IoT service platform for secure, flexible device management

Designed for easy, secure deployment and management devices in the Internet of Things (IoT), this service platform lets you choose the options, so you can optimize costs while benefiting from advanced levels of device security.

To protect data, ensure privacy, and prevent cyberattacks, IoT devices are increasingly required to use authentication, based on keys and certificates. NXP's EdgeLock 2GO cloud service gives device OEMs a secure, simple, and flexible way to provision and manage device credentials, over the entire device lifecycle and, because NXP is fully authorized to provide certificates for standards such as Matter or Qi Wireless Charging, EdgeLock 2GO saves time when pursuing device certification.

Key Features

- Highly flexible approach to IoT security
- Provisioning services for credential injection and maintenance
- Secure key injection leverages device's hardware capabilities
- Approved Product Attestation Authority (PAA) for Matter device certificates

Key Benefits

Security

- Deliver end-to-end security from chip to cloud, based on a certified Trust Anchor
- Manage security independent of device manufacturing and supply chain
- Protect the entire device lifecycle, from day one of deployment

Flexibility

- Tailor the options for every type of IoT device roll-out
- Support every type of IoT device, from sensor to edge-computing platform
- Accelerate time-to-market with late-stage device configuration in the field

Ease of use

- Zero-touch onboarding of devices into the cloud
- Simplified maintenance of credentials during device lifetime
- Easy management of even large fleets of IoT devices

Approved for Matter

- Approved PAA for Matter device certificates

- Secure injection of device attestation keys into silicon

- Flexible options for delivery of device attestation certificates

NXP's EdgeLock 2GO service saves device OEMs from having to establish and maintain an infrastructure for device provisioning, which is an expensive and complex undertaking. For OEMs deploying devices certified for Matter or Qi Wireless Charging, the undertaking is especially challenging, since becoming a Matter- or Qi-certified provider of attestation certificates is an even more ambitious undertaking. What's more, enabling the infrastructure to support ongoing credential management and secure updates adds to the expensive of device provisioning, and increases the complexity of maintaining a secure deployment.
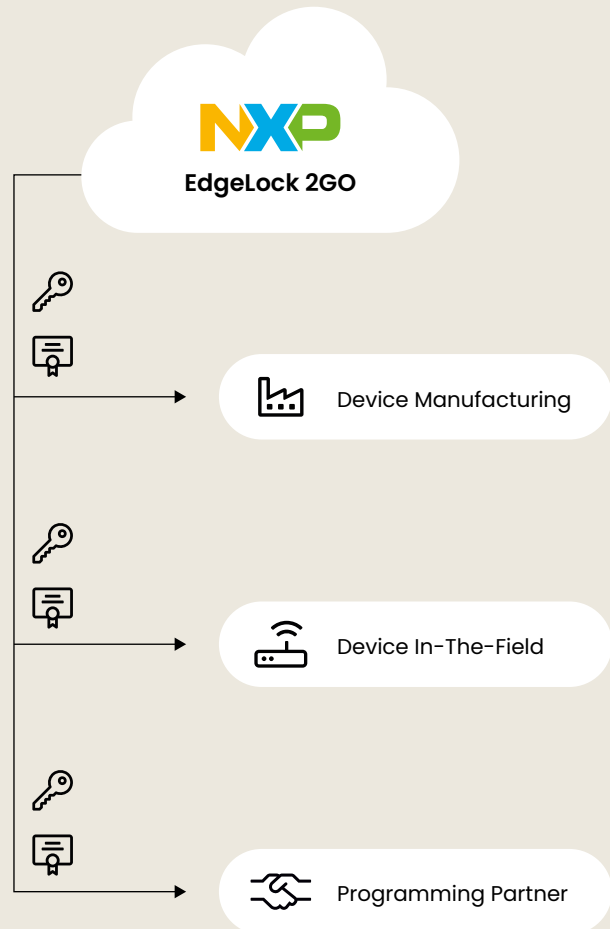
A Simpler Way to Manage Credentials

Device OEMs can sidestep all these issues by using NXP's turnkey EdgeLock 2GO service for credential management. NXP is a recognized leader in IoT security and one of the few semiconductor manufacturers that not only provides comprehensive device provisioning for a wide range of IoT use cases, but is also a fully authorized provider of certificates for Matter and Qi. Our EdgeLock 2GO cloud service gives device OEMs a secure, simple, and flexible way to provision and manage device credentials, over the entire lifecycle of the device, from manufacturing to deployment and retirement.

EdgeLock 2GO is secure, in that it provides end-to-end protection with NXP's security infrastructure and hardware-based root of device, and it's simple, in that device OEMs aren't forced to create a security infrastructure for their manufacturing sites. EdgeLock 2GO is also flexible, in that it's compatible with PKI and IoT services, and is fully approved for popular standards, including Matter and Qi.

Three Ways to Provision Trust

To maximize flexibility and reduce time-to-market, EdgeLock 2GO offers three ways to perform trust provisioning:

1. **At device manufacturing** – At the point of manufacture, EdgeLock 2GO lets OEMs securely provision devices with keys and certificates, with different configurations for different products, and is set up to safely include contract manufacturers in the process.

2. **In the field** – EdgeLock 2GO can also be used to provision devices in the field, with credentials provided at commissioning, and can be used to add, update, and revoke credentials throughout the device's time in the field.

3. **Through a Programming Partner** – Device manufacturers can request one of NXP-selected partners to securely provision secure elements, secure authenticators, and compatible MCU products with certificate authorities and device credentials secured with NXP EdgeLock 2GO. Device manufacturers receive parts that are already provisioned and ready to use.

EdgeLock 2GO

Device Manufacturing

Device In-The-Field

Programming Partner

Features

Certificate Authority	• Configure the Certificate Authority for your devices • Link to your Root CA of choice or use NXP Root CA • Use NXP-approved root for Matter and Qi Wireless Charging

Device Key Pairs	• RSA 1024- to 409-bit
	• ECC keys different curves including
	  – ECC NIST (192- to 521-bit)
	  – Brainpool (160- to 512- bit)
	  – Twisted Edwards Ed25519
	  – Montgomery Curve25519
	  – Koblitz (192- to 256-bit)

X.509 Certificates	• Select the Certificate Authority for your devices • Customize device-certificate fields (common name, validity period, key usage, etc.)
Other Keys and Data Provisioning	• Firmware verification and decryption keys • AES-128 and AES-256 keys • HMAC key • Public keys and certificates • Sensitive or non-sensitive binary data (hashes of host software, passwords, etc.)
Web Portal for Setup and Monitoring	• Use the EdgeLock 2GO web portal to configure product credentials • Monitor device provisioning • Define limits and alerts to protect against overproduction
REST API for Automation	• Automatically configure new credentials for new projects • Automate the provisioning and monitoring of your devices

Visit nxp.com/EdgeLock2GO