WHITE PAPER

How to securely scale up IoT device certificate management

Automated IoT device certificate management futureproofs your device security and protects your business.

Abstract

Digital IoT device certificates (X.509 certificates) are a cornerstone of a secure, trusted IoT. Issued by recognized certificate authorities, they make it possible to verify the identity and authenticity of IoT devices and host the secrets required to enable the cryptographic methods used to encrypt and decrypt communications.

For businesses with large fleets of IoT devices, managing IoT device certificates can become logistical challenge. When a single compromised or expired certificate can interrupt service, expose private customer data, or tarnish their reputation, reliable device certificate management becomes a business-critical function.

In this white paper we explore common approach to managing IoT device certifications, discuss benefits of automated solutions, and offer insight into an effective way of cost-effectively and securely scaling up certificate lifecycle management.

White paper: How to securely scale up IoT device certificate management

Author: Giovanni Solito, Senior Product Manager, Product Center Services, u-blox AG

Contents

Digital device certificates: A cornerstone for a trusted IoT

Ubiquitous connectivity is at the heart of the Internet of Things' potential to positively impact almost every aspect of our lives. From anywhere on the globe, mobile sensors, static end devices, and cloud servers can connect to each other to share data and enable value-adding applications.

But behind this ubiquitous connectivity lurks an equally massive threat. If hackers take control of a single device anywhere on the planet, they can use it to mount cybercrime campaigns for their own financial gain. Meanwhile, they can endanger both individuals and entire businesses while eroding trust in the IoT as a whole.

Digital device certificates play an essential role in contributing to an IoT users can trust. Issued by recognized certificate authorities (CA), they make it possible to verify the identity and authenticity of IoT devices and host the secrets required to enable the cryptographic methods used to encrypt and decrypt communications.

As a response to increasingly sophisticated hackers, requirements on the validity of digital device certificates are becoming more and more restrictive: Whereas in the past, certificates issued during the production of a device remained valid throughout its lifetime, cloud service providers now require regular certificate renewals to protect their businesses and the customers they serve.

For businesses with fleets of hundreds, thousands, or millions of IoT devices, these heightened requirements can become a logistical nightmare. And the stakes couldn't be higher, given that a single compromised or expired certificate can interrupt their service, expose private customer data, or tarnish their business's reputation.

In this white paper we look at how digital device certificates help secure the IoT and present common applications that depend on them for security. We then present how digital certificates are commonly managed and pinpoint some of the weaknesses inherent in this approach before outlining the benefits of an automatic certificate management solution that integrates natively with today's leading cloud service providers. Finally, we present u-blox's new IoT certification manager, offering lifetime protection for connected devices on the IoT.

What are digital device certificates?

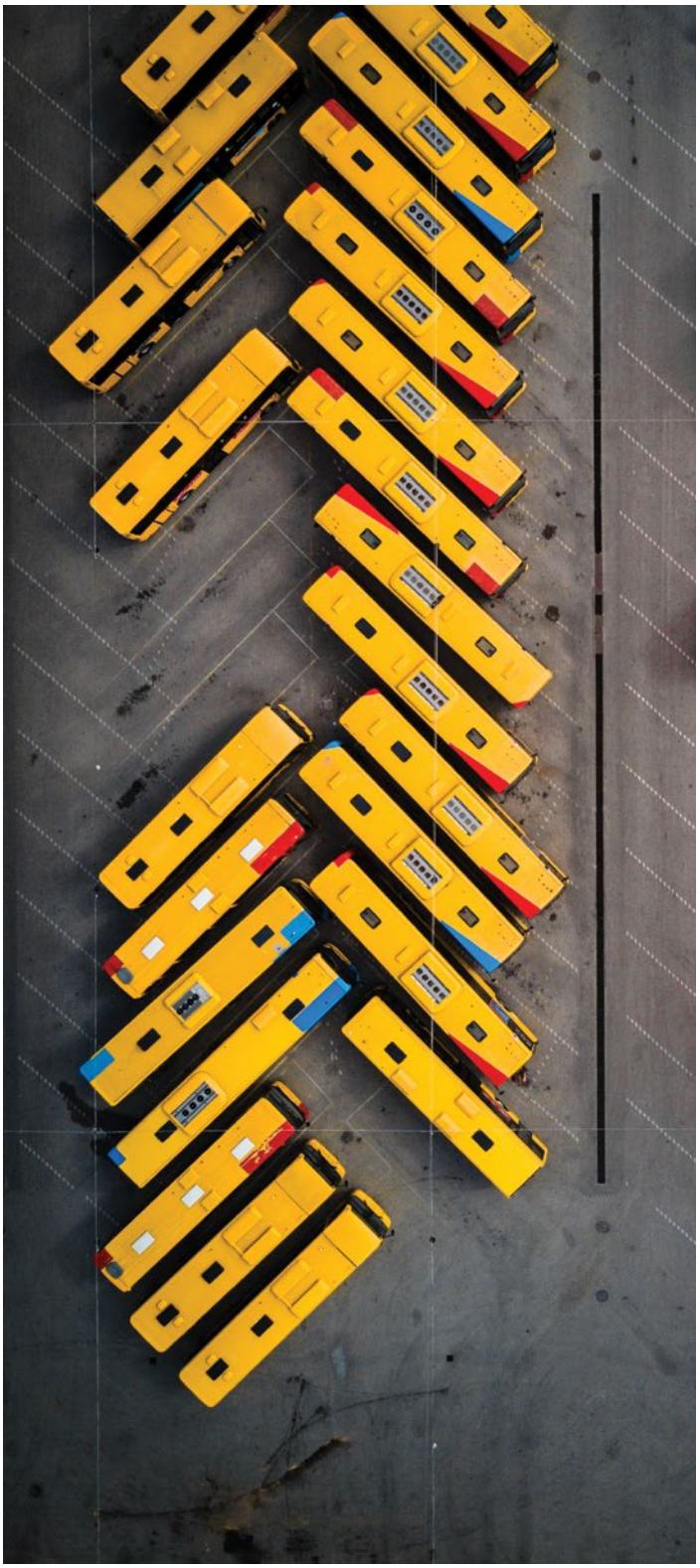
Digital device certificates, more specifically X.509 certificates, are digital documents that are used to authenticate client and device connections on the IoT. Built based on a similar approach used to authenticate connections across the internet, X.509 certificates have established themselves as the most widespread client authentication system. Its advantage over username and password schemes, for example, is that the private key – the key secret behind the authentication process – is hosted on the device and never exposed to the internet.

X.509 certificates are issued by trusted certification authorities and contain:

- Information about the certified device
- Information about the issuing certificate authority
- The public key that corresponds to the device's private key
- The supported encryption and digital signing algorithms
- Information on the certificate's validity status

Particularities of the ownership of IoT devices bring new demands for X.509 certificates. While many IoT devices are used by a single owner, e.g., fitness wearables, others, such as IoT devices installed in smart homes or used in rental equipment, can change ownership over and over again. In these cases, service design needs to consider device ownership changes and their effect on privacy, offering a way to delete data when the device is passed on to a new owner.

Another common scenario involves companies that manage vast fleets of IoT devices, for instance for vehicle fleet management, asset tracking, or smart metering. If poorly secured, these devices, which are typically far less sophisticated than consumer devices, can offer hackers multiple attack vectors to break into corporate IT systems, steal or manipulate data, or block services or infrastructure to demand ransom. In these scenarios, robust system design can be the best defense.



IoT use cases that depend on digital device certificates

X.509 certificates work silently behind the scenes to secure a variety of common IoT use cases:

Connected health

Because of the sensitive data they deal with, connected health devices used in telehealth, patient monitoring, and health data collection are subject to stringent safety and security requirements in order to protect the privacy of their users.

Asset tracking

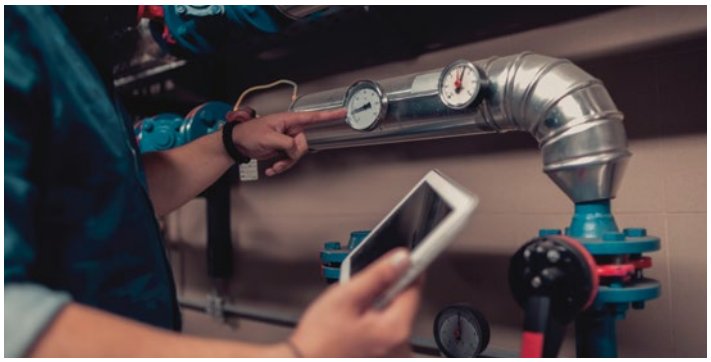
In asset tracking use cases, data authenticity is essential to monitor regulatory compliance and support decision making. At the same time, businesses want to protect confidential asset tracking and telemetry data and secure their devices and corporate IT infrastructure against cyberattacks.

Industry 4.0

Smart factories come to rely more and more on IoT solutions, making it critical for them to keep devices online and ensure device authenticity and data integrity. At the same time, they need to protect confidential data that would give outsiders a view into business secrets.

Smart cities

Hacking and ransom attacks are rampant in smart city applications, making IoT security critical to maintain 24/7 service availability, prevent hackers from taking control over smart city infrastructure and public utilities, and protect the physical safety and data confidentiality of residents.



Telematics and fleet management

In telematics and fleet management use cases, it is vital to keep constant control of vehicle fleets. This allows users to protect billings by ensuring the authenticity of data, ensure 24/7 service availability, protect the safety of personnel, and ensure the privacy of personal data.

Metering

Metering applications want to protect billing revenues by ensuring the authenticity and integrity of end-user data, securely remote-control meters for safety and billing purposes, and establish trusted communication to securely transmit data to authorized servers.

Regardless of the specific application, being able to ensure device authenticity and data integrity and keep unauthorized devices from accessing your platform is a concern shared by all IoT applications. Additionally, devices must always be secured to prevent hackers from taking control of them, be it to exploit them as an entry point into your corporate IT infrastructure, or as a platform upon which to mount coordinated cyberattacks against other third parties, exposing everyone involved to a tremendous risk of loss of reputation and revenues.

The standard approach to provisioning digital device certificates

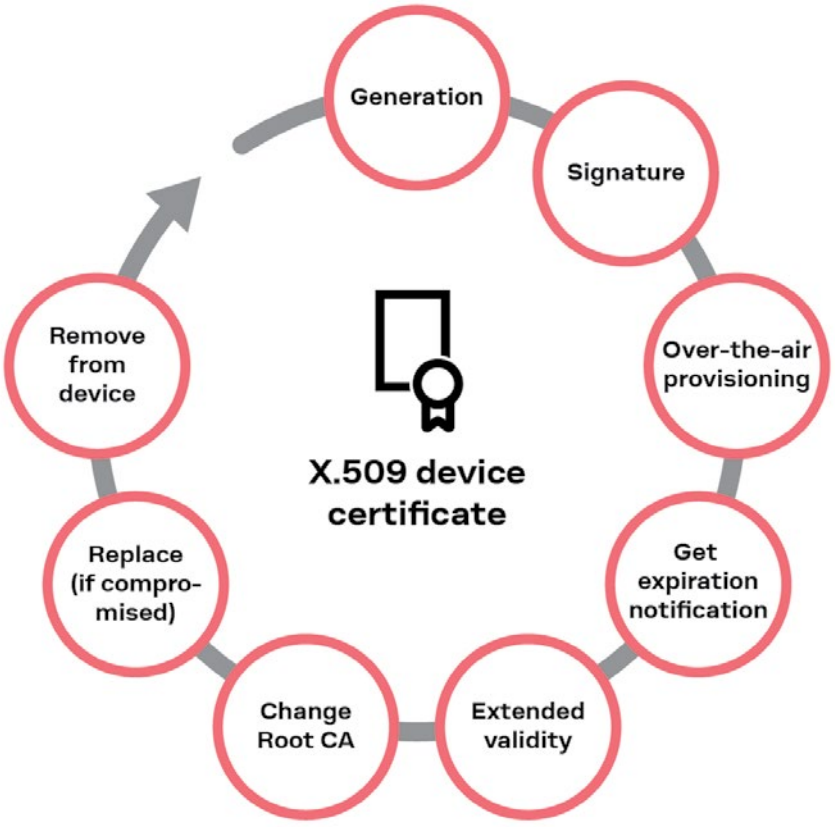
Once issued and digitally signed by a trusted certificate authority, X.509 certificates act as an electronic passport that validates the identity of the device they are hosted on – a prerequisite to establishing a secure (D)TLS session for encrypted communication.

While the customer gets the full benefit of a seamless, secure solution, the device developers carry the full burden of setting up the secure processes involved, stress testing them, and scaling them up.

The schematic below illustrates the steps involved in provisioning devices with X.509 certificates using a root certificate issued by a certificate authority.

1. Securely create a public / private key pair and the device's X.509 certificate
2. Securely store the root certificate's private key as well as each device's private key in the cloud using a hardware security module
3. Securely provision the device's certificate and its private key without exposing them over the internet
4. Implement secure private key storage in the device with the required level of protection
5. Configure the device to authenticate itself using the certificate
6. Provision the IoT platform with the device's digital certificate to enable authentication.

Because these steps must be repeated during production for each individual device, device provisioning can easily become a bottleneck for device manufacturers seeking to scale up production.



Challenges with the standard approach to managing digital certificates

The standard manual approach to managing digital certificates involves keeping track of device certificates, their validity periods, related policies, revocations, and configuration data in a spreadsheet. The list of pain points product developers encounter when managing digital certificates with the conventional approach, which we explore here, can make IoT device development appear daunting, in particular for small to mid-sized companies with little experience in secure service development and cryptographic methods.

Logistics: As outlined in the previous section, securely provisioning digital device certificates and the private keys required for modern encryption methods onto devices in production is operationally and logistically challenging. In addition to being difficult to automate, it requires secure production facilities and carefully designed and tested secure manufacturing processes.

Security: Keeping every single device's private keys private is essential to maintaining a high level of security. While repeating the provisioning process done during production is too costly for most typical IoT devices, keeping the same key pair throughout the device's lifetime is too risky. Maintaining key freshness is a fundamental challenge for IoT devices that remain in use for sometimes over a decade.

Costs: Securely storing the private encryption keys on the IoT device requires dedicated hardware, such as a trusted platform module (TPM), which increases bill of material costs. Additional cost points include investments in secure production facilities, in-house expertise in secure software development, and maintenance work required to continuously stay one step ahead of cybercriminals.

Maintenance: Once devices are deployed, device owners need to ensure that their digital certificates are renewed before they expire and that any devices that are comprised quickly receive a new digital certificate and private key before being reprovisioned to the cloud service provider with which they communicate. Failure to respond swiftly in either case can lead to local service interruptions or potentially devastating outages caused by cybercriminals.

Scalability: As businesses scale up production, challenges in terms of logistics, costs, and, ultimately, security compound, making it all but impossible to manage digital certificates effectively and efficiently without a dedicated team of experts and highly sophisticated processes such as cloud-based secure key storage that further drive up costs.

The benefits of zero-touch provisioning

Zero-touch provisioning helps overcome the potential bottleneck of developing and scaling the production and deployment of connected devices. Its most obvious benefit lies in simplifying the deployment of IoT devices by streamlining the registration and on-boarding process required to connect IoT devices to major cloud IoT platforms.

Arguably more importantly, however, working with connectivity hardware supporting zero-touch provisioning essentially outsources many of the costly and challenging steps involved in developing secure IoT devices, including i) hiring highly skilled security experts, ii) setting up secure production logistics, iii) procuring the most appropriate trusted platform module, and iv) secure product development.

The benefits of automated IoT certificate lifecycle managementt

Automated IoT certificate lifecycle management further addresses many of the aforementioned pain points, making it possible to effectively and efficiently manage any number of certificates throughout the lifetime of the deployed devices. Automated IoT certificate lifecycle management offers important benefits to IoT device fleet operators:

1. Zero-touch provisioning of IoT devices onto cloud service infrastructure.
2. Fleet-level certificate expiration date monitoring and renewal, even remotely.
3. Automated recalling and replacement of compromised certificates.
4. Automated handling of expired root certificates, including certificate and private key replacement on all devices that derive their device certificates from that root certificate.
5. Simplified management of segregated device fleets into groups that use different root certificates to reduce the risk associated with one root certificate being compromised.
6. Automated migration of device fleets from a root certificate used for testing a final production root certificate.
7. Simplified certificate replacement in the case of change of ownership.

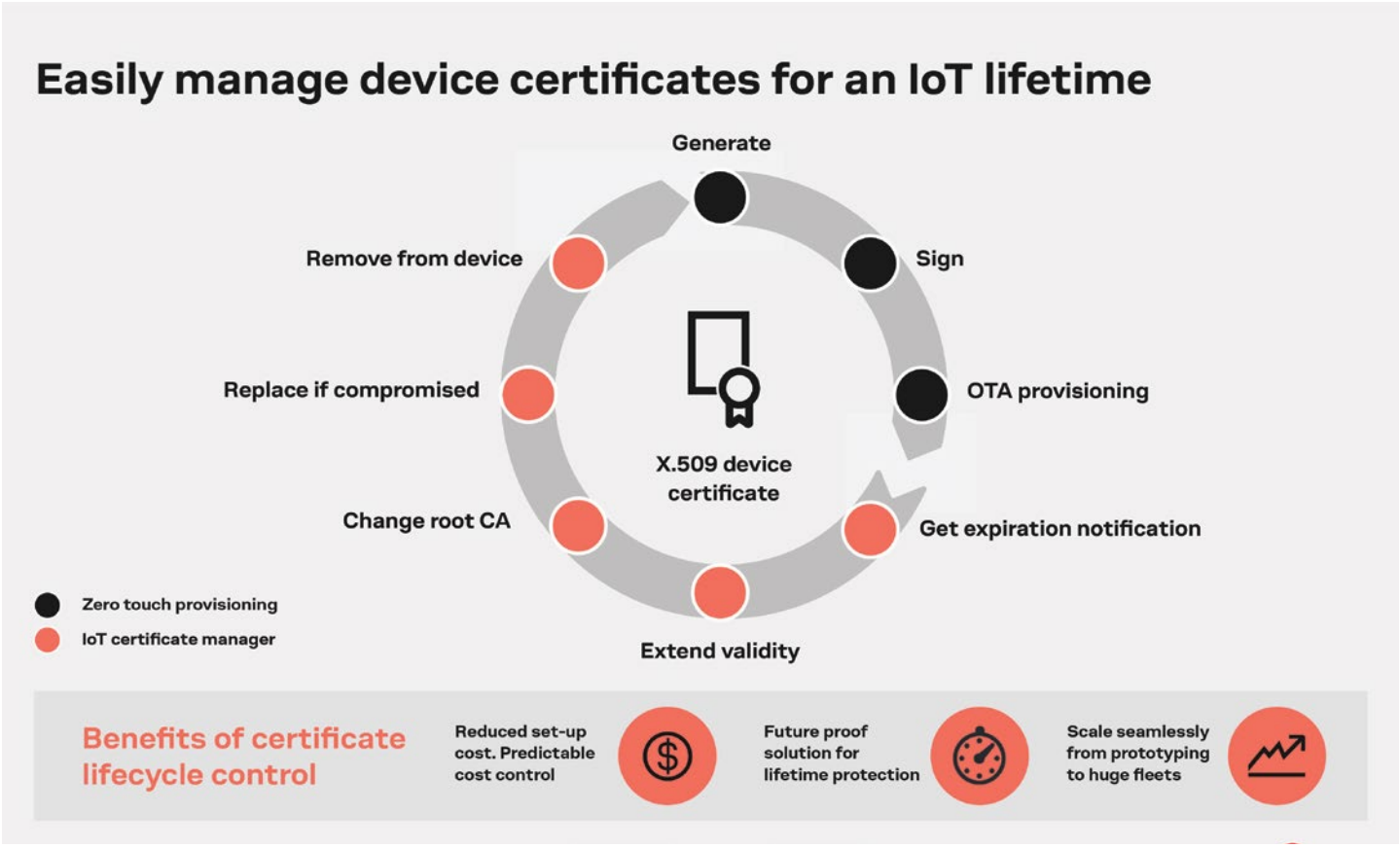
Securely scale up certificate lifecycle management with u-blox

The u-blox certificate lifecycle control package simplifies every aspect of IoT certificate lifecycle management offering:

- **Fast time to market** by minimizing the need for time, expertise, resources, development, and testing.
- **Hassle-free certificate management**, including certificate generation, provisioning, replacement, and removal.
- **Reduced set-up cost and predictable cost control.**
- **Future-proof lifetime protection.**
- **Seamless scaling from prototyping to huge device fleets.**

Our certificate lifecycle control package comprises two separate services:

- **Zero touch provisioning service** speeds up the deployment of IoT devices with a quick and easy registration and on-boarding of devices to major cloud IoT platforms such as AWS and Microsoft Azure as well as your own custom platform.
- **IoT certificate manager service** provides total control of the device certificate lifecycle, eliminating the task of manually managing credential renewal on any number of devices.



The solution is fully integrated with the u-blox R5 cellular platform, leveraging its industry hardened root of trust as well as a secure dedicated communication channel to automate all operations involved, ensuring that device credentials are always valid and fresh.

Learn more

Learn more about our certificate lifecycle control security toolkit and our SARA-R5 series LTE-M and NB-IoT modules that together provide a fully integrated silicon-to-cloud security solution that is unmatched in the industry. Explore our Thingstream IoT service delivery platform, learn more about our entire IoT Security-as-a-Service portfolio, get a SARA-R5 evaluation kit, and check out our YouTube video on zero touch provisioning.

And if you have any further questions, reach out to your nearest sales representative or contact us here. We look forward to hearing from you!

About the authors

Giovanni Solito, Senior Product Manager, Product Center Services, u-blox.

Giovanni Solito joined u-blox after being Head of Engineering and Senior Product Manager B2B services at Linkem, the Italian broadband service provider and leader in fixed wireless access.

He has over 15 years of leadership experience in product management, strategy, and business development roles in the telecommunication industry, with a focus on broadband and B2B solutions.

Giovanni holds an Executive MBA the School of Management at the MIP Politecnico in Milan and a BS in Telecommunication Engineering from the University of Padua.

About u-blox

u-blox (SIX:UBXN) is a global provider of leading positioning and wireless communication technologies for the automotive, industrial, and consumer markets. Their solutions let people, vehicles, and machines determine their precise position and communicate wirelessly over cellular and short range networks. With a broad portfolio of chips, modules, and a growing ecosystem of product supporting data services, u-blox is uniquely positioned to empower its customers to develop innovative solutions for the Internet of Things, quickly and cost effectively. With headquarters in Thalwil, Switzerland, the company is globally present with offices in Europe, Asia, and the USA.

u-blox AG
Zuercherstrasse 68
8800 Thalwil
Switzerland

www.u-blox.com