Nexus GO IoT

Nexus GO IoT is a service for issuing and managing PKI certificates for secure identification of IoT devices. It’s easy to get started with the Nexus GO IoT service, and it can be used for different types of certificates for your IoT devices, such as factory certificates and operative certificates. You can access the service using standard protocols. Nexus GO IoT is based on best practices and long-time expertise in delivering PKI.

Secure your IoT devices with certificates

Today many IoT devices on the market, even still being released, are only protected with passwords or shared keys. A certificate is more than just an identity for your device, it can be used for all types of TLS based communications like HTTPS and MQTT.

PKI certificates enable authenticated and encrypted device-to-cloud and device-to-device communication, to secure the supply chain against product forgery and provide for secure enrollment and provisioning of devices. Public key infrastructure (PKI) certificates are the best available technology to use in Internet of Things (IoT) devices for security. Thereby, integrity, safety and privacy are maintained during the device lifecycle.

Get started quickly with a trial version

It’s straightforward to use PKI certificates in IoT applications, since PKI certificates are supported by most communication protocols, authentication and access products, and digital services. Most of the operating systems and libraries that are used in IoT devices today also have support for certificates, so it’s easy to start using certificates from the Nexus GO IoT Service.

Setting up your IoT application and devices for managing and using PKI certificates demands careful planning and implementation work. During this period, you can sign up to the Nexus GO IoT trial version to quickly get started and test the service with your IoT application.

The trial version helps you develop and verify the certificate provisioning and the PKI-based security functions. The certificate content can be adjusted and verified before devices are marketed and productively deployed. For more information, see Get started with Nexus GO IoT.

Grow with your IoT deployment

The Nexus GO IoT Service is a high performance service that allows you to grow with your IoT deployment. You also get access to the Nexus experts with extensive experience in large scale PKI deployments.

Manage the whole lifecycle

The Nexus GO IoT Service can help you with all your certificate related needs for your IoT deployment. We can provide different types of certificates through a broad range of protocols for better automation.
• **Factory certificate – Birth certificate**
  When devices are produced, they can be equipped with a so called factory certificate or birth certificate. This certificate will be valid for the whole lifecycle of the device, and is the base for issuing other certificates. Factory certificates are requested by the manufacturing system. A REST API is provided for easy integration.

• **Lifecycle certificates – Device to CA**
  To reflect the change of state or ownership of the device, the device itself can request a so called operative certificate when it’s deployed. Depending on the device type, different protocols can be used for certificate request. EST or EST-coaps is recommended for constrained devices.

• **Lifecycle certificates – Device to Platform to CA**
  In some cases you want the IoT platform to request the operative certificate for the device. Use the provided REST API and plug in to your industrial eco-system.

• **Revocation**
  The certificates can be revoked through our REST API, so you can integrate this in your IoT backend. Revocation status is available both as CRLs and with OCSP (Online Certificate Status Protocol).

• **Registration – Approval**
  You can preregister your devices in the service, so only the valid devices can request certificates.

**Protect keys with a Hardware Security Module (HSM)**

As standard your CA keys will be stored in a shared HSM (Hardware Security Module) environment, which gives your keys both logical and physical high-level protection. We can also offer the option to store your CA keys in a dedicated HSM, allowing easy migration.

**Support standard protocols, algorithms and certificate formats**

The certificate enrollment can be done directly from the device using our broad support for standard protocols.

An easy-to-integrate REST API is also provided for device registration, certificate issuing, renewal and revocation to be integrated from your IoT platform. The REST API is available as an OpenAPI (Swagger) for easy back end implementation.

**Specification**

**Certificate Enrollment Protocols:**

- EST – Enrollment over Secure Transport, RFC 7030
- EST-coaps – EST over coaps, IETF draft
- ACME – Automatic Certificate Management Environment, RFC 8555
- SCEP - Simple Certificate Enrollment Protocol, draft-nourse-scep-23
- CMC - Certificate Management over CMS, RFC 5273

**Certificate formats:**


**Algorithms and key types:**

- CA signatures: RSA, RSASSA-PSS, DSA
  Key lengths as supported by HSM (e.g. RSA 1024 - 16384 bit), Algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RipeMD-160.
- CA signatures: EC, Prime field based ECDSA algorithms with named curves as supported by HSM, hash functions as above.
- End user keys: RSA, 1024-4096 bits (soft tokens and on smart card/token type).
- End user keys: EC, Prime field based ECDSA algorithms with arbitrary curve parameters (only on smart cards). Certificates for ECDSA keys can be requested only via CM SDK.