A Use Case Concerning IoT Device Management

Technology Working Group

Industrial Internet Consortium

Shi-Wan Lin

shi-wan.lin@intel.com

Robert Lembree

robert.Lembree@windriver.com

In an Industrial Internet network, there are many devices with sensors and actuators of various kinds. These connect to each other, to other smart devices, to gateways at the edge, as well as to public clouds or private/on premise services (which we'll refer to as "fog"). The volume of the devices to be deployed is necessarily very large, the environments into which they will be deployed will vary greatly, and the geographic locations of deployments can be highly disperse.

The success of the industrial internet depends heavily upon how easily these devices can securely connect with each other, and be managed by the next tiers of elements in the IoT systems.

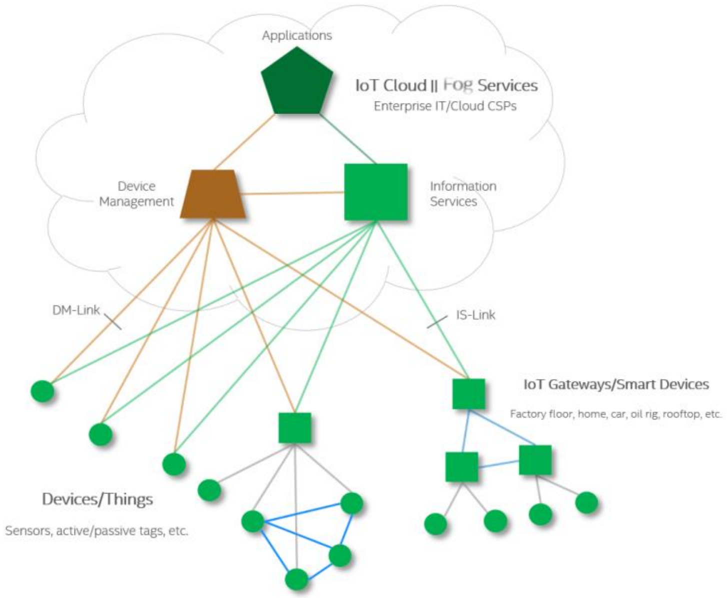
Each of these elements, sensors, actuators, devices, edge gateways, and cloud/fog services, will be provided by a variety of manufacturers as well as product and service providers. It is thus imperative for the industry to develop and deploy a common industrial internet architecture framework and a common reference architecture from which the interactions of the elements in an IoT system can be standardized.

With a widely adopted and implemented standard, we expect that any device from any manufacturer can readily connect to others, to the next tier of edge gateways, and to cloud or fog services, regardless of vendor.

To this end, we use this usecase as *a starting point* to discuss a specific and important aspect of the interactions between the devices, edge gateways and cloud/fog services: device management. As a starting point of discussion, this architecture view and the scenarios in which the interactions are described are not meant to be complete and comprehensive.

A simplified architecture of an IoT system can be depicted as follows:

1. Devices deployed in the fields, factory floors, homes, transportation vehicles, vessels and crafts, etc., connect to each other, to the edge gateways and to the cloud/fog services;
2. Edge gateways connect to the devices, other edge gateways and to the cloud/fog services;
3. Cloud/fog services connect to devices, edge gateways, and other cloud/fog services.


Applications
IoT Cloud || Fog Services
Enterprise IT/Cloud CSPs
Device Management
Information Services
DM-Link
IS-Link
IoT Gateways/Smart Devices
Factory floor, home, car, oil rig, rooftop, etc.
Devices/Things
Sensors, active/passive tags, etc.

There are many possible interactions/links between the IoT elements. We are focusing this discussion on two important interactions as denoted in the diagram as Device Management (DM)-Link and Information Services (IS)-Link.

The Device Management component is concerned with:

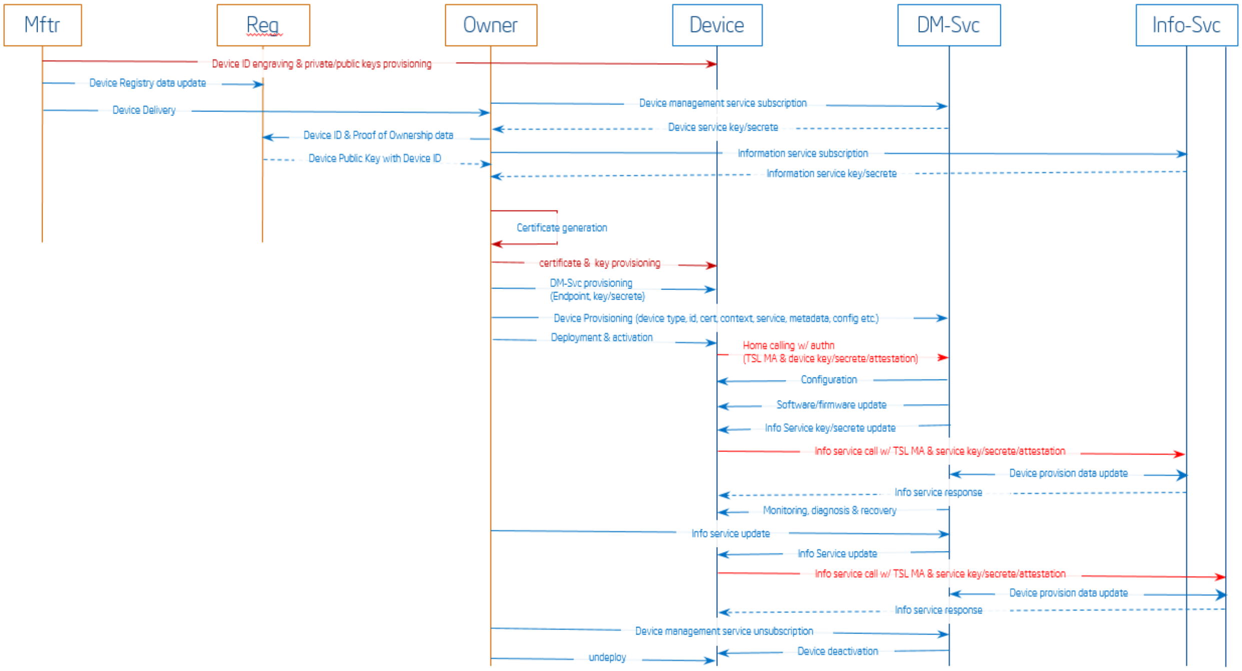
1. In-factory provisioning, e.g. device identity and cryptographic keys – the keys are used to protect the device identity and to secure the communications to other entities;
2. Device ownership and data governance and policy management;
3. Device owner provisioning, e.g. assigning X.509 certificates and other keys to the devices – these keys may be required to connect the devices to other elements or services in the network;
4. Device Management Service subscription and provisioning for the devices;
5. Device deployment, activation and onboarding to the IoT network;
6. Device automatic configuration;
7. Device firmware and software automatic update;
8. Device monitoring and automatic diagnosis;
9. Device de-provisioning, deactivation and un-deployment;
10. Other device management functions.

The Information Services component is concerned with:

1. Authenticating devices connecting to its services; it may rely on device services provided by the Device Management to accomplish this task;
2. Receiving, verifying, transforming, processing and storing data received from the devices;
3. Perform analytics of data gathered from the device and other sources;
4. Provide services to application to consume the device data and the result of analytics;
5. Other information services.

We foresee that the Device Management and the Information Services can be implemented by the same service provider or offered separately. In the former case, some interactions described above can be streamlined. However, the Device Management and Information Services functions are still distinct and best to be implemented as different modules. It is also a possible scenario that a device is managed by one Device Management Service, but sends data to multiple Information Services. In this scenario, it is foreseeable that the Device Management Service may serve as a marketplace for devices whose data can be sent live to a number of Information Services that require them. For example, our weather station in the use cases below could be providing data to the National Weather Service as well as wunderground.com. Similarly, an ADS-B receiver could supply data to both Flightradar24.com and Flightaware.com. Such a one-to-many relationship requires that there be an established trust relationship between the information consumers and the device management organization. For the sake of simplicity however, we leave out the function of command and control (actuation) in our discussion for now.

The following is a sequence diagram depicting interactions of potential actors in the lifecycle of a device, from being added to, and removed from an existing IoT network. It assumes that SIM cards are not used in this example. This is not intended to be a description of a solution to the Device Management problem but rather to highlight the many interactions that we must consider and must look into standardization for the broadest interoperability for all the devices, gateways and cloud/fog services.


Mftr
Reg
Owner
Device
DM-Svc
Info-Svc
Device ID engraving & private/public keys provisioning
Device Registry data update
Device Delivery
Device management service subscription
Device service key/secrete
Device ID & Proof of Ownership data
Information service subscription
Device Public Key with Device ID
Information service key/secrete
Certificate generation
certificate & key provisioning
DM-Svc provisioning
(Endpoint, key/secrete)
Device Provisioning (device type, id, cert, context, service, metadata, config etc.)
Deployment & activation
Home calling w/ authn
(TSL MA & device key/secrete/attestation)
Configuration
Software/firmware update
Info Service key/secrete update
Info service call w/ TSL MA & service key/secrete/attestation
Device provision data update
Info service response
Monitoring, diagnosis & recovery
Info service update
Info Service update
Info service call w/ TSL MA & service key/secrete/attestation
Device provision data update
Info service response
Device management service unsubscription
Device deactivation
undeploy

Here we will not discuss how the Device Management Service and the Information Service establish trust and communicate securely since there are proven common practice for this between two cloud or cloud-like services. We will not elaborate on the trust establishment and secure communication between the device and the Information Service once a device has been successfully connected and provisioned into the Device Management Service either. We want to focus on a secured process of onboarding of a new device into a Device Management Service.

There are existing industry standards governing device management. For example,

1. OMA-DM – Open Mobile Alliance – Device Management, a Working Group (WG) that specifies protocols and mechanisms to achieve the management of mobile devices, services access and software on connected devices. Recently this WG has extended their scope of work with the OMA Lightweight M2M protocol, which focuses on constrained cellular and sensor network M2M devices.
2. **TR-069** (Technical Report 069) - Broadband Forum (formerly known as DSL Forum) technical specification entitled *CPE WAN Management Protocol* (CWMP) for remotely managing Customer-Premise-Equipment (CPE) using bidirectional SOAP/HTTP protocols through broadband fixed network.

Both specifications cover many common functions concerning device management and use similar communication technologies, e.g. XML/HTTP/SSL to realize these functions. However, OMA-DM is for managing mobile devices and TR-069 fixed network devices. However, IoT devices may use mobile or fixed or both networks for communications. Many IoT devices are constrained in both processing and networking capabilities. The creation of a common Device Management framework and standards for IoT devices are an important and challenging topic. If and how to leverage existing device management specifications such as OMA-DM and TR-069 for IoT device management is an open question.

Use Cases

The following use cases use a weather station as their example. For the purposes of this set of use cases, the weather station is considered to be part of a widely spread weather gathering network, where member stations are in potentially vulnerable locations and subject to tampering. The data provided by the member stations is considered to be valuable. Here are some examples:

- If the weather network was part of an airport weather monitoring system, a hacker could inject false data that would effectively result in a denial of service attack on the airport itself, where air traffic would be diverted to avoid weather phenomena that do not truly exist.
- In a deployment over agricultural lands, an attack could result in crops damaged by incorrect assessment of rainfall.
- In a deployment as part of tornado warning system, malicious intent could lead to false tornado warnings.

These examples illustrate that the network and its data needs to be protected from tampering or being spoofed, so efforts are put into network access control and station authentication.

Also, for the purposes of these use cases, we should assume that boot security is in place so that sophisticated attempts to spoof the hardware can be thwarted.

For the use cases, we envision using either MQTT, or XMPP with XEP-0295 (JSON Encodings for XMPP) to communicate, but the model is not dependent upon either.

Device Management/UC007-1: Weather station manufacturing	
Vignette	Weather station is manufactured and engraved with its unique identity
Actor	weather station under factory provisioning (unit)

Event	Unit is assembled and powered on for the first time
Pre-/Post-Conditions	Pre: Unit has been assembled and initial firmware/software load completed Post: Unit is packaged and ready for installation
Technology	
Fit Criteria	
Scenario	1. Completed unit is connected to a factory network and switched on 2. Unit boots into “factory new” mode 3. Unit generates a public and private key pair using some factory-provided entropy 4. Unit stores its private key in tamper-proof on-die secure storage 5. Unit sends its public key and hardware serial number to a secured server 6. Unit encrypts a known format test message with its private key and sends it to the server, which then decrypts and validates the message. 7. Server then indicates that engraving is complete and unit is released to be packed.

Device Management/UC007-2: Weather station installation	
Vignette	Weather station is unpacked, installed and makes its first contact with a server
Actor	weather station under installation (unit)
Event	Unit is powered on
Pre-/Post-Conditions	Pre: Unit has been unpacked Post: Unit has been connected to the network and is operational.
Technology	
Fit Criteria	
Scenario	1. Unit is unpacked, installed, and switched on for the first time outside the factory 2. The serial number of the unit has been provisioned into the weather network service out of band 3. Weather station contacts its pre-configured server over a mutual authentication TLS secured connection and also proves its ownership of the identity 4. The server, having seen an authentic introduction, instructs the station that it is now online, and to begin reporting.

Device Management/UC007-3: Weather station software update becomes available	
Vignette	Weather station is notified that a software upgrade is available and performs its upgrade
Actor	Communicating weather station (unit)
Event	Unit has been installed and functioning, but is notified that it needs a software upgrade
Pre-/Post-Conditions	Pre: Unit is installed and functioning Post: Unit is functioning with a new version of software
Technology	
Fit Criteria	
Scenario	1. Unit is functioning 2. Unit receives a message that an update is available, including a timeframe in which is expect to take action 3. Unit reaches a point at which updating is convenient 4. Unit starts update 5. Unit completes update 6. Unit restarts and reports that the update is complete

Note: other use cases are relatively straightforward and similar to UC007-3 above and are not discussed further.