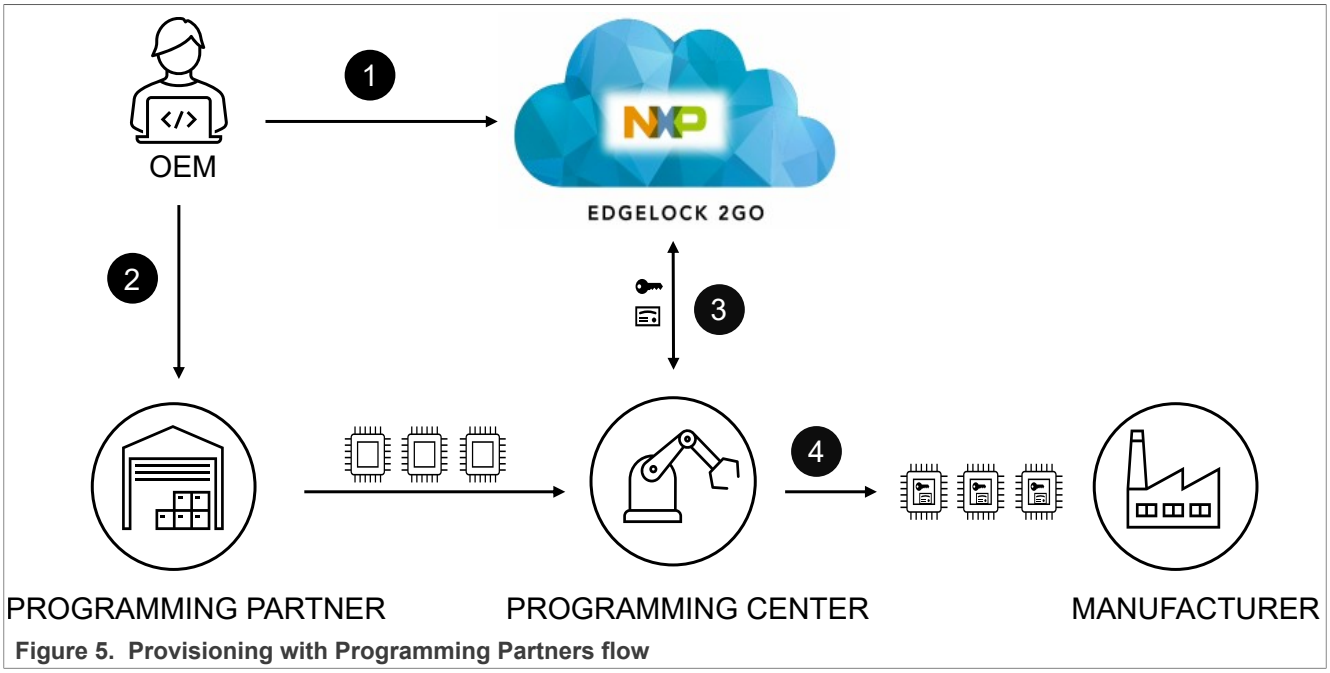

Figure 5. Provisioning with Programming Partners flow

1. OEM configures secure objects in their account via the EdgeLock 2GO portal or API and grants provisioning rights to the programming partner.
2. OEM orders parts and programming services from one of the NXP programming partners.
3. The programming center provisions devices as configured by the EdgeLock 2GO account of the OEM.
4. The programming center ships provisioned parts to the manufacturing site.

3.3.2 Why use Provisioning with Programming Partners flow?

Some of the reasons to use the Provisioning with Programming Partners flow are listed below:

- Manufacturing time is reduced by using pre-provisioned/pre-programmed devices.
- Limited network connectivity available at manufacturer.

Keep in mind that the Provisioning with Programming Partners flow can be combined with other flows as needed. For example, the Provisioning via Cloud flow is used by the application for in-field management after a programming center does initial provisioning.

4 Summary

Table 1 provides a summary of all the EdgeLock 2GO flows supported for MCU and MPU devices and lists the features available for each flow.

Table 1. EdgeLock 2GO Feature Summary

Feature	Provisioning via Proxy flow	Provisioning via Cloud flow	Provisioning with Programming Partners flow
Internal object provisioning (device keys, configuration, and life cycle)	✓	×	✓
External object provisioning (application keys and certificates)	✓	✓	✓ [1]
Over-production control	✓	✓	✓
Supports claim codes	×	✓	×
In-the-field key management	×	✓	×
Device unique certificate generation	✓	✓	✓
Counterfeit chip detection	✓	✓	✓
Application provisioning	×	×	✓ [1]

[1] Only supported for devices with on-chip flash.

5 Resources

- EdgeLock 2GO landing page – Overview of service, supported products, documentation, and design resources
- EdgeLock 2GO Access Request – Form to request access to EdgeLock 2GO service platform for evaluation
- EdgeLock 2GO documentation – Developer guides and application notes hosted on the EdgeLock 2GO server. Requires EdgeLock 2GO service platform access (see access request form above).

6 Revision history

Table 2 summarizes the revisions to this document.

Table 2. Revision history

Document ID	Release date	Description
AN14544 v1.1	27 March 2025	Update all images
AN14544 v1.0	22 January 2025	Initial public release

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.

Contents