WHITEPAPER

Secured Device Credential Provisioning in IoT:

A Joint Solution by CommScope and Infineon

COMMSCOPE®

Infineon

Abstract

Secured device credential provisioning has become a critical requirement in the rapidly growing Internet of Things (IoT) ecosystem. As IoT devices scale across consumer, industrial, and infrastructure sectors, manufacturers are under mounting pressure to address security, streamline production, and meet a widening array of regulatory requirements. This white paper introduces a scalable, production-ready solution developed jointly by **CommScope and Infineon**, combining **CommScope's PKIWorks® platform** with **Infineon's OPTIGA™ Trust M** to enable secured and efficient provisioning of connected devices.

The paper outlines the technical design and operational benefits of the joint solution, focusing on fundamental challenges such as secured key generation, provisioning at scale, and credential lifecycle management. This approach supports both factory and in-field provisioning. In the factory, it streamlines complex manufacturing workflows by eliminating the need for SKU-specific provisioning, reducing upfront costs, and accelerating time to market. In the field, it enables devices to provision their intended credentials on demand, allowing them to seamlessly join new ecosystems at any time—even long after deployment.

By combining these capabilities, the solution not only allows compliance with global security standards and delivers end-to-end cryptographic protection but also provides the flexibility to help manufacturers and service providers future-proof their IoT deployments and maintain a competitive edge.

TABLE OF CONTENTS

1 Introduction

The Internet of Things (IoT) is expanding at an unprecedented pace, with billions of connected devices entering global markets across consumer, industrial, and healthcare sectors. This explosive growth brings significant complexity to device manufacturing—particularly in securing devices at scale while maintaining operational agility. Manufacturers must not only embed security into their products but also ensure compliance with an increasingly complex and evolving regulatory landscape. As device lifespans stretch over a decade, solutions must support long-term credential management, secured updates, and reliable identity verification throughout the product life cycle.

In response to these demands, **CommScope and Infineon** have collaborated to deliver a joint solution for secured device credential provisioning. This integrated approach combines **CommScope's PKIWorks® platform**, a cloud-based certificate authority and provisioning service, with **Infineon's OPTIGA™ Trust M**, a hardware root of trust embedded within IoT devices. Together, the two technologies enable manufacturers to provision strong device identities efficiently—both at the factory and in the field—while simplifying workflows, minimizing risk, and reducing time to market.

This white paper is structured to guide readers through the key motivations, technical architecture, and real-world benefits of the joint solution. We begin by outlining the top security challenges facing IoT manufacturers today, followed by a brief introduction to Public Key Infrastructure (PKI) and the role of certificate authorities. Next, we provide an overview of the OPTIGA™ Trust M and walk through the design of the Infineon–CommScope joint solution, including its unique support for field provisioning and reusable TypeIDs. The final sections cover deployment steps, business value, and key takeaways—equipping stakeholders with a practical roadmap for integrating secured provisioning into their IoT products.

2 Key Security Considerations in IoT Industry

In conversations with original-equipment manufacturers (OEMs) and design houses across the IoT landscape, three pain points surface again and again:

1. **Cost-versus-security tension.** Hardware roots of trust, secure elements, and lifecycle management tooling add complexity, extend development time, and raise the bill of materials. In highly price-sensitive product lines, even a few extra cents per unit can become a hard veto, forcing teams to choose between margins and robust protections.

2. **Escalating regulatory mandates.** Frameworks such as the EU Cyber Resilience Act (CRA), the U.S. IoT Cybersecurity Improvement Act, and emerging state-level statutes are turning "security-by-design" from marketing language into a legal prerequisite. Non-compliant devices face delayed certifications, blocked market entry, and downstream liability exposure.
3. **Sustained security maintenance.** IoT devices may remain in service for a decade or more, but manufacturers rarely plan for long-term security support beyond the initial launch. Without a secured update pipeline, cryptographic agility, and a plan for key rotation, vulnerabilities discovered post-deployment can linger unpatched for years—putting users, networks, and brands at risk.

Taken together, these realities shift security from a feature checkbox to a lifelong product commitment—one that must be designed, budgeted, and governed from the first architecture review through end-of-life decommissioning.

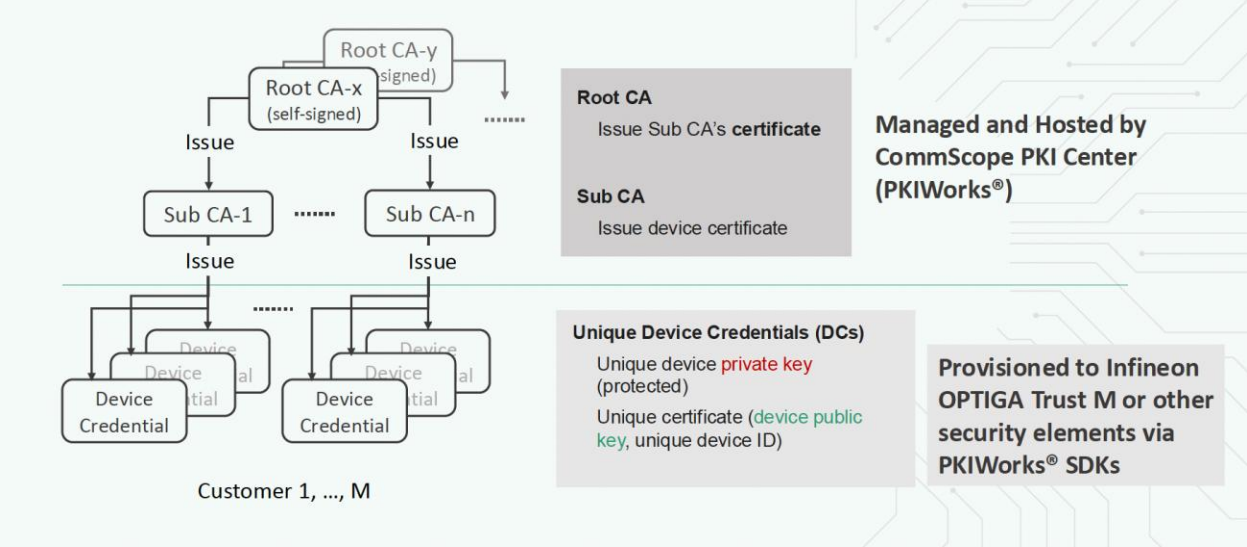
Overcoming these challenges starts with a solid security foundation built on two pillars: device software security and device credential security. The focus of our joint solution is on the second pillar. Unique, tamper-resistant credentials are essential for satisfying both technical integrity and regulatory mandates. Each credential must be tied to a single device, cryptographically protected throughout its life cycle, and administered by a trusted Certificate Authority—a topic we'll examine in more depth next.

3 Technical Background on CA and PKI

Before we dive into how our joint solution works, let's take a moment to review the basics of Certificate Authorities (CAs) and Public Key Infrastructure (PKI).

Here are some key concepts:

- Root CA
- Sub CA
- Device Credential



A helpful analogy is the driver's license system. In PKI, Root CAs act like a federal government—they're the ultimate trust anchors, issuing certificates to subordinate CAs (Sub CAs), much like a federal agency sets the security standards for licenses used for federal purposes like boarding planes or entering federal buildings (e.g. REAL IDs), which are issued by state DMVs, Sub CAs, in turn, issue certificates to individual devices—these are the digital equivalents of driver's licenses, used to prove a device's identity.

Each device is assigned a unique key pair (a public and private key) along with its corresponding certificate, which serves as a secured digital ID. To maintain trust, this key material must be protected within secured memory.

CommScope manages the entire trust chain through our PKIWorks® platform, including creation and operation of both Root and Sub CAs. PKIWorks® has already been used to provision and manage billions of device credentials in the field. We also handle secured provisioning of credentials into OPTIGA™ Trust M or other secure elements, using our SDKs to integrate directly with the PKIWorks® infrastructure—accessible anytime, from anywhere.

This end-to-end trust chain allows that when a device "presents its license," other systems can verify its authenticity with confidence, knowing it was issued by a trusted authority under our full control.

4 Overview of Infineon OPTIGA™ Trust M

As embedded systems (for example, IoT devices) are increasingly gaining the attention of attackers, Infineon offers the OPTIGA™ Trust M as a turnkey security solution for industrial automation systems, smart homes, consumer devices and healthcare devices. This high-end security controller comes with full system integration support for simple and cost-effective deployment of high-end security for your assets.

Integrated into your device, the OPTIGA™ Trust M supports protection of your brand and business case, differentiates your product from your competitors, and adds value to your product, by making it stronger against cyberattacks.

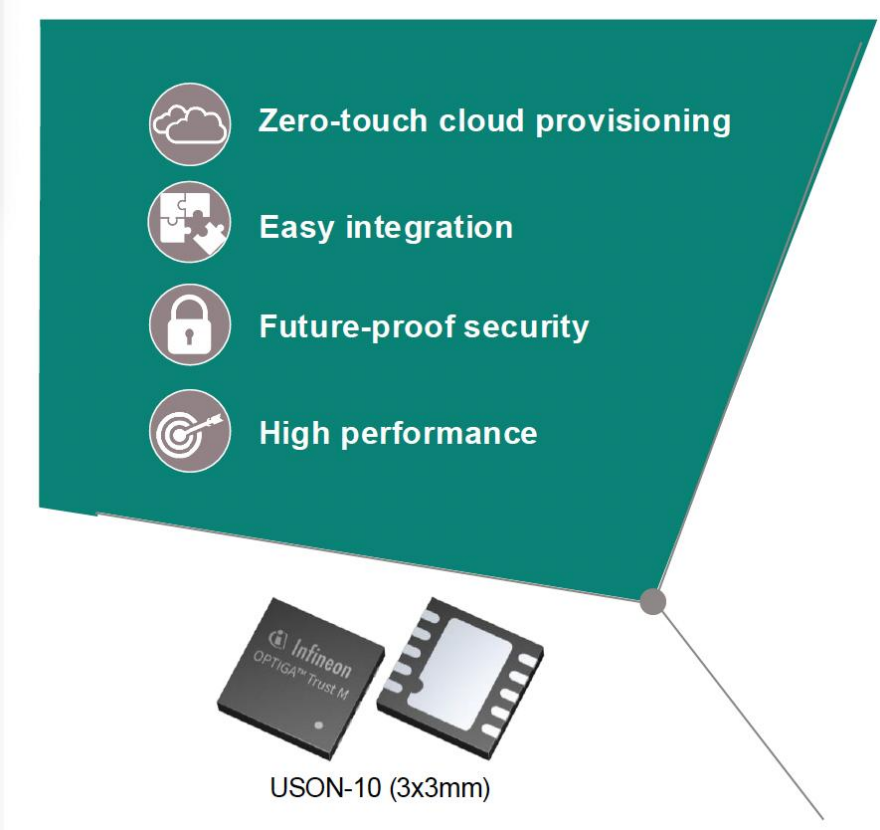
The OPTIGA™ Trust M is based on an advanced security controller with built-in tamper-resistant NVM for secured storage and Symmetric/Asymmetric crypto engines to support ECC NIST curves up to P-521, ECC Brainpool curve up to P-512, RSA® up to 2048, AES key up to 256, HMAC up to SHA-512, HKDF up to SHA-512 and SHA-256. This new security technology greatly enhances your overall system security.

The turnkey setup – with full system integration and all key/certificate material preprogrammed – reduces your efforts for design, integration and deployment to a minimum. As a turnkey solution, the OPTIGA™ Trust M comes with preprogrammed OS/Application code locked and with host-side modules to integrate with host micro controller software. The temperature range of −40°C to +105°C combined with a standardized I2C interface and the small PG-USON-10-2,-4 footprints will facilitate onboarding in your existing ecosystem. Almost 30 years in a market-leading position with nearly 20 billion security controllers shipped worldwide are the results of Infineon's strong expertise and its commitment to make security a success factor for you.

The OPTIGA™ Trust M covers a broad range of use cases necessary for many types of applications that include the following:

1. Network node protection using Mutual Authentication such as TLS or DTLS
2. Protect the Authenticity, Integrity and Confidentiality of your product, data and IP
3. Secured Communication
4. Datastore Protection
5. Lifecycle Management
6. Platform Integrity Protection
7. Secured Updates

The OPTIGA™ Trust M comes with up to 10 kB of user memory that can be used to store X.509 certificates and data. OPTIGA™ Trust M is based on Common Criteria (CC) EAL6+ (high) certified hardware enabling it to prevent physical attacks on the device itself and providing a high level of protection for stored keys or arbitrary data stored against access by an unauthorized entity. OPTIGA™ Trust M (SLS 32AIA010MK) is certified to PSA Level 3. The PSA certificate can be found at http://www.psacertified.org. The CC certificate can be found at www.bsi.bund.de by searching for BSI-DSZ-CC-0961 (Hardware Identifier IFX_CCI_00000Bh) and referring to the latest CC certificate. OPTIGA™ Trust M supports a high-speed I2C communication interface of up to 1 MHz (FM+).



Key Features

High-end PSA Level 3 certified security controller

Turnkey solution

Up to **10kB** user memory

I2C interface with Shielded Connection

Cryptographic support: ECC : NIST curves up to P-521, Brainpool r1 curve up to 512,

RSA® up to 2048,

AES key up to 256, HMAC up to SHA512,

TLS v1.3 PRF and HKDF up to SHA512

Crypto ToolBox commands for SHA, ECC and RSA® Feature, AES, HMAC and Key derivation

Shielded Connection for encrypted host communication

Hibernate for zero power consumption

Temperature: -25°C to 85°C and -40°C to 105°C

5 Infineon-CommScope Joint Solution

5.1 Main Challenges in Device Provisioning

With the foundation of PKI and device credentials established, we can now shift our focus to two of the most pressing challenges in bringing secured IoT products to market: **security risk** and **production complexity**.

For many device manufacturers, incorporating secured credentials into the production process can be daunting. Whether provisioning keys during manufacturing or retrofitting deployed devices to enable new functionality, these tasks often require significant planning and technical adaptation. Maintaining production yield while embedding robust security is a delicate balancing act—especially when security expertise is limited or fragmented across teams.

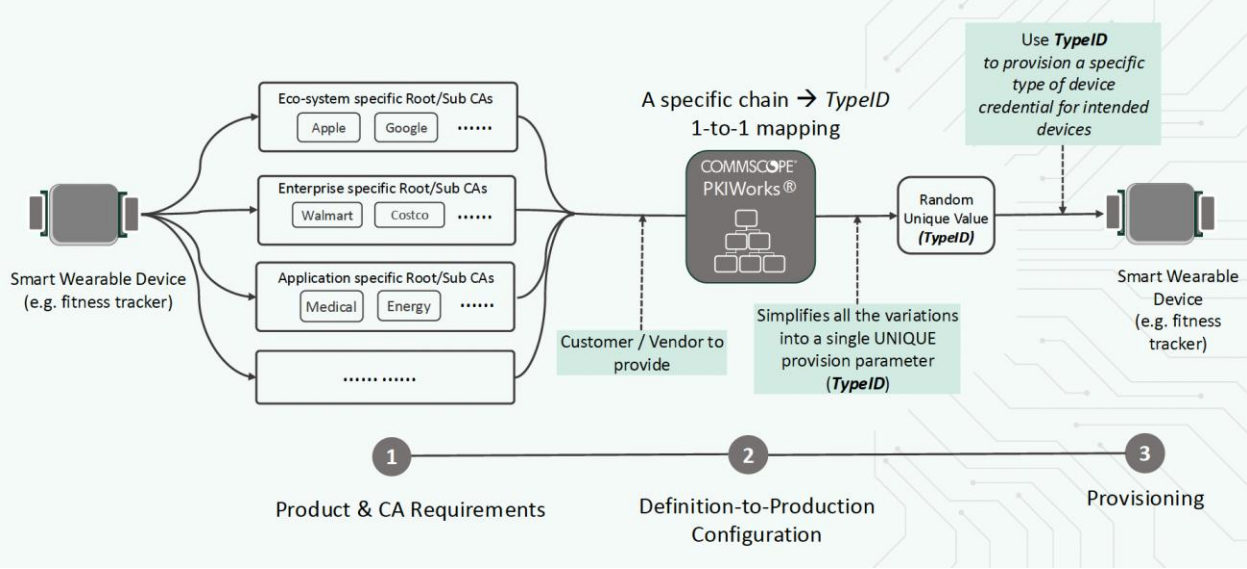
Attempting to design and implement a secured provisioning flow internally not only demands specialized cryptographic knowledge but also introduces additional time, resource strain, and operational costs. This is where the joint CommScope–Infineon solution offers a meaningful advantage. Our pre-integrated platform offloads the complexity—handling everything from cryptographic operations and secure key provisioning to cloud-based infrastructure and lifecycle management, helping manufacturers meet their security goals without disrupting production efficiency.

5.1.1 Addressing Production Complexity

As a concrete example, consider a fitness tracker—a seemingly simple device that reveals the complexity of credential provisioning and PKI requirements.

If the tracker connects to Apple HealthKit or Google Fit, it may require ecosystem-specific credentials to securely sync user data with cloud accounts tied to those platforms. If the same tracker is sold through Walmart, it might need to be enrolled in Walmart's enterprise system before reaching store shelves. And if the device integrates with a health app that offers insights or connects to electronic healthcare records, app-specific credentials may be required to take care that sensitive health data is encrypted and only accessible by authorized services.

Each of these scenarios demands a different type of credential—ecosystem, enterprise, or application-specific—to enable secured, trusted communication. The diversity of use cases illustrates why credential provisioning must be flexible and scalable to meet real-world deployment needs.



We address this complexity through a streamlined three-step process:

First, we work closely with the enterprise customer to define and input all required product and PKI parameters into CommScope's PKIWorks® platform—this includes information such as company identity, product line details, and the specific credentials needed for each use case.

Second, a unique identifier, called a **TypeID**, is generated. This TypeID maps one-to-one to the specific set of product and PKI parameters defined by the customer, effectively serving as a secure template for credential provisioning.

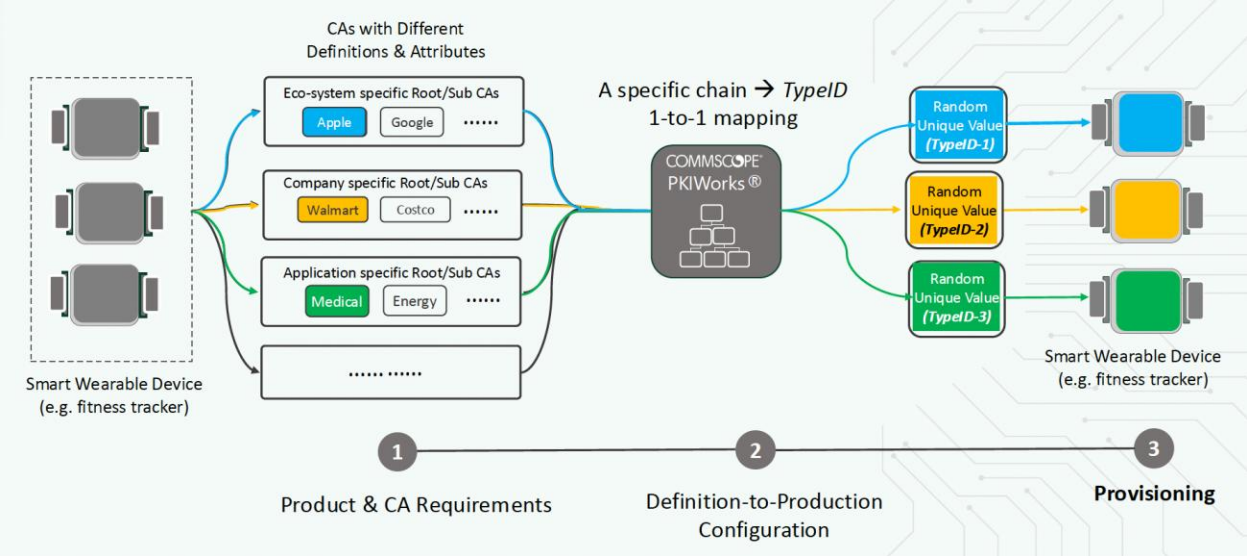
Finally, the customer uses the TypeID to provision the appropriate type of device credential onto each target device. Thereby, every device receives the correct credentials for its intended deployment scenario, while reducing manual effort and the risk of misconfiguration.

Let's return to our fitness tracker example to see how this approach works in practice.

You begin with a generic fitness tracker—identical hardware, no credentials yet provisioned. When you provision it with Apple ecosystem credentials, it becomes the *blue watch*, ready to sync with Apple Health. Provisioning it with Walmart's enterprise credentials, and it becomes the *yellow watch*, configured for Walmart's systems. Provision it with credentials for a healthcare application, and it becomes the *green watch*, ready to handle sensitive health data securely.

The real value here lies in how we simplify and scale PKI management. Instead of tracking dozens of attributes for every device variation, customers only need to manage a single item: the **TypeID**. Each TypeID encapsulates all relevant product and certificate parameters, serving as the definitive reference for what a device is and how it should be provisioned.

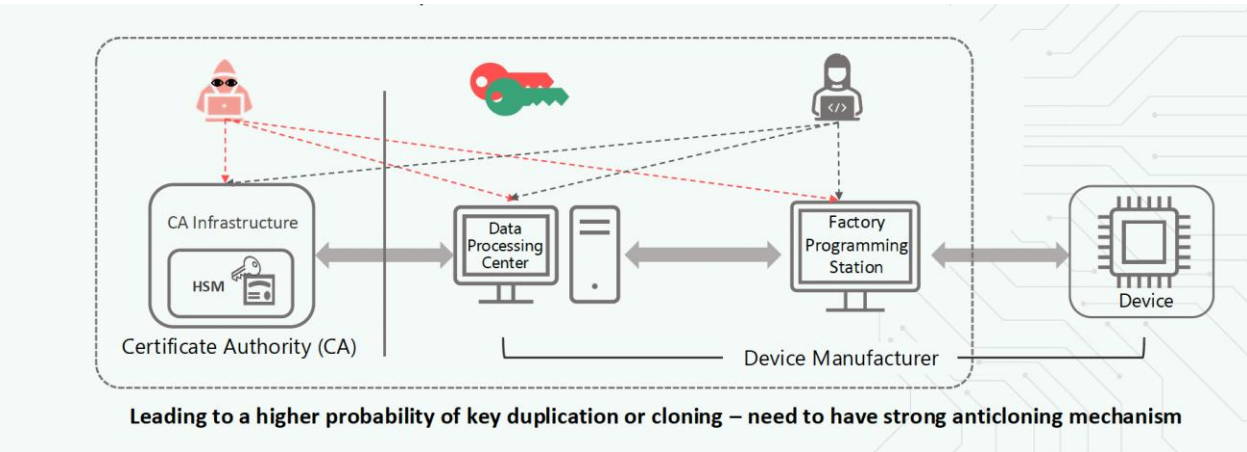
With this model, manufacturers can build and ship a unified hardware SKU—as long as the devices share core functionality—and defer differentiation to the provisioning step. By assigning a specific TypeID at provisioning time, they take care that each device receives the correct credentials for its intended use case, whether it's for consumer fitness, retail environments, or medical applications.



5.1.2 Addressing Security Risk and Reducing Errors

Let's start by examining the security risks associated with a typical factory configuration—using a conventional provisioning setup as an example.

First, consider the process of key generation. When key pairs are generated outside the device, such as by a certificate authority, then passed through internal data systems, out to programming stations, and finally into each device—the attack surface becomes broad and difficult to secure. Every step along that path introduces potential vulnerabilities. Recent cyberattacks have shown that high-volume, high-value environments like manufacturing lines are increasingly being targeted. A single successful breach can compromise device credentials at scale, posing a serious threat to product integrity and customer trust.
Second, as production volume increases, so does the likelihood of operational errors. Manual processes and multiple handoffs can lead to mistakes—such as provisioning the same credential to more than one device. This kind of duplication undermines the trust model of PKI, much like issuing the same driver's license to multiple individuals would compromise identity systems. In both cases, the consequences can be far-reaching, eroding security at both the device and system level.



Our joint solution is built around two key goals: reducing security risk and minimizing production errors.

To reduce security risk, each key pair is generated *inside* the device itself. The private key is created and remains securely stored within an Infineon Secure Element, such as OPTIGA™ Trust M. This approach dramatically shrinks the attack surface to just the device itself. Any potential

attacker would need to compromise devices individually, a task made even more difficult by the advanced security features embedded in Infineon's secure elements.

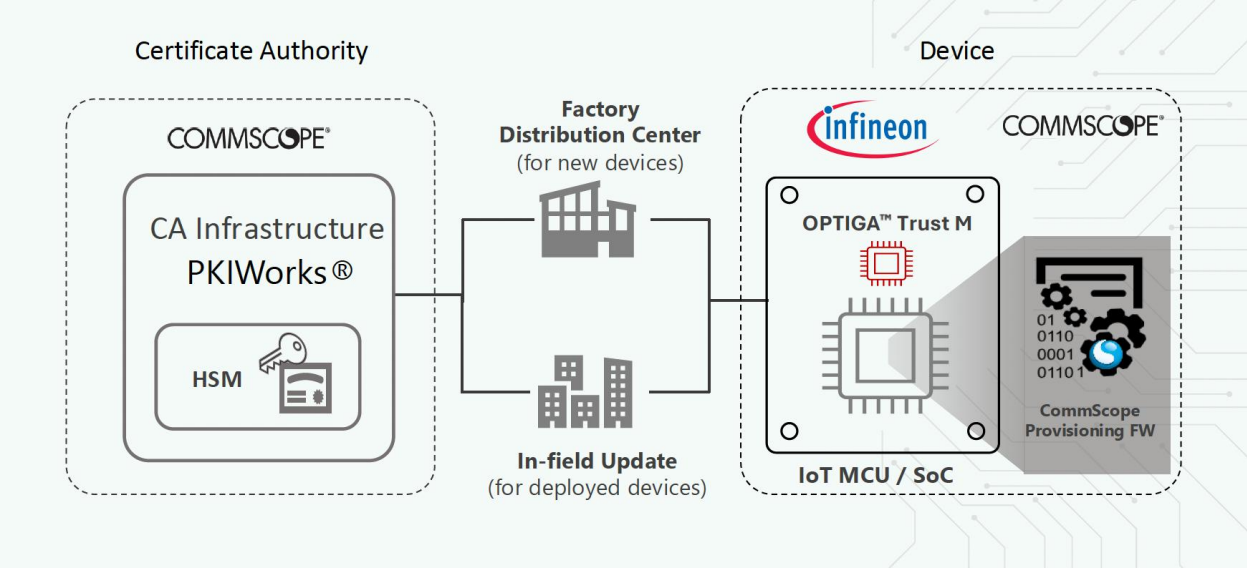
To minimize production errors, we tightly couple the credentialing process with the device. The matching certificate is provisioned directly back into the same device that generated the key pair, eliminating risks of mix-ups, duplication, or misassignment that can occur when managing high volumes of credentials across distributed systems.

The result is a provisioning process that is both well-secured and reliable—protecting device credentials while enforcing accuracy at scale.

5.2 Overview of Joint Solution

Together, CommScope and Infineon have developed a **joint solution** that makes provisioning device credentials onto the OPTIGA™ Trust M simple, well-secured, and highly efficient.

- Device provisioning is powered by **CommScope's PKIWorks®** certificate authority server, which issues trusted device credentials with full cryptographic integrity.
- The **OPTIGA™ Trust M** is provisioned through an **Infineon MCU** acting as the host, orchestrating secured communications with PKIWorks®.
- **CommScope's provisioning client firmware**, running on the host MCU, enables seamless and secured provisioning experience that's tightly integrated with the hardware.
- Whether on the **production line** or already **deployed in the field**, devices can be securely provisioned at any stage—for long-term flexibility and robust security throughout the device lifecycle.



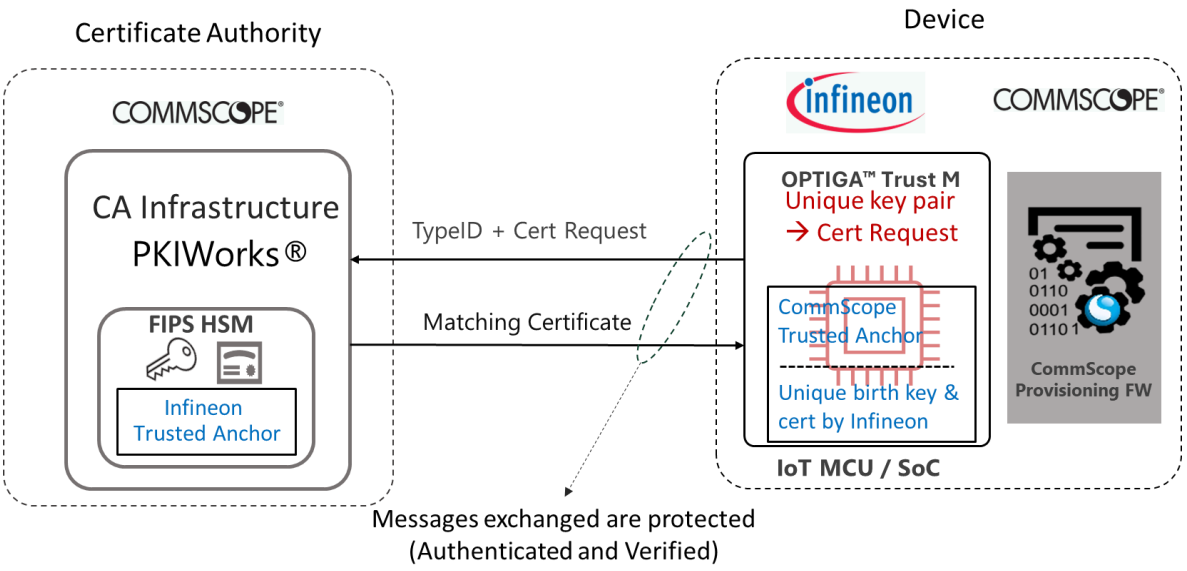
5.3 CommScope Specific SKU of OPTIGA™ Trust M

In this section, we provide some technical details of the CommScope specific SKU of the OPTIGA™ Trust M, designed for enhanced security and seamless credential provisioning.

Consider the diagram of the joint solutions given in Section 5.3. The setup for the CommScope-specific SKU includes two trust anchor certificates, by CommScope and Infineon respectively. On the device side, each CommScope-configured Trust M chip preloaded with a unique Infineon key and certificate at birth, along with the CommScope trust anchor certificate. On the server side, CommScope's PKIWorks® platform is pre-configured with the Infineon trust anchor certificate. Collectively, the two trust anchor certificates establish a secured foundation from the very beginning.

When new credentials are required, the device generates a fresh key pair internally and creates a certificate signing request. This request—along with the associated TypeID—is signed using the Infineon birth key and transmitted to the PKIWorks® server. Because the server recognizes and trusts the Infineon trust anchor, it can authenticate the request and issue a corresponding certificate.

The returned certificate in response message is then signed using the CommScope private signing key. Since the CommScope specific SKU of OPTIGA™ Trust M includes the CommScope's trust anchor certificate, the response message can be authenticated by the device – checking the certificate was issued by CommScope, not a rogue third party.



At every stage of this process, all provisioning messages are cryptographically authenticated using the built-in trust anchors—for secured, reliable, and fully traceable communication from device to cloud.

This solution works the same way for both initial factory or in-distribution builds and for in-field device credential updates. Customers can order CommScope-specific SKU for their applications.

5.4 In-Field Device Update with Non-CommScope Specific SKU

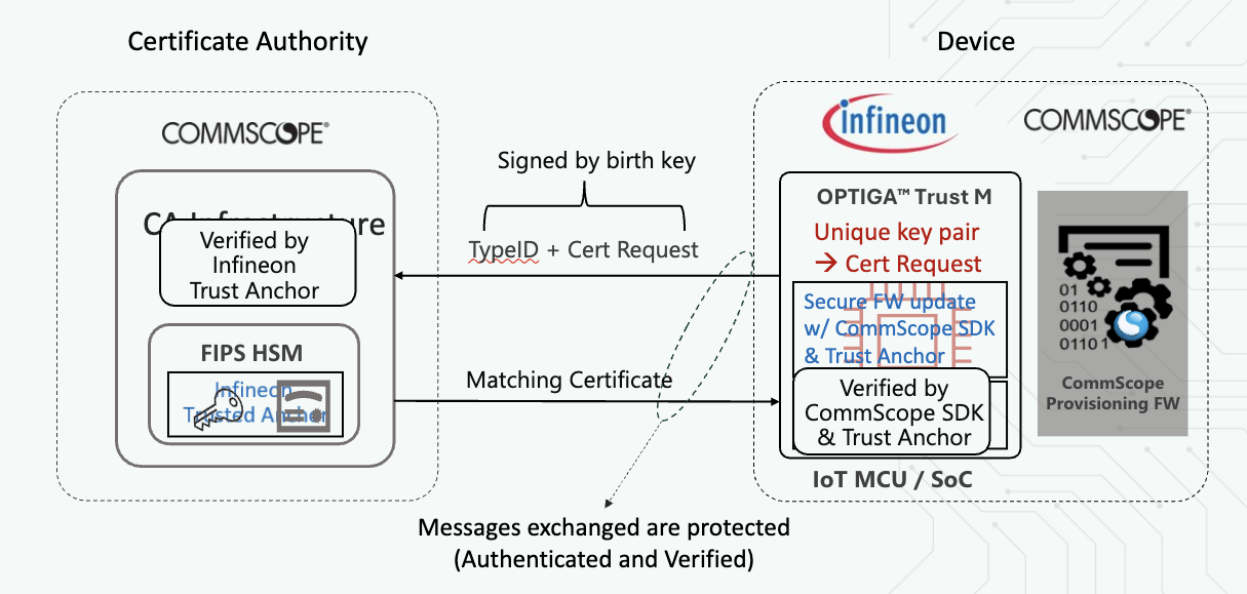
Our joint solution also supports **secured in-field provisioning** for devices that do not use the CommScope specific SKU of OPTIGA™ Trust M. This enables devices already deployed with customer-specific or generic OPTIGA™ Trust M chips to receive new credentials—extending their capabilities and/or lifetime.

The general prerequisites are that (1) the devices already have their original Infineon or customer specific birth key and certificate and (2) the devices have secured software/firmware update capabilities. With these basic prerequisites, simple setup/update can be done on both the server side and the device prior to new credential provisioning.

On the server side, the CommScope PKIWorks® can be configured to trust either Infineon's embedded trust anchor certificate or a customer-specific certificate. So the server can authenticate any messages from fielded devices equipped with OPTIGA™ Trust M and running on an Infineon MCU. On the device side, leveraging its built-in update capability, a **secured**

firmware update can be done to deliver the CommScope provisioning SDK and trust anchor to the device.

The device generates a certificate signing request (CSR), tagged with the desired TypeID, and signs it using its Infineon or customer-specific birth key. PKIWorks® validates the request against the appropriate trust anchor (Infineon or customer-specific) and returns a newly issued certificate. The CommScope SDK, delivered to the device through a secure firmware update process, authenticates the response from the server using the CommScope trust anchor certificate.



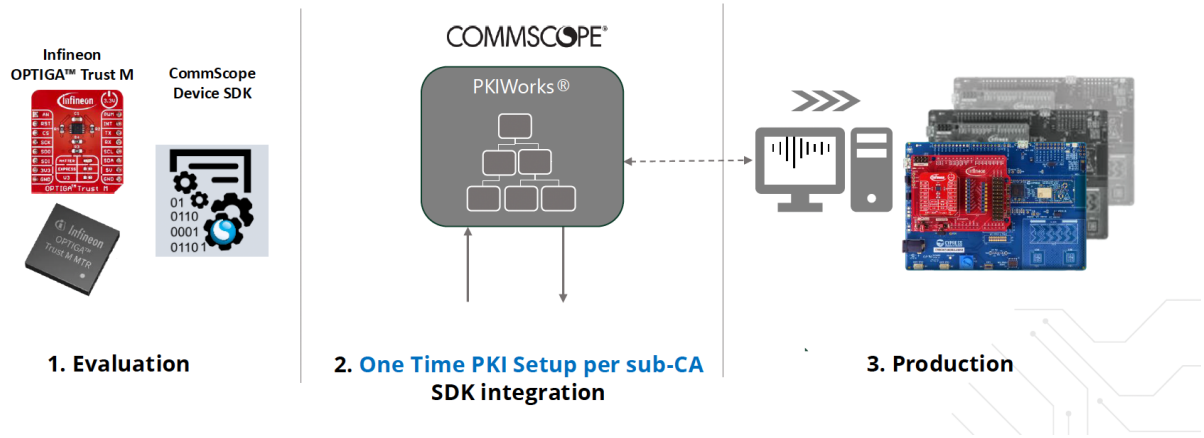
This **mutual authentication** ensures that every message exchanged is verified, protected, and fully trusted—delivering **end-to-end security**, after the devices are already deployed in field.

Secured in-field provisioning opens powerful new opportunities for already deployed devices. It allows devices to gain new features, join new ecosystems, or take on new roles at any point in their lifecycle—even years after deployment. By removing the dependency on factory pre-provisioning, manufacturers can reduce upfront costs, accelerate time to market, and adapt products more flexibly—gaining both operational agility and a lasting competitive edge.

6 Business Processes and Values

6.1 Working with CommScope: Step-by-Step Process

Here's how customers collaborate with CommScope to deploy the joint solution:



- **Start with evaluation**: Customers begin by testing the solution using our SDK, running on an Infineon MCU paired with an OPTIGA™ Trust M. This allows them to provision test keys and certificates, gaining hands-on experience with the workflow.
- **Define credential types**: We then work together to identify the specific credential types required for each use case. CommScope assigns a corresponding **TypeID** to each credential type, enabling streamlined and consistent provisioning.
- **Integrate and validate**: CommScope supports the integration of the SDK into the customer's production flow or firmware update process. We also assist with pre-production trial runs to validate the end-to-end setup—helping to ensure a smooth, secured, and reliable deployment before going live.

6.2 Value Propositions for Infineon Customers

Our vision is to deliver scalable, streamlined solutions that enable Infineon to serve customers of all sizes across today's fragmented IoT landscape.

By consolidating multiple product variations (SKUs) into a unified offering, we reduce deployment complexity, making it easier for manufacturers to roll out devices in diverse environments while lowering operational costs. To support this unified approach, the platform

enables both factory-floor and over-the-air (OTA) provisioning, giving customers a consistent workflow for newly built devices as well as in-field retrofits. The OTA capability extends device lifecycles and helps safeguard installed bases.

The solution minimizes the attack surface, keeps private keys permanently out of reach, and aligns with evolving government regulations and industry standards. These attributes combine to provide an end-to-end foundation that allows Infineon—and its customers—to scale more confidently while staying secure.

In addition, the solution is delivered pre-integrated and fully tested, helping customers reduce development time and cost, achieving production efficiency, and accelerating their products to market.

7 Conclusions

In today's evolving IoT landscape, secured credential provisioning is no longer optional—it's a foundational requirement. As this white paper has shown, device manufacturers face mounting challenges from rising regulatory demands, increasing production complexity, and growing cybersecurity threats. Traditional approaches to key injection and certificate management often fall short, introducing vulnerabilities and operational inefficiencies that are difficult to manage on a scale.

The joint solution from Infineon and CommScope directly addresses these challenges by combining Infineon's robust OPTIGA™ Trust M with CommScope's scalable PKIWorks® provisioning platform. Together, we deliver a flexible, factory-to-field provisioning solution that enables strong device identity, minimizes attack surfaces, and drastically reduces the risk of credential duplication. Through the use of PKI TypeIDs and mutual authentication anchored in hardware-based trust, this solution empowers customers to ship a single hardware SKU and dynamically define multiple PKIs with tailored attributes for specific deployments or applications—accelerating time to market while maintaining end-to-end trust.

Ultimately, this collaboration offers more than just technology—it offers a path to greater operational simplicity, regulatory readiness, and long-term security assurance across diverse IoT deployments.