IoT Device Management - How to Achieve Trusted Factory Provisioning

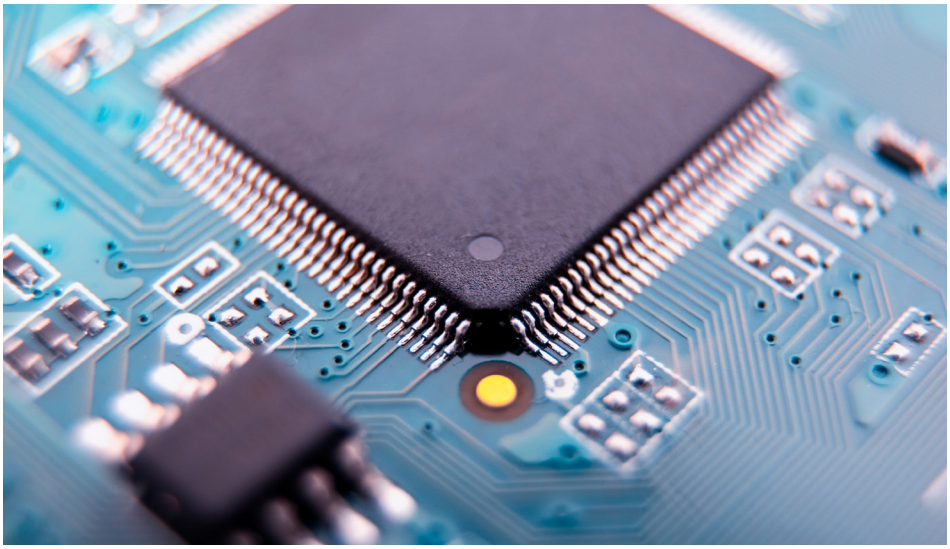
Removing Complexity and Instilling Security and Scalability in IoT Devices

November 2019

The unprecedented growth in IoT (Internet of Things) deployments are a growing target for cybercriminals; exposing individuals, their data and their infrastructure to risk if the threat of attack remains unaddressed.

A deployed device moves through several stages during its life cycle as it progresses from deployment, to regular use, and periodic updates to eventual retirement. Each of these stages pose a new risk to an unsecured device as attack methods can vary. For example, tactics employed during a mid-life update campaign will differ to the methods used to hack a retired device. Threat mitigation at each phase of a product's life begins with a robust factory provisioning process that forms the basis for a secure device life cycle as it provides the protocol and certification to ensure that all future interactions between an IoT device and its management platform remain secure.

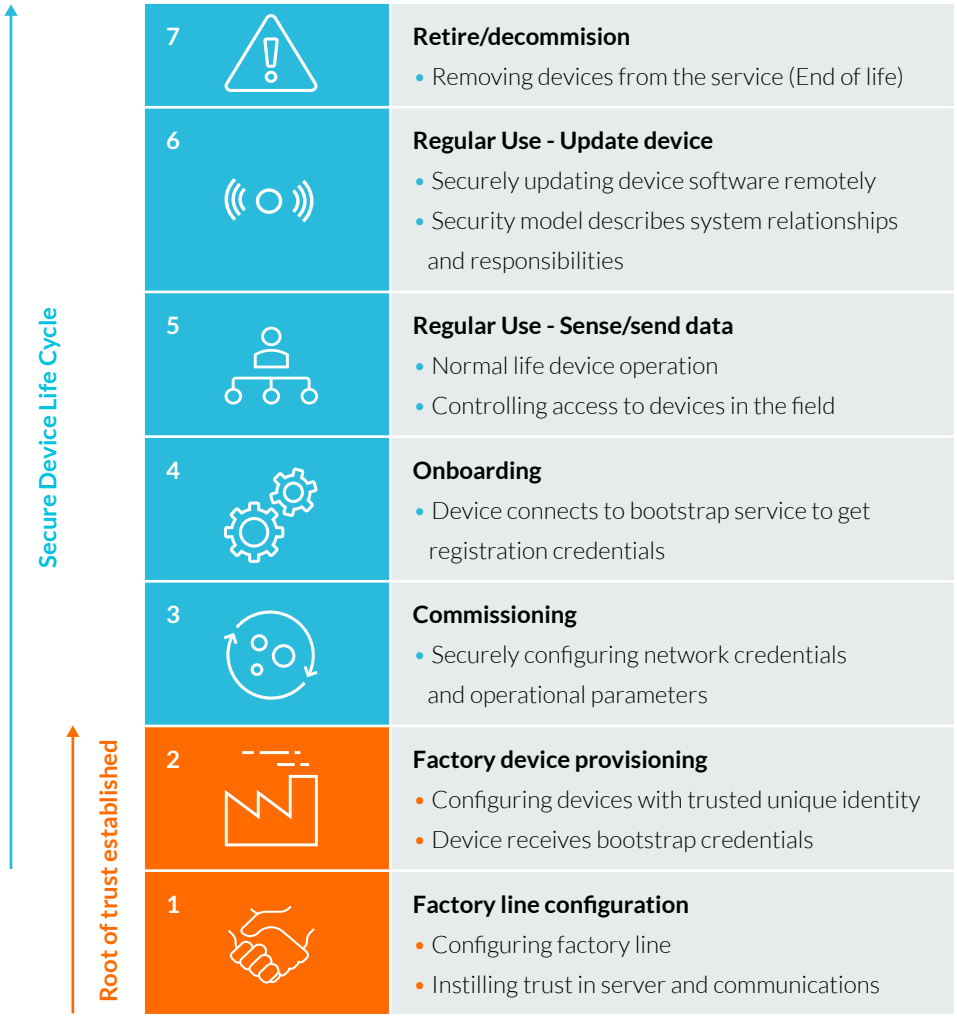
The complexities of mitigating this spectrum of threats has the potential to inhibit the deployment of devices on a larger scale, but the adoption of a device management platform and adherence to some key principals can ensure a secure baseline, scalability and operability for a device's working life.



Factory Provisioning: Forming the Foundation for a Secure Life Cycle

Pelion Device Management is an IoT Platform that provides a secure foundation for disparate IoT devices types, promoting scalability, whilst reducing complexity and time to market. A device manufactured without security remains insecure for the remainder of its working life regardless of the management, updates and security measures that follow. Injecting credentials on to a single device can mitigate this risk, but the ability to scale device identity to millions of devices is key to maintaining the balance between efficiency and security, which is why the following best practice is recommended:

Factory provisioning providing the baseline for a secure device life cycle



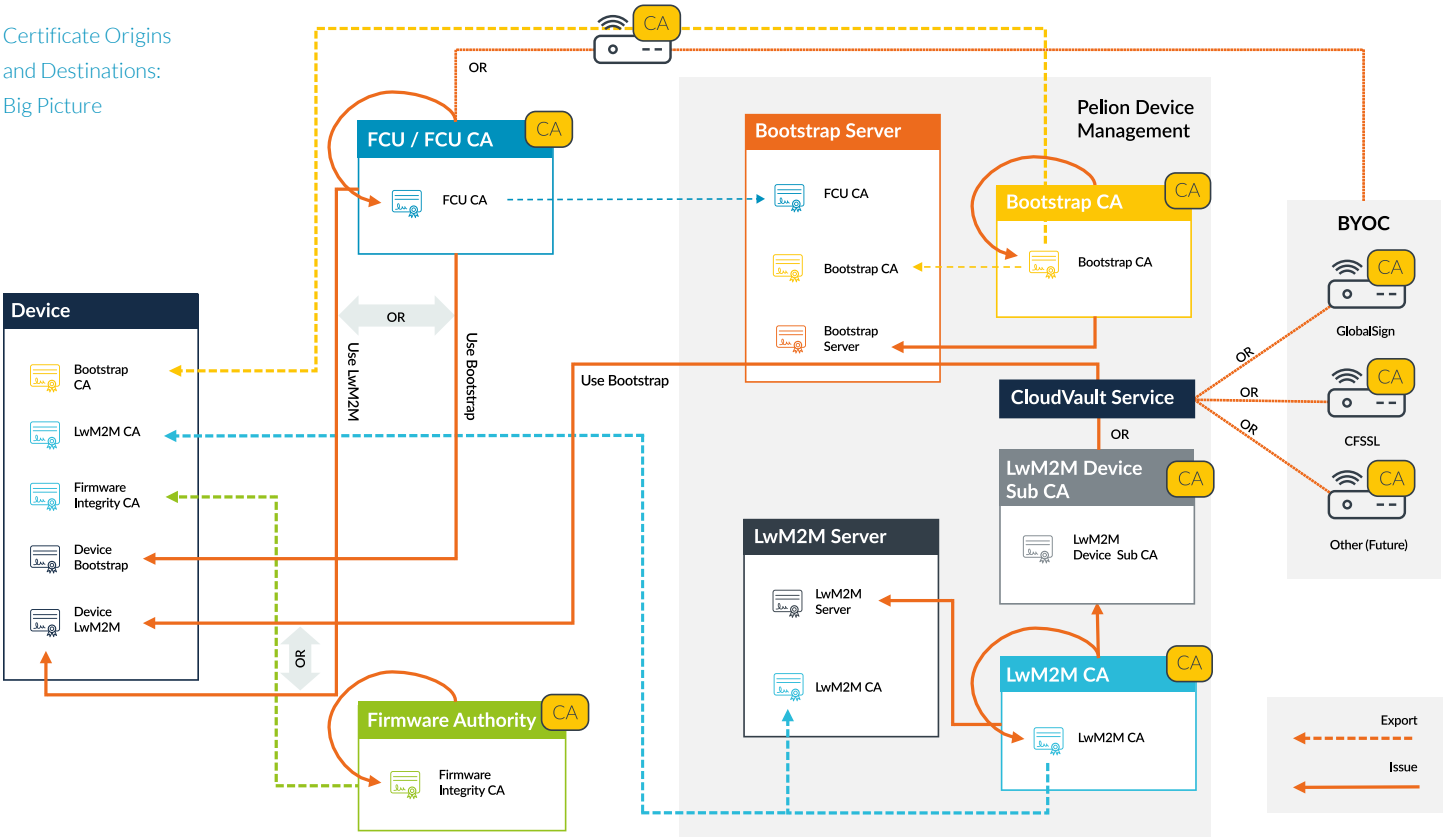
Commissioning a secure factory line and developing trust in server creates attestation that underpins the device provisioning stage by creating a foundation that allows a trusted unique ID and bootstrap credentials to be assigned to a device.

Each stage builds upon previous actions to ensure integrity as a device progresses from creation to retirement, and whilst Over the Air (OTA) Updates ensure a global estate of devices remains protected from the latest threats, how can we be certain that update is trusted? Factory provisioning ensures a reliable baseline of in-built device credentials to secure OTA updates, and secure commissioning in the field.

Production facilities, the devices they produce, and their supply chains are diverse, which means there is no 'one size fits all' solution that provides all factories producing IoT nodes with a secure foundation for their life cycle as it would be incredibly constrictive and inefficient. Luckily, Pelion Device Management offers enterprises and original equipment manufacturers (OEMs) clear, flexible templates and tools for instilling trust at provisioning and update stage without adding complexity, or constricting output and preferred distribution methods.

Incorporating a Public Key Infrastructure (PKI) and public key encryption as part of the provisioning process ensures that a deployed device is trusted by the Device Management platform and enables Device Management to authenticate devices when they attempt to connect to a manufacturer's account. Provisioning these credentials to your devices in the factory enables them to trust a device management platform and enables a platform to authenticate devices when they attempt to connect to a specified account.

Certificate Origins and Destinations: Big Picture



Instilling Trust in the Factory Line

How can a manufacturer or OEM be sure if the initial connection between two uninitiated entities is secure? If chip to data security is to be maintained a root of trust needs to be established across three facets:

1. Instilling Trust at Server Level

In order to communicate in a secure manner, certificates and keys need to be injected into the device which allows identification and verifies that the LwM2M server is trusted. This process of obtaining credentials is carried out by using verification provided by either Pelion Device Management or the manufacturer's own authority. Whilst both options are perfectly viable, Pelion offers a more streamlined approach to securely producing keys and certificates.

2. Instilling Confidence in Communications

Industry-standard Transport Layer Security (DTLS) not only acts as a cryptographic protocol, it also removes the need for cumbersome and insecure passwords. This is because the act of presenting a signed certificate which includes the subject name provides Pelion accounts with a validated unique device I.D, removing the need for other forms of identification.

3. Instilling Trust during Firmware Updates

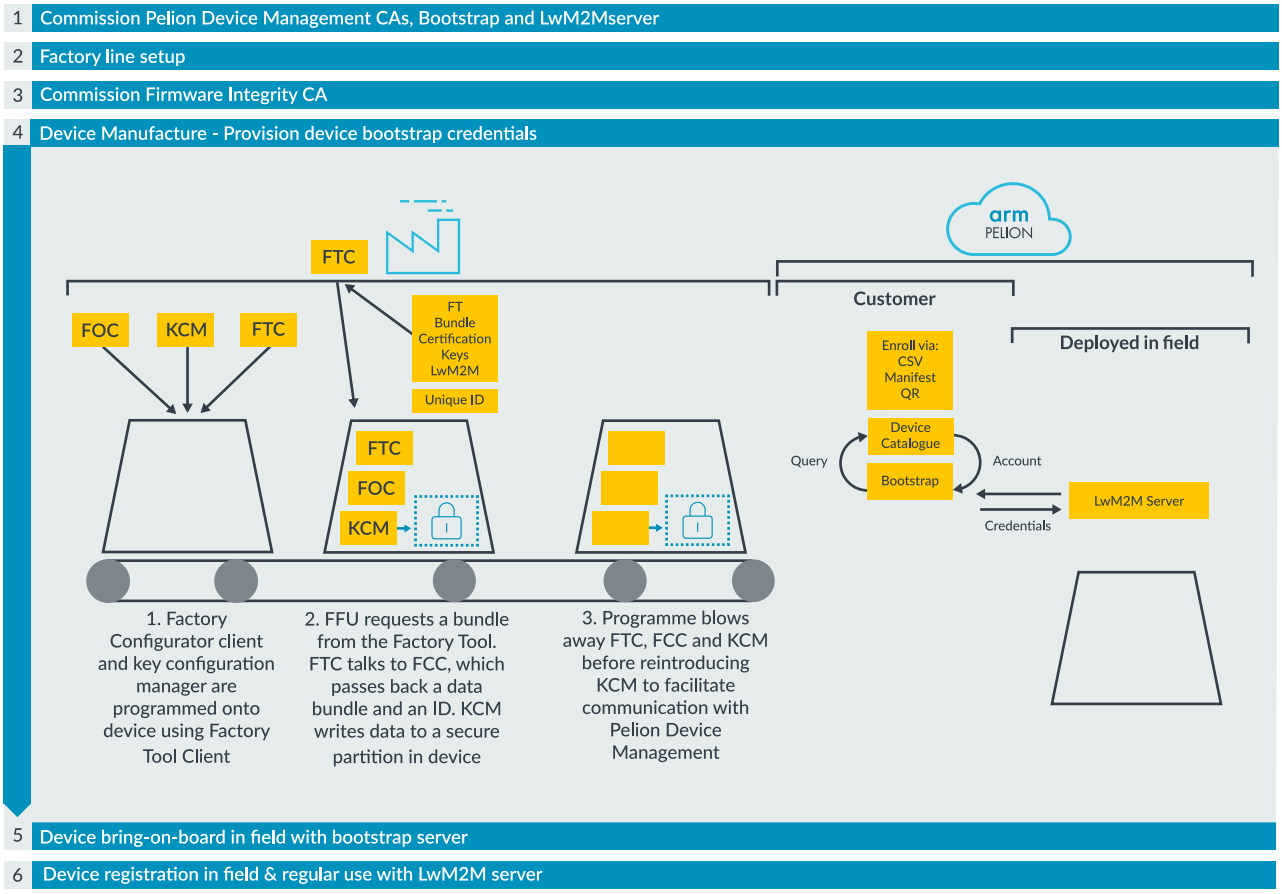
Injecting certificates and keys onto the device creates root certification and a chain of trust that allows any subsequent actions to be authenticated. Pelion can act as a certificating authority that generates keys and certificates on your behalf if required.

Preparing a Production Line for Provisioning

The act of configuring the factory instills trust at root by administering certificating authorities that cross-reference Pelion, Bootstrap and LwM2M servers. This set up requires some certificate authority (CA) configuration, which is why Pelion offers clear processes for factory configuration and a range of CA configuration tools to prepare your organization for efficient production of secure IoT devices.

An overview of the factory commissioning process

1. Commission Pelion Device Management CAs, Bootstrap and LwM2Mserver
2. Factory line setup
3. Commission Firmware Integrity CA
4. Device Manufacture - Provision device bootstrap credentials
5. Device bring-on-board in field with bootstrap server
6. Device registration in field & regular use with LwM2M server



The diagram above outlines how these components are programmed into the device on the production line and how features like DTLS, FCU and, FCC facilitate secure, scalable factory provisioning.

The Pelion device management service only establishes connections to devices that have certificates signed and trusted by the CA, which requires uploading a CA certificate containing the CA's public key before a connection between a device and Pelion can be established. Once the CA is configured and linked to the manufacturer's Pelion account the factory line is ready to provision devices.

This four-stage provisioning process involves:

1. Injecting the software image, which includes the KCM and FCC modules onto the device.

2. Generating device keys, certificates and configuration parameters for the device.

3. Using the factory tool to inject the generated keys, certificates and configuration parameters to the device on the manufacturing line.

4. Using the KCM and FCC APIs in the device to validate the information, before finalizing the provisioning process and blocking the FCC code in the production image.

Provisioning information

Some information is required to ensure a successful connection and this bundle of parameters also helps automate subsequent device configuration within Pelion device management.

Provisioning Information Bundle (When using a bootstrap server)

General Device Information	Communication Configurations	Update Authority	Ownership Claiming (or 1st to claim)	Secure Device Access
• Endpoint name • Entropy • Verify Device Configuration on Device • LwM2M Device Object • Model Number • Serial Number • Device Type • Hardware version • Memory Total Size • Time Synchronization • Device Current Unix Time (UTC) • Time Zone of the Device • Offset of the Device Time Zone from UTC Time Synchronization	• Bootstrap Configuration • Bootstrap Server URI • Bootstrap Server CA Certificate • Bootstrap Device Certificate • Bootstrap Device Private Key	• Update Auth. Certificate • Vendor ID • Device Class ID	• First to Claim • Device Enrolment ID	• Trusted Anchor Public Keys

This information is required for the factory process regardless of whether the manufacturer opts to utilize Pelion's FCU. Full supporting documentation on how to correctly format the data bundle for swift configuration can be found here. This information also serves as a reference when debugging the parameter generation process at a later stage.

Deployment methodology and provisioning protocol will differ depending on a manufacturer's supply chain. Thankfully, Pelion Device Management provides different ways of onboarding and connecting a device to the cloud. Which means that the communication/configuration element (detailed in column two of the above provisioning bundle) also has an effect upon how certificates are renewed, and connections are maintained.

More detail relating to device onboarding and connection options can be found here.

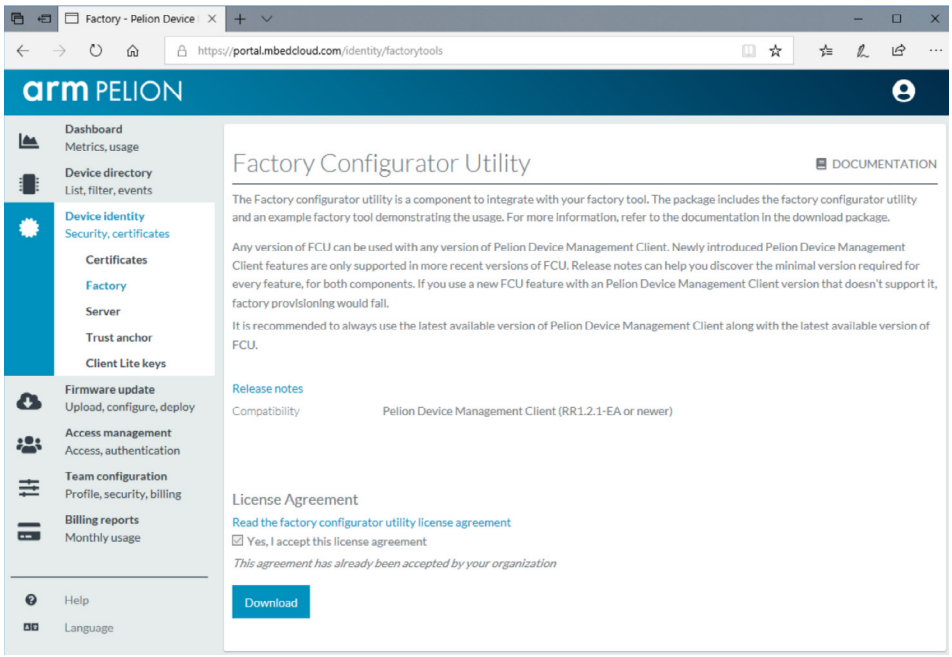
Provisioning Considerations & Flexibility

The simple act of injecting credentials on to a single device can be relatively simple, but the ability to scale this process to the millions of devices is key to maintaining the balance between efficiency and security for not only manufacturers, but also OEMs who are one step removed from the end user and may require additional provisioning flexibility. This can be achieved by two main methods. Firstly, some OEMs prefer to create their own keys and certificates, before bundling them in Pelion's FCU, which is essentially a Python library used to configure and validate device parameters. However, some OEMs may choose not to use the Pelion FCU at all and inject data directly into the device. But using the FCU for the generation of DTSL keys and certificate is by far the most efficient method as generation and bundling of keys and certificates is administered automatically by the FCU. It's this preferred automated process for factory provisioning that we will be focusing on when considering how a device's ownership is claimed.

Preparing for Device Provisioning

Now that the factory itself is configured to provision secure devices, a manufacturer or OEM can rely upon several readily available tools to expedite the provisioning process. These tools require some preparation before device provisioning can begin.

Pelion's open-source Factory Provisioning Tools (FPT) accepts the factory-configured data and stores it within the device during factory provisioning. Later these credentials are used to connect to Device Management Services. This allows the manufacturer to program the software image and then configure the device's parameters:



A. The factory configurator utility (FCU) sits within the factory line and works alongside the manufacturer's factory tool to configure and inject a device with the credentials required for connecting the device to Pelion device management, plus generate and inject keys and certificates in the factory line.

B. Pelion's factory configurator client (FCC) ingests credentials prepared by the FCU and passes this data into the key and configuration manager (KCM) which stores the keys and certificates securely.

Claiming device Ownership

Devices need to be connected to an owner account within Pelion, however, the owner may not always be known at the point of production, plus there is also a strong chance of ownership changing during a device's lifetime which also necessitates account administration post-deployment. Which is why Pelion device management offers two options for assigning devices to an account:

1. Pre-assigned management is typically used when the manufacturer knows who will be using the device in the field. This process automates account assignment during the manufacturing phase, so a device leaves the factory pre-assigned to a unique account. In this scenario, the factory floor provisioning includes account identification in the bootstrap configuration, which associates the device with a specific account. This option is preferred by manufacturers producing their own devices and therefore know which account the devices need to connect to.

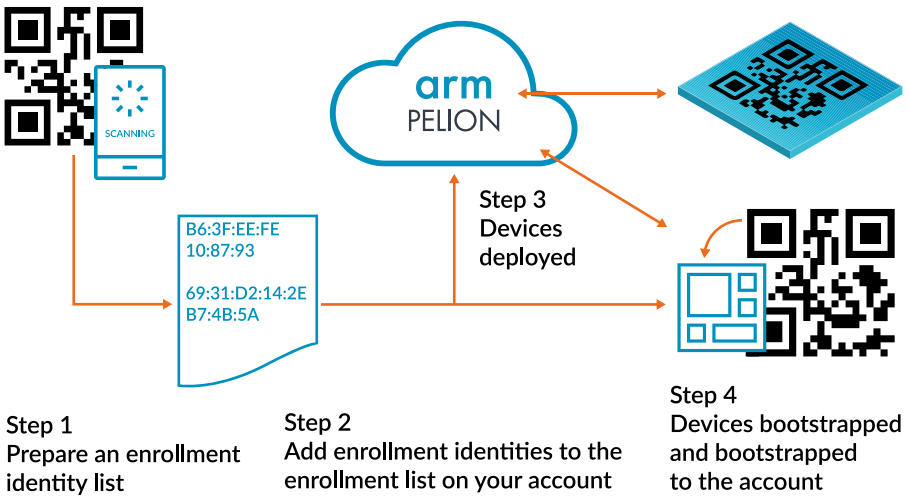
2. First to Claim (Via an enrolment list) is a Pelion feature that allows flexibility for manufacturers and OEMs by not provisioning a device with account identification during the production phase. Instead, a device is assigned with an enrolment identification that can be used to be claimed by an account at a later date. This flexibility enables:

    - A device owner to assign a device to an account post-production
    - An OEM to manufacture a device that can be registered by third parties at a later date
    - The transfer of ownership if sold post-deployment
    - A range of options that help strike a balance between security and logistics

First to Claim Device Ownership and Identification Process

A 'virgin' device leaves the factory without an assigned account, the owner claims device ownership by adding the device identifier to the Pelion enrolment list before shipment takes place. Pelion recognizes the deployed device trying to connect has no assigned account, it verifies the unique ID to match the credentials to the enrollment information in a specific Pelion Device Management account, the device is then assigned to the account.

Providing device identities to Pelion



Pelion needs the device ID to match the ID uploaded into the Pelion Portal, flexibility is provided by supporting several methods for uploading these unique identities. The unique identifier generated by the factory could be batch uploaded via:

- CSV upload
- NFC
- RFID tag
- QR code
- Device GUI
- A simple manifest contained within the shipment packaging

Whilst providing this level of flexibility, Pelion maintains security during the unique identity upload at the bootstrap stage, the interaction takes place as part of the data transfer with the Bootstrap Server over encrypted DTLS communications.

Pelion enables the transfer of ownership at any point in the device's life cycle by the original owner releasing the device from their account in the Pelion Portal. This initiates a factory reset, allowing the new owner to enroll the device once more.

Conclusion

Forward-thinking enterprises and OEM Manufacturers are capitalizing upon the profitability and revenue opportunity presented by burgeoning IoT deployments. Yet the speed and scale of this growth presents significant opportunities to cyber criminals as the attack surface increases with each device deployed. This means an increasing number of organizations are assessing how secure provisioning impacts production efficiency, flexibility and ultimately, profits.

Pelion Device Management's range of flexible tools and supporting documentation allow organizations to swiftly configure a factory line to efficiently provision connected devices with the means to remain secure in subsequent stages of a device's life cycle without compromising on production methods or profit.

Further information on the factory provisioning process and how Pelion Device Management provides a secure foundation for your IoT deployments please head to https://cloud.mbed.com/docs/current/provisioning-process/index.html

arm