Product summary

Certificate lifecycle control

Easily manage device certificates for an IoT lifetime

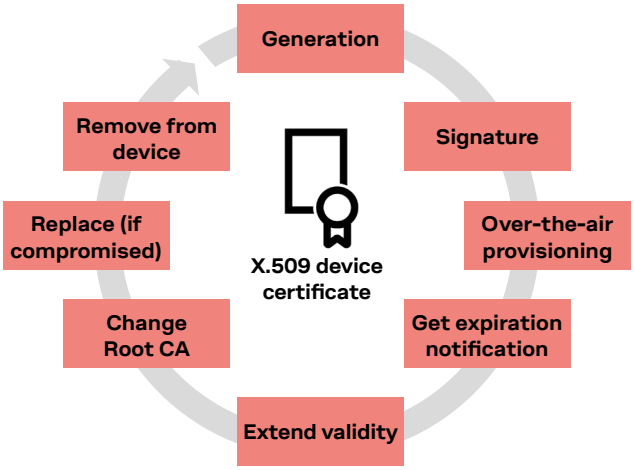
Out-of-the-box on-boarding to IoT cloud platforms with total control of the device certificate lifecycle

- Device on-boarding on IoT cloud platforms, based on X.509 certificates
- Remote deployment of device and root certificates into the device with zero touch provisioning
- Renewal of credentials in a fully automatic mode to ensure future-proof protection
- Quick and easy remote corrections in compromised scenarios, thus avoiding costly field dispatches
- Root of Trust to provide unmatched security for generation and storage of X.509 credentials
- Designed and optimized to seamlessly scale from prototyping to huge fleets

Certificate lifecycle control services description

Speeding up the deployment of your IoT devices allows you to focus on growing your business instead of on operational burdens. The certificate lifecycle control package offers an out-of-the-box experience for the registration and on-boarding of devices to cloud IoT platforms such as AWS, Azure, or even to custom platforms, making it simple, secure and cost effective.

The management of the device certificate lifecycle is essential to establish and maintain trust for IoT devices throughout the product lifecycle. In all IoT deployments, managing certificates is a difficult challenge that requires a sophisticated system and on-going effort. Failure to renew certificates before expiration can put your IoT asset at risk, completely blocking the source of your revenue.



IoT Security-as-a-Service features and services	LARA-R6 series	SARA-R410M-x3B	SARA-R422	SARA-R422S	SARA-R422M8S	SARA-R5 series	ALEX-R510M8S
Foundation security							
Security root of trust	TEE	TEE	TEE	TEE	TEE	SE	SE
Secure boot	•	•	•	•	•	•	•
Secure production	•	•	•	•	•	•	•
Secure updates	•	•	•	•	•	•	•
Anti-cloning detection & rejection	•	•	•	•	•	•	•
Secure communication (D)TLS	•	•		•	•	•	•
Design security							
Local data protection	•	•		•	•	•	•
Local C2C Security						•	•
End-to-end security							
E2E symmetric KMS	•	•		•	•	•	•
E2E data protection	•	•		•	•	•	•
E2E data integrity	□			□	□	•	•
Certificate lifecycle control							
Zero touch provisioning	□			□	□	•	•
IoT certificate manager	□			□	□	•	•

C2C = chip-to-chip E2E = end-to-end KMS = key management system

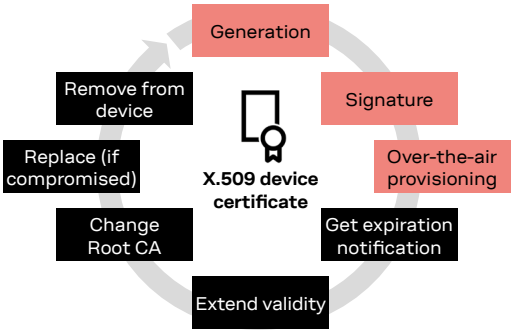
TEE = trusted execution environment □ = Available in future FW version
SE = secure element

Certificate lifecycle control

Zero touch provisioning

Zero touch provisioning is the ideal solution to securely deliver IoT device credentials over the air to enable IoT platform authentication. The X.509 certificate is stored in the module Root of Trust to allow hosting devices to be securely provisioned and automatically configured in a cloud IoT platform.

Its out-of-the box, secure, cost effective and fully automated credential provisioning, thus removes the need to set up complex software, tools, and processes for a production line.

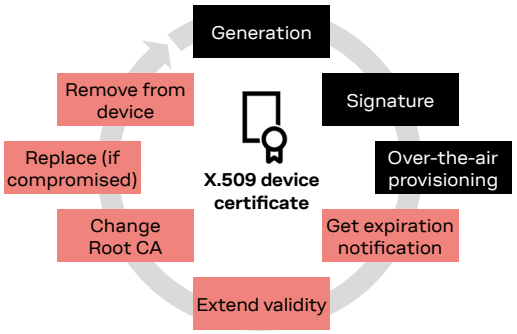


IoT certificate manager

The IoT certificate manager provides total control of the device certificate lifecycle, eliminating the task of manually managing credential renewal on thousands of devices.

It leverages the module Root of Trust and a secure dedicated channel to automate all the operations necessary to always maintain fresh and valid device authentication for IoT platforms, even in challenging scenarios such as on large fleets where credential replacement is required every month.

Designed and optimized for IoT scenarios, it eliminates the errors that can occur during manual operation on large IoT deployments, freeing resources for other activities.



Assured service availability

Certificate lifecycle control, like all u-blox services, is delivered by the Thingstream IoT cloud-based delivery platform and administration interface for enterprise IoT services. The Thingstream platform comprises IoT connectivity, security, an enterprise-grade MQTT broker, visual programming, simple enterprise integration, and support for u blox positioning chips and modules.

We stand behind our services with the highest levels of availability and delivery quality by providing full warranty, support, and with premium service levels available, tailored to suite your specific needs. The technology building blocks are developed in-house where we have full ownership without the external dependencies that can be barriers to responsiveness.

Integration with leading IoT platforms

Today it is a widely recognized benefit to use existing leading IoT platforms rather than to build your own, a benefit that inevitably absorb costs and effort, especially when a business needs to scale up from prototyping to an active fleet of thousands or hundreds of thousands of devices.

The IoT certificate manager is integrated with the AWS IoT Core and Azure IoT Hub and DPS services, to provide a seamless solution to accelerate prototyping and market scaling. While those platforms take charge of the device management and the data aggregation, the u-blox service provides an effortless and secure way to manage the X.509 certificate that AWS and Azure require as credential for device authentication.

Lifetime protection

IoT devices can remain in the field for a very long time, generally several years, and very often with no direct access other than a remote one. It is very important to preserve the privacy and integrity of the communication channel between the device and the IoT platform, for two main reasons:

- To avoid theft of sensitive data
- To prevent unauthorized access to company IT systems via use of the device as a backdoor to silently gain control of crucial IT infrastructure, such as the IoT fleet or the IT corporate database.

Until 10 years ago, the device credentials (X.509 certificates) were valid for the entire lifetime, but due to increasing infrastructure complexity and risks, in recent years the regulatory bodies have gradually suggested implementation strategies to renew credentials more often. Because of the high estimated risk both for companies and end users in a climate of continuous hacking attacks, experts are now suggesting changing the credentials every few months.

The IoT certificate manager provides the capability to continuously renew credentials according to industry needs, in a fully automatic mode to ensure future-proof protection. It generates a fresh certificate via over the air provisioning for each device, thus avoiding service interruptions.

Scale up to millions of devices

x 100	x 1000	x 10,000	x 1,000,000

Further information

For contact information, see www.u-blox.com/contact-us.