

# Zero Touch Provisioning—Approaches to Network Layer Onboarding

Mini TT

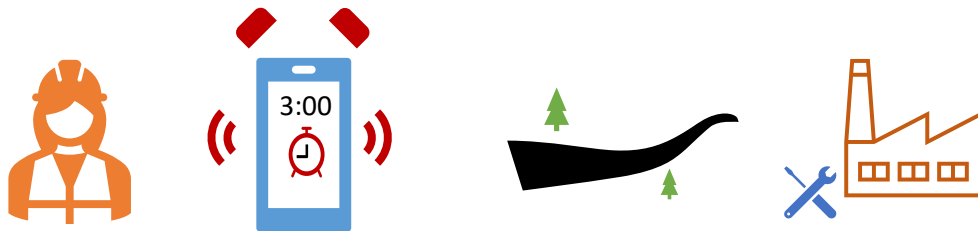
[Mini.tt@Dell.com](mailto:Mini.tt@Dell.com)

**Abstract:** Zero Touch Provisioning generally refers to the methods of configuring hardware devices when they are added to a network. With ZTP, the need for an expert to provision hardware devices is reduced. In addition, this mechanism reduces the risk of human error and speeds up network setup. One specific aspect of ZTP is certificate provisioning in the operational environment. This article discusses the challenges of certificate provisioning and various industry initiatives towards ZTP. Considerations for ZTP in different environments and evaluation of various approaches to suit the characteristics of the environment concludes this article.

**Keywords:** Zero Touch Provisioning, Voucher, Device Identity, Supply Chain Security

## Introduction

It is 3 am in morning. The alarm goes off. The maintenance engineer wakes up with a jolt from a deep sleep and checks the alarm on the mobile phone. On seeing that it was 3 am, she was worried. She was certain in her mind, even in those early hours, that she did not keep a wake-up alarm for 3 am. Then, why the alarm!!! Ah! This is the alarm from the control system that she is responsible for maintaining. She checks the details of the alarm and understands that she probably may have to replace the instrument. She gets ready quickly and goes off. Indeed, the instrument needs a replacement. She gets to the storeroom for a spare, gets one and tries to replace the faulty one. On replacing, she was perplexed by the many scary acronyms that came up on the screen. She was confused, not knowing what to do with the term AES, ECC, P256, CSR and a whole lot of acronyms. Is there a way that is just replacing the faulty one with a new working instrument just works without having to deal with the certificate related acronyms?



*Figure 1: 3:00 am service by a security novice*

This article talks about solutions to deal with the situations as above without having a maintenance engineer with expertise in setting up digital certificates; the maintenance engineer need not even have to be aware of the certificate exchanges. The system has the awareness to accept a device if it is genuine. Similarly, the Device has the awareness not to join the network if the network is not what it is intended to join to, and all these happen in a zero-touch manner.

During the device onboarding phase to a network, there are various stages of onboarding performed. Among them are network layer onboarding, Identity bootstrapping, application onboarding and configuration onboarding. Depending on the deployment scenario, there could be other domain-specific onboarding steps. This article discusses Identity bootstrapping solutions. When a device is manufactured, the manufacturer provides an initial Identity, which is in the domain of the manufacturer.

During the life of the Device, onboarding may have to happen many times due to various reasons such as a security breach, maintenance, patches and updates, device repurposing, device resale. NIST paper[1] on device onboarding talks about characteristics that are of interest to manufacturer, service provider and end user. Table 1 list the security characteristics of interest that are discussed in this article.

*Table 1: Security characteristics*

Characteristic	Description
Device Identity	Unique Identity of the Device, specific to each instance. This Identity is cryptographically bound to the individual instance of the Device

Device Authentication	Verification that the claimed Identity of the Device is its actual Identity
Trust Anchors	Elements that security depends on. If the trust anchor is compromised, security is undermined
Network Authentication	Verification that a claimed identity of the network is its actual Identity
Device Attestation	Proof that specific device elements have not been tampered with
Secure onboarding	Locally significant, Device specific credentials are provisioned automatically
Proof of ownership	Verification that a device has a specific owner
MUD	Manufacturer Usage Description

## Identities

A Device Identity is any information that is used to identify the Device and distinguish it from other devices. Strong device identities are those that can be cryptographically verified. They are not easily spoofed, modified or copied.

Some examples of strong identities are:

1. DevIDs as described in IEEE 802.1AR[2]. A DevID comprises:
  - A DevID secret that is the private key portion of a public-private key pair.
  - A DevID certificate containing the corresponding public key and a subject name that identifies the Device.
  - The certificate chain from the DevID certificate up to a trust anchor contained in the DevID trust anchor store available to potential authenticators.

There are two types of DevIDs described by 802.1AR—IDevID and LDevID. IDevID provides information to establish the manufacturer of the Device. These are created before the Device is supplied to the customer. LDevID is a locally significant DevID in the domain of operation of the Device. The process of provisioning obtains an LDevID for the Device in the customer domain. These DevIDs are depicted in Figure 2.
2. DICE CDI from TCG[3]
  - Serves as Device Identity and facilitates attestation of the device firmware.
  - Derived from a Unique Device Secret (UDS) and the Identity of the first mutable code.
  - Implemented in hardware during manufacturing.
3. Direct Anonymous Attestation (DAA) Identity
  - a. DAA provides an irrevocable identity that is immutably written into processors that implement DAA.
  - b. In DAA, individual devices have unique group membership private key. Devices are authenticated as group members. Intel EPID[4] is one of the mechanisms for implementing proof of group membership.
4. Certificate based embedded subscriber identity module(eSIM)
  - a. eSIM[5] enabled remote SIM provisioning. eSIM is soldered inside the Device that can accommodate multiple SIM profiles.
5. Wi-Fi DPP capable devices
  - a. Wi-Fi DPP capable devices have a private bootstrapping key stored securely in them. As part of onboarding process, the Device is provisioned with unique credential which includes unique network access key for the Device.

Out of these identities, DevIDs offer multiple security advantages over others as it relies on digital certificates, and the Device themselves being capable of securely storing the Identity by secure elements.

This article discusses the use of DevIDs for securely onboarding a device. The proposed onboarding solution makes use of concepts like Manufacturer Usage Descriptions (MUD) vouchers[7][8]. A voucher artifact provides a mechanism to securely assign a device to an owner. For example, when a device is sold to a specific customer, the manufacturer of the Device provides a voucher to the customer so that the customer network can prove legitimate ownership of the Device. The Device uses this information to authenticate the network and makes decisions whether to join the network or not.

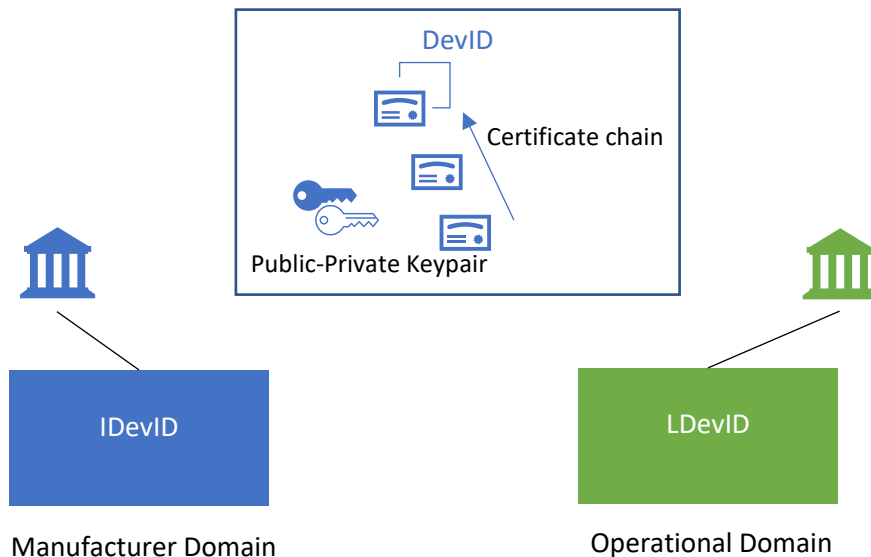


Figure 2: Device Identities

## Problem Statement

The problem addressed in this article is provisioning of network credentials to a device. The provisioning is performed when the Device is connected to the network in the operational environment. The Device is provisioned with a unique credential valid in the domain of operation. As part of the provisioning process, Device and the network have the opportunity to authenticate each other. During the provisioning process, human interaction is minimal, and access to credential is not given to humans.

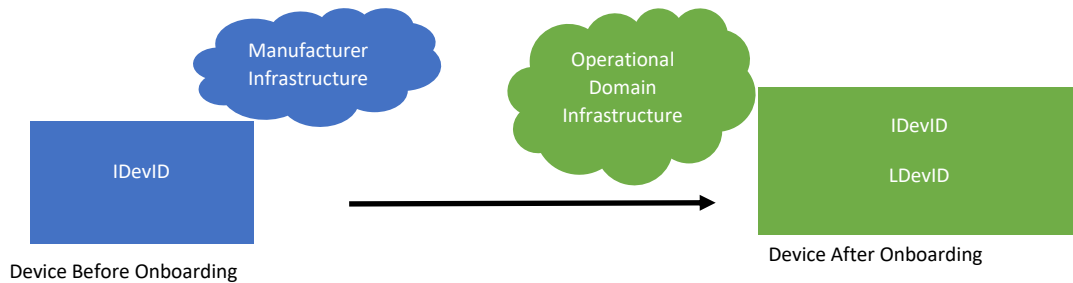


Figure 3: Onboarding Problem Statement

Figure 3 shows the onboarding scenario. At the end of the onboarding process, the Device obtains an LDevID, which it can use to communicate with entities in the operational domain. The following security requirements are proposed for the onboarding solution. The proposed onboarding solution in this article recommends a solution that aims to provide a foundation to meet these security requirements.

## Device Authentication

The Device asserts a specific identity and proves that the Identity is cryptographically bound to the Device. In the case where the device identity is an IDevID, the Device presents the certificate chain associated with IDevID and responds to a challenge to prove possession of the IDevID private key. Authentication enables the network to authenticate the Device before accepting it.

In situations where anonymous identities are used, such as in DAA, the Device may not be asserting a specific identity. Instead, it would be asserting to be a particular type of Device and proving a group membership.

## Device Authorization

Device authorization determines whether a device should be granted access to the network. The authorization decision may be based on authorization policies and device information.

## Secure Credentialling

This requirement identifies the purposeful step in the onboarding process. Secure credentialing provisions credentials such that it protects them from disclosure both while in transit to the Device and while stored on the Device. This is a mandatory requirement for any onboarding solution. This requirement identifies the primary goal of onboarding. The credentials thus obtained identify the LDevID of the Device, which is significant in the domain of operation.

These credentials allow the Device to communicate to the operational network. The network owner is in control of managing the lifecycle of these credentials.

## Network Authentication

Network authentication provides assurance to the Device that it is not connecting to a rogue network. Device verifies that the network identity is the Identity that the network claims it to be. The network onboarding component presents the Device with credentials bound to the network. The credential could be in the form of an X.509 certificate.

## Network Authorization

Network authorization determines whether a network is allowed to onboard a device. Network authorization decisions could be based on information provided in the device declaration, which identifies which networks are authorized to onboard the Device.




In addition to the requirements discussed above, a few of the additional requirements to consider for an onboarding solution include

- Maintainable Credentials
- Device Type Verification
- Device Attestation
- Proof of Ownership
- Secure Ownership Transfer
- Supply chain Assurance

## Applicable scenarios

This section discusses some of the applicable domains and scenarios where the onboarding solution is necessary. There are domain specific constraints to be considered while adopting the generic solution proposed in this article. Few of the domains of considerations are discussed.

Table 2: Applicable domains

Domain		
Consumer	Enterprise	Industry
		
Domain Characteristics		
Lack of expertise	Available IT expertise	Available OT expertise
Presence of internet	Internet present most of the time	Not on internet
Small number of devices	Many devices	Many devices
Needs Zero Touch	Desire Zero Touch	Needs Zero Touch
Retail Supply	Professional Channels	System Integrators

## Solution Approaches

A solution to secure zero touch provisioning requires multiple elements. Identities form the foundation of such a solution. Apart from device identity, a notion of home, where the Device or an entity on behalf of the Device can reach out to for gathering additional information about the Device is necessary. The approach to trust establishment based on the risk factors in the environment, feasibility based on supply chain complexities, and available infrastructure support is a critical dimension to consider. The approaches discussed in this article are based on Trust of First Use (TOFU) and Mutual trust establishment.

This section introduces the building blocks that would serve as concepts for these solution elements.

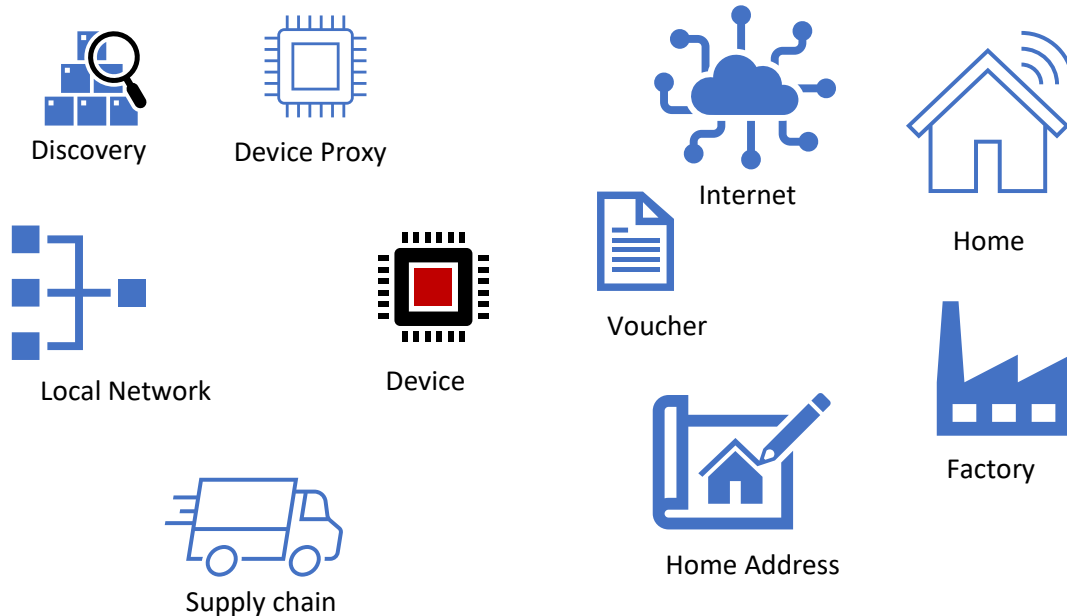


Figure 4: Involved elements in the secure zero touch scenario

### Home

Home is the notional ancestral home of the Device. In most cases, this is the manufacturer of the Device. The Device could obtain additional information about the properties of the Device by calling home. A sample realization of call home is by embedding a URI, which points to a service hosted by the manufacturer which provides additional information. The URI could be present in uniformResourceIdentifier field in subjectAltName field in an X.509 certificate. The URI could provide instance specific information about the Device, such as device voucher, and other life cycle specific information about the Device. The hosted service could also provide information about the device family, such as the latest version of the firmware, identified security vulnerabilities for the firmware present in the Device, a security status indicating whether the Device is currently having a version free of any known vulnerabilities.

During the provisioning process, the Device has not yet obtained local identities to establish communication with the local network. In most of the scenarios, the Device communicates with the local network in the normal operational scenarios. A device proxy in the network could act on behalf of the Device to call home and gather the information by obtaining the home address from the Device.

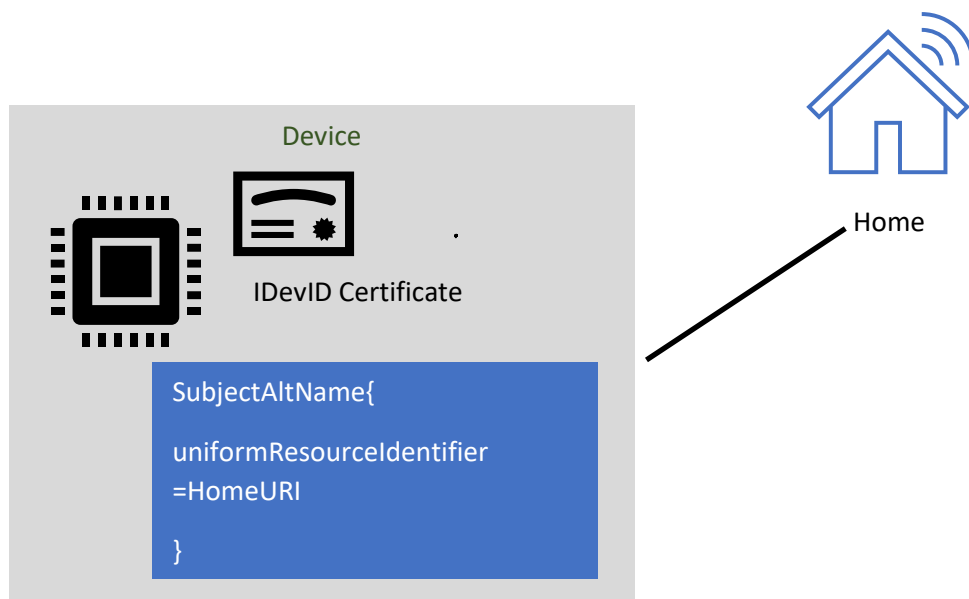


Figure 5: Home

### Trust on First Use

The principle of trust on first use was discussed in [9]. A duckling emerging from its egg will recognize as its mother the first moving object it sees that makes a sound, regardless of what it looks like: this phenomenon is called imprinting. Similarly, our Device will recognize as its owner the first entity that provides it with a credential valid in the operational domain. As soon as the credential is received, the Device is no longer a newborn and will stay faithful to its owner for the rest of its life. If several entities are present at the Device's birth, then the first one that sends it a key becomes the owner.

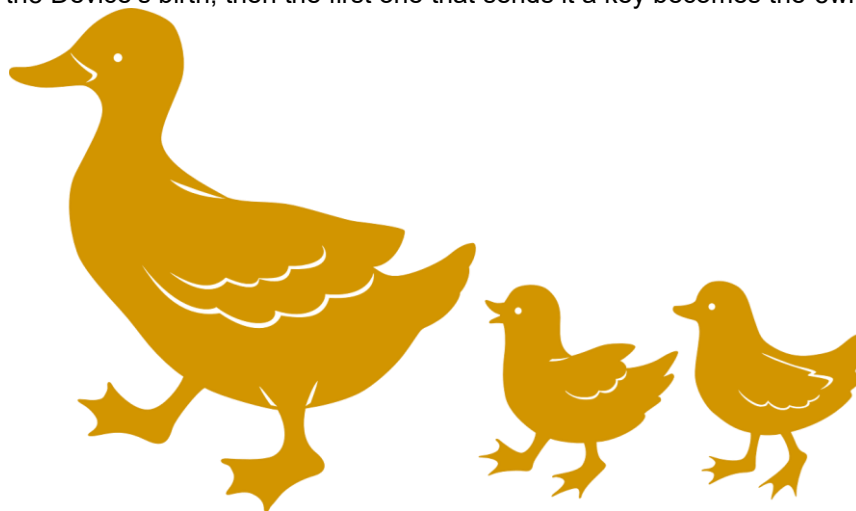



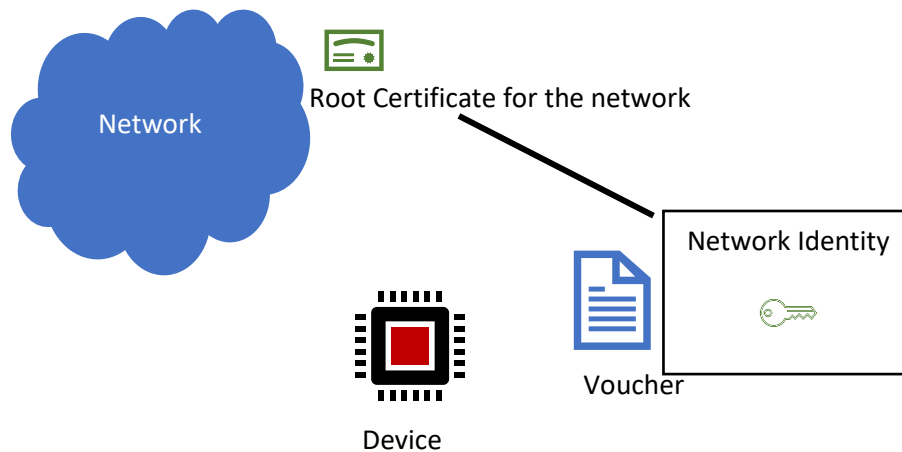
Figure 6: Trust on First Use

If it happens to be a wolf or a crocodile  that the duckling sees as the first moving object, there is a risk that the duckling will be eaten up. A form of this imprinting is seen in the character of Mowgli in the story, Jungle book.

*“So Mowgli went away and hunted with the four cubs in the jungle from that day on. But he was not always alone, because years afterwards he became a man and married.  
But that is a story for grown-ups.”*

## Two way Trust Establishment

When a two way trust establishment is done as part of the provisioning process, the risks associated with TOFU is absent. Here, the Device establishes that the network is trustable, in addition to the network establishing that the Device is genuine. The Device uses vouchers to identify the customer to whom the Device is sold to. This network identity is used by the Device to make decisions on whether to join the network or not. The network identity defines the trust domain. One realization of the network identity could be the root certificate of the network domain. The root certificate may be identified by the thumbprint or the hash of the root certificate node.



*Figure 7: Network Identity in the voucher*

In larger enterprises where the same Certificate Authority is used for the entire enterprise, the certificate hierarchy could be organized as segments where the Device could join a segment of the network.

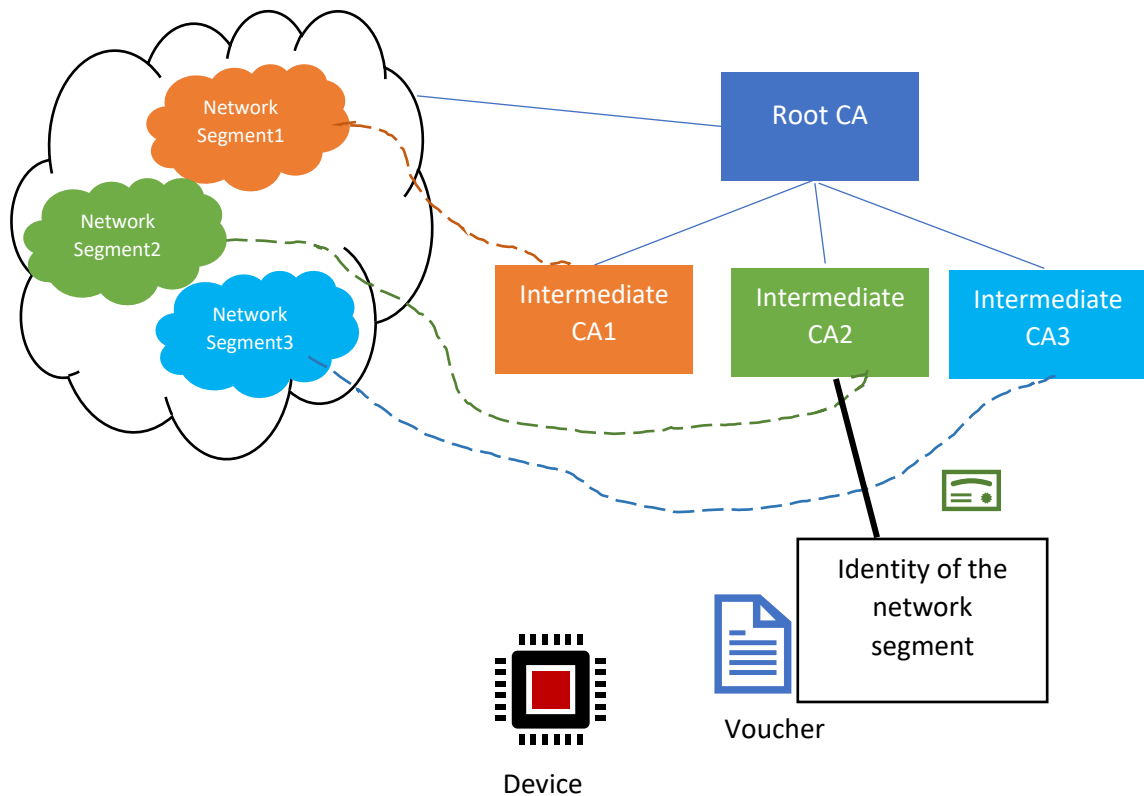


Figure 8: Identity of the network segment

## Vouchers

Voucher is a manufacturer provided artifact that provides information needed to provision the Device. The device manufacturer creates and signs a voucher. The voucher associates the Device to the owner network. The Device can use the information in the voucher to determine if the network that is trying to onboard the Device is where the Device is expected to be onboarded to. The Device could allow only its owner network to take control. The voucher supports to prevent situations where a device is stolen and getting onboarded to a network which is not the genuine owner.

RFC 8366[8] and RFC 8250[7] provide additional details of voucher specifications. Reference [10] describes other forms of voucher artifact in the form of a Ticket describing Device specific information and Machine specific information.



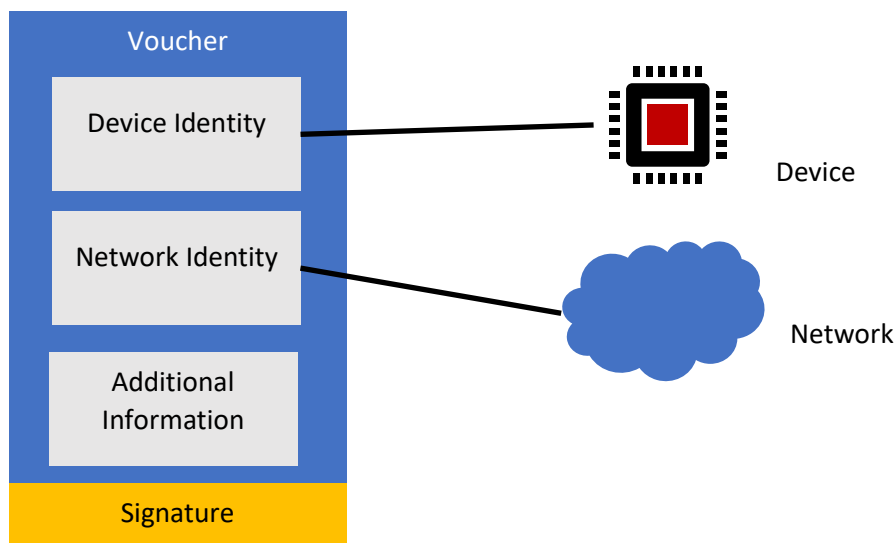


Figure 9: Voucher - Binding between Device and Network

The voucher is prepared as part of order handling or at a stage when the information about the target network and its Identity is known. The voucher artifact is signed by the manufacturer or a manufacturer authorized signing authority. The voucher is signed using a commonly trusted Certificate Authority (CA), which is part of a Public Key Infrastructure (PKI).

#### Voucher Distribution methods

The voucher is required by the Device and the network during the onboarding process. This is for a mutual authentication situation. Device needs to identify the network to join to, which is contained in the voucher. The network needs to know the Identity of the Device to accept to the network. The network establishes the source of origin of the Device from the Device identity. Different trust domains involved in the bootstrapping process are Network domain, Manufacturer domain and publicly trusted manufacturer domain. Network presents an identity that belongs to the network domain. The Device identity certificate belongs to the manufacturer domain. The voucher belongs to the manufacturer domain, which is publicly trusted. The bootstrapping process establishes trust relationships among these domains.

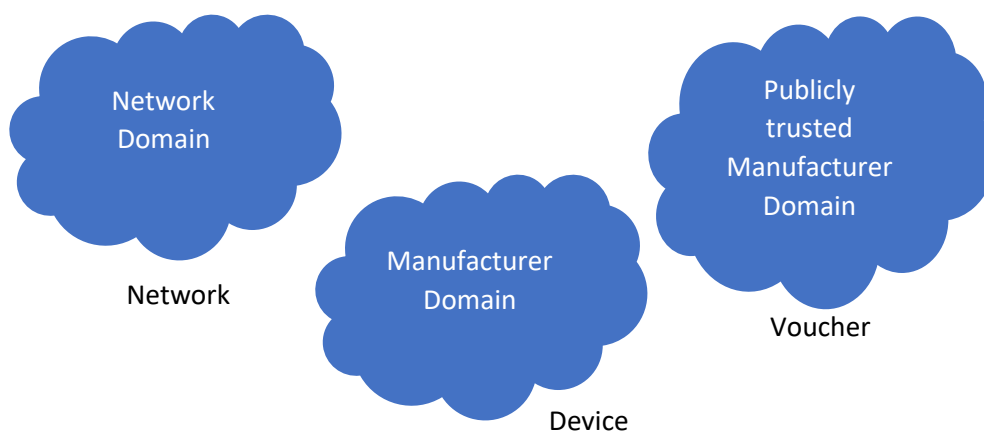


Figure 10: Trust Domains

The voucher distribution strategy is selected based on the deployment constraints and the risk factors involved. Multiple approaches are described below.

1. No voucher

In situations where a TOFU strategy is used, it is possible to perform the onboarding process without the vouchers. Device trusts the network on a TOFU basis. If the network has the trust anchor of the manufacturer domain by out of band means, the network trusts the Device.

2. Voucher embedded in the Device.

In this method, the voucher is embedded in the Device along with the Device ID certificate. This method offers simplicity in the voucher distribution channels. This method has constraints in the deployment and supply chain environment. The voucher is prepared before the Device leaves the manufacturer environment, which means that the information about the network domain should be known upfront. In situations where channel distributors are present, where devices are stored as spares, this method is not feasible.

3. Vouchers provided as a service

The vouchers could be made available as an internet hosted service by the manufacturer. The hosted service is the home for the Device to reach out and gather the voucher corresponding to the Device. A call home URI is parametrized with the instance specific information about the Device, such as a serial number. The hosting service provides the voucher in response to the call. This approach is suitable when the internet connectivity is available during the bootstrapping operation. In isolated networks, this is not a feasible option

<https://www.manufacturer.com/device/voucher?Instance=SerialNumber>

4. Out of band distribution

In this approach, the vouchers are made available to the network in an out of band channel, such as email. During the onboarding process, the onboarding component makes the vouchers available to the Device. The network onboarding component could use a suitable solution such as DNS redirection to make the vouchers available based on the call home URI.

## Discovery

When the Device is first connected to the network, it needs to discover a communicating end point so that the onboarding process can begin. The communication end point that facilitates the onboarding is the onboarding component in the network. The discovery mechanisms are not detailed in the document. An indicative solution to such discovery is mDNS.

## Process

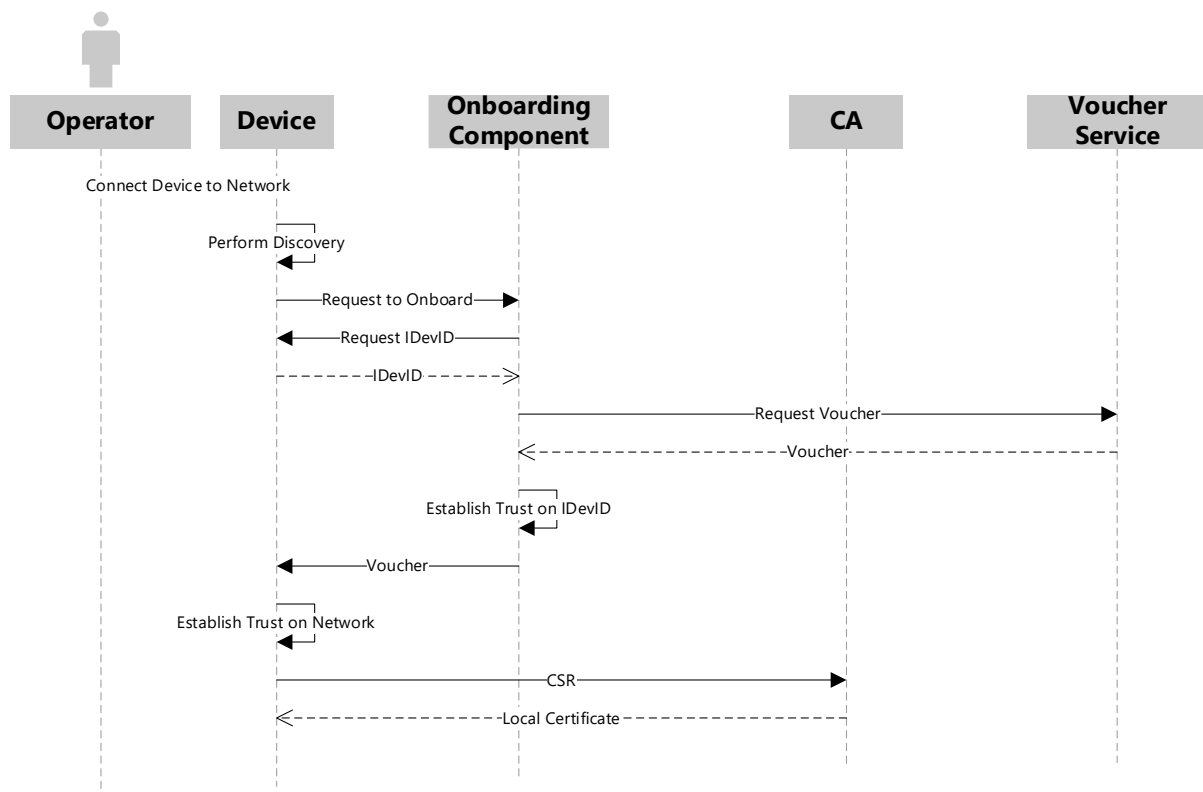


Figure 12: Onboarding Process

The sequence of steps for a zero touch provisioning is shown below.

1. Device is physically connected to the network
2. Device performs a discovery process to locate an onboarding component
3. Onboarding component collects IDevID from the Device
4. Onboarding component obtains a voucher corresponding to the Device
5. Onboarding component establishes trust on the Device
6. Device establishes trust on the network based on the information contained in the voucher and the network identity
7. Once the mutual trust is established, the device request for an LDevID and the network provides an LDevID
8. Now on, communication continues between the Device and the network

## Ongoing work in various domains

This section introduces the ongoing effort in various domains on provisioning solutions. These solutions are considering the constraints and risk factors in the domain in which the solutions are used.

### NIST - Trusted IoT Network-Layer Onboarding and Lifecycle Management

The NIST specification discusses methods for IP based devices. Access methods such as Bluetooth, Zigbee are not considered. The specification covers entire sequence of onboarding covering mutual authentication and voucher usage. The solution considers end user interests, manufacturer interests and service provider interests.

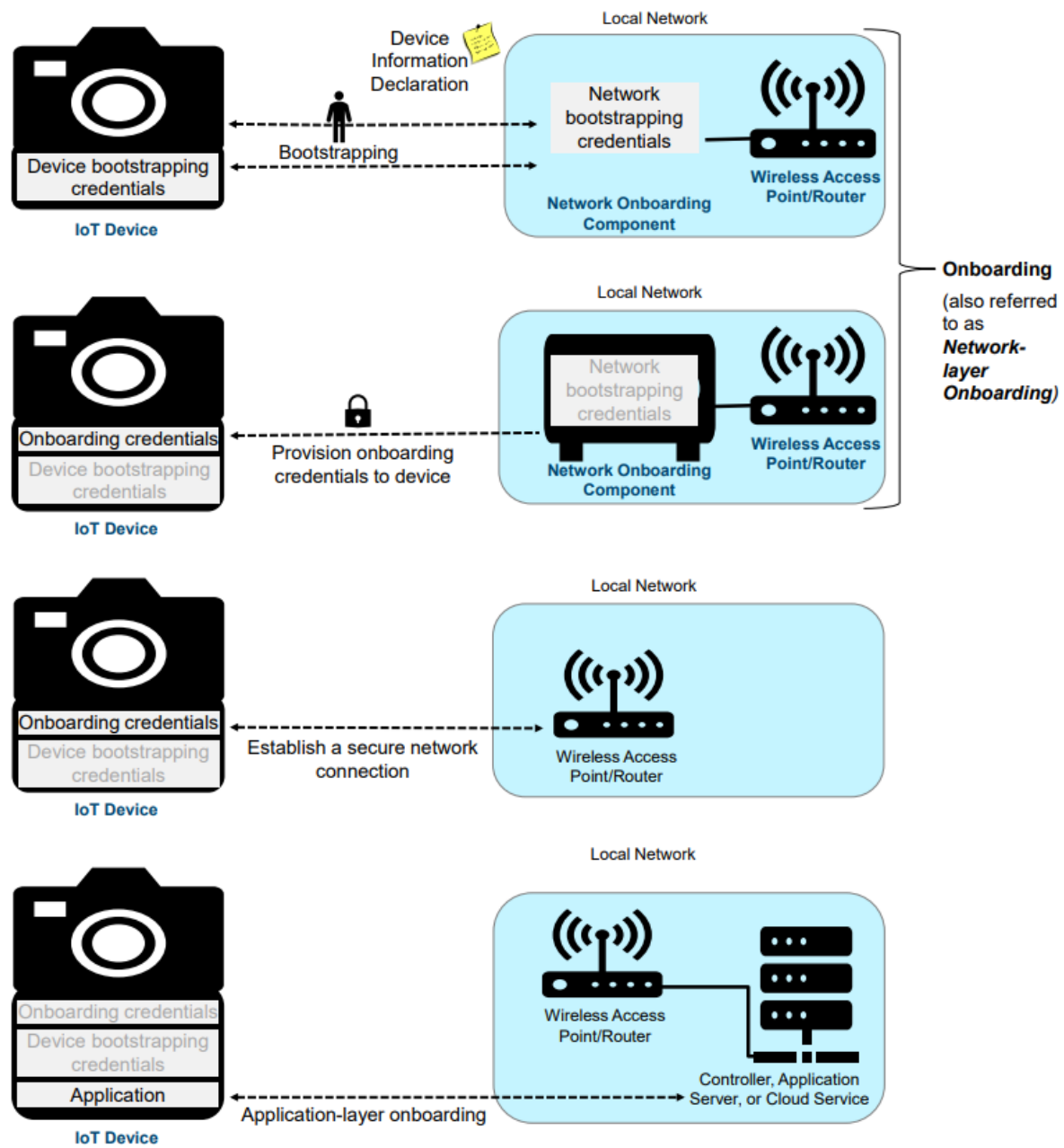


Figure 13: IoT Onboarding scenario (Image courtesy [1])

The different components involved in the onboarding process is shown in Figure 13.

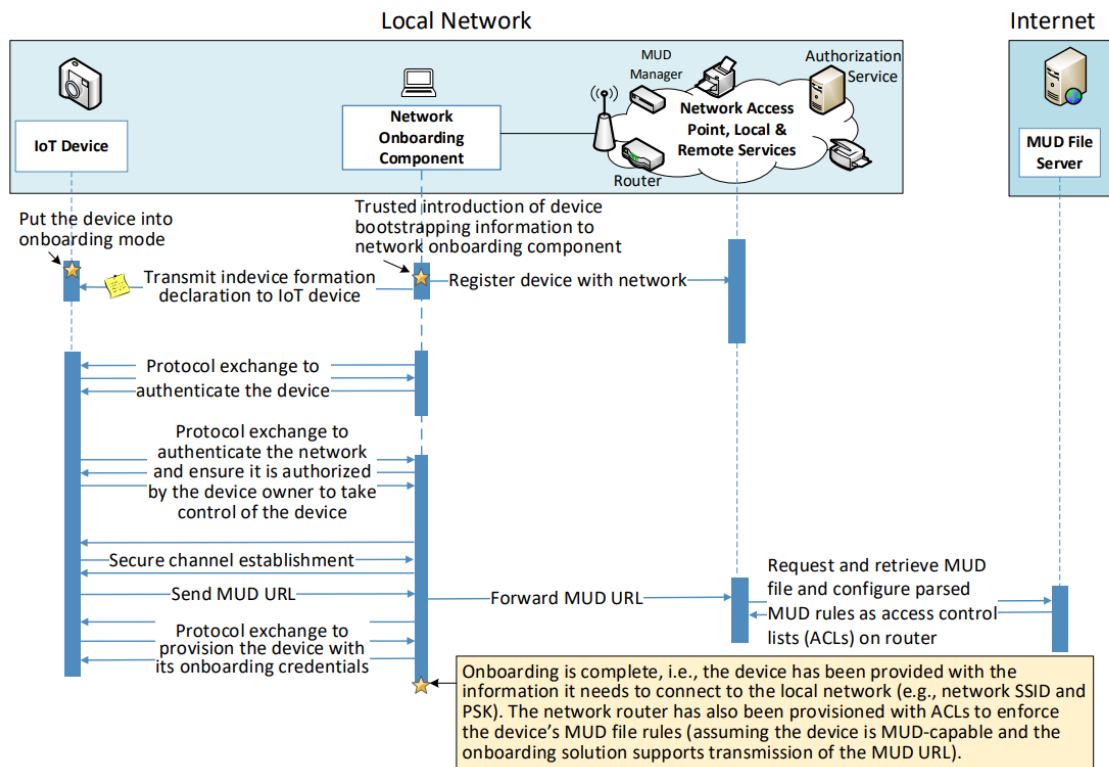


Figure 14: IoT Onboarding Process (Image courtesy [1])

The sequence of onboarding as envisioned by [1] is shown in Figure 14.

### Intel Secure Device Onboarding

Intel SDO uses the approach of anonymous identities based on Intel EPID. EPID provides a privacy preserving solution where the group membership is established without disclosing own Identity. The SDO identity is embedded in silicon before it is assembled into the Device. The solution uses a rendezvous URL to the Intel SDO service, where a private channel between Device and the onboarding platform is established.

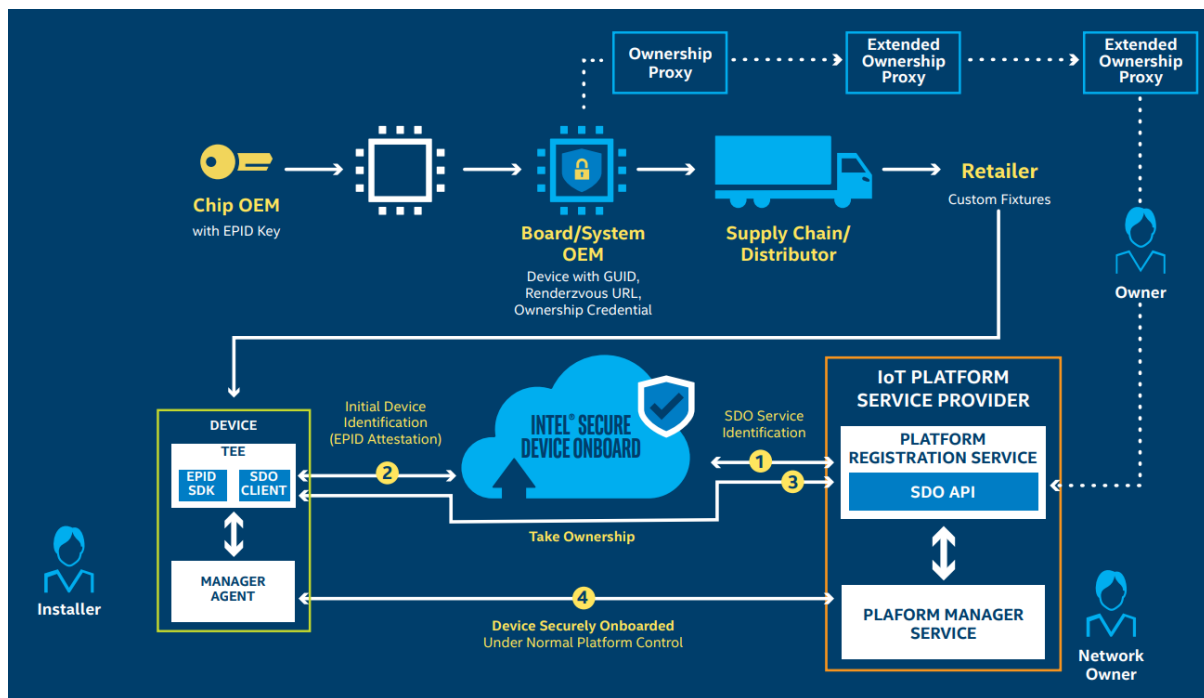


Figure 15: SDO Onboarding solution (Image courtesy [12])

EPID uses the group key schemes of public key cryptography. In the traditional PKI, there is one private key corresponding to the public key. Knowledge of the public key uniquely identifies the private key or the holder of the private key. In the group key scheme, there are many private keys corresponding to a public key. Using this, the Identity can be kept anonymous, at the same time proving group membership. Details of EPID scheme are described in [13].

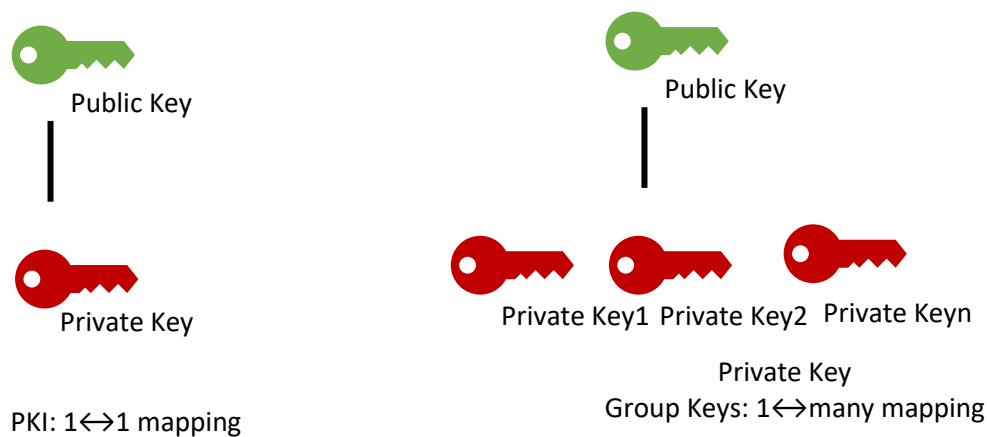


Figure 16: Group Keys

## Arm Pelion

Arm Pelion offers an IoT platform for device management. This solution is built around Intel SDO to manage device lifecycle. SDO solution is used for linking devices to Pelion cloud service.

## Bootstrapping Remote Secure Key Infrastructure( BRSKI)

BRSKI protocol is part of a group of specification from IETF Autonomic Networking Integrated Model and Approach (anima). BRSKI protocol is defined in RFC 8995. BRSKI protocol provides a solution for automated secure zero-touch bootstrap of new unconfigured devices that are called "pledges". Pledges have an Initial Device Identifier (IDeVID). The onboarding component is identified as registrar in the BRSKI protocol. BRSKI provides multiple options such as onboarding with a nonce, nonceless onboarding, audit logs, onboarding with Enrollment over Secure Transport (EST) as a certificate Signing request (CSR) protocol.

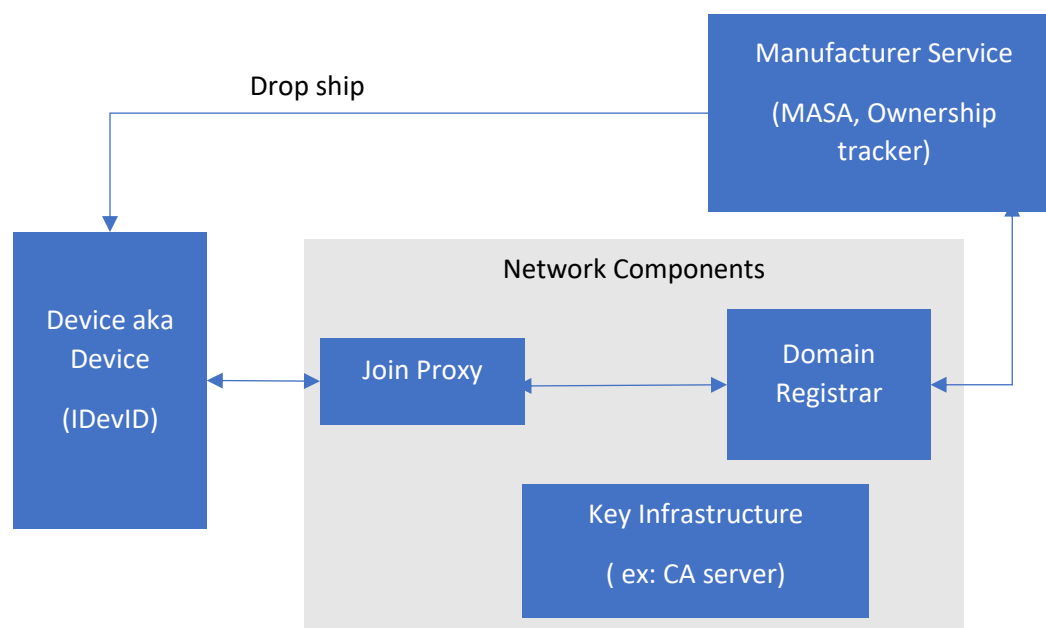


Figure 17: BRSKI Architecture

BRSKI provides a solution for establishing mutual authentication as part of the process

1. Registrar authenticating the Device: "Who is this Device? What is its Identity?"
2. Registrar authorizing the Device: "Is it mine? Do I want it? What are the chances it has been compromised?"
3. Device authenticating the registrar: "What is this registrar's identity?"
4. Device authorizing the registrar: "Should I join this network?"

RFC 8572 provides a Secure Zero Touch Provisioning definition which involves activities beyond the network layer onboarding. The provisioning steps are able to update the boot image, commit an initial configuration, and support other auxiliary needs.

## Siemens - SICAM Gridpass

Gridpass is a solution based on BRSKI where the certificate manager plays the role of the registrar. More information about the solution is available at [15].

## Azure Device Provisioning Service (DPS)

Azure IoT device provisioning service is a part of Azure IoT Hub that enables zero touch, just in time provisioning to the right IoT Hub without requiring human intervention. The solution uses an enrollment list which is manually created in the provisioning service. The provisioning process uses the enrollment list to provision individual devices.

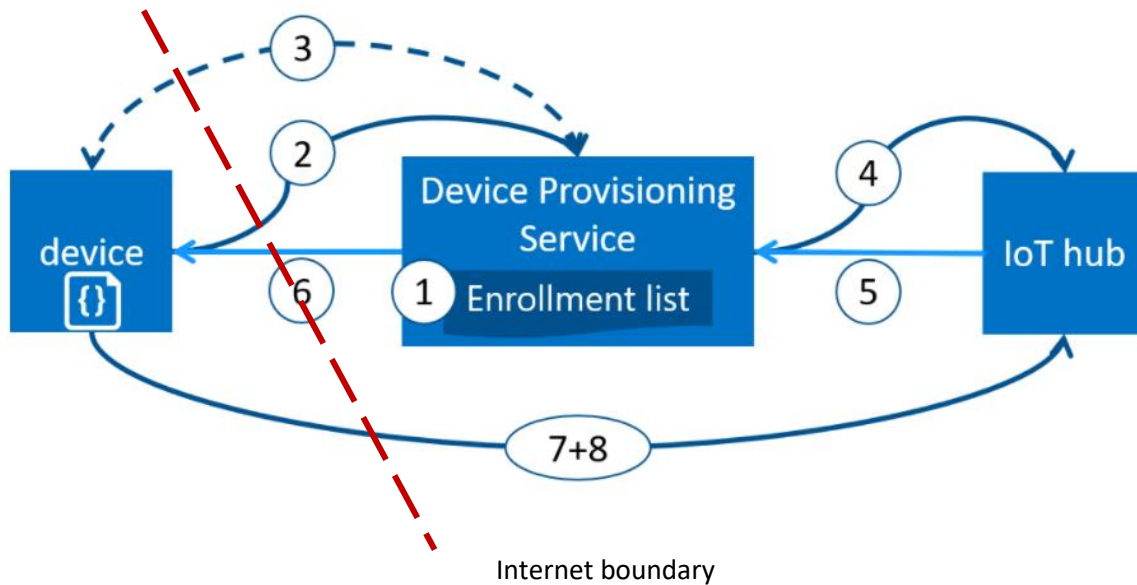


Figure 18: Azure DPS (Image courtesy [18])

1. The device manufacturer adds the device registration information to the enrollment list in the Azure portal.
2. Device contacts the DPS endpoint set at the factory. The Device passes the identifying information to DPS to prove its Identity.
3. DPS validates the Identity of the Device by validating the registration ID and key against the enrollment list entry.
4. DPS registers the Device with an IoT hub
5. The IoT hub returns device ID information to DPS.
6. DPS returns the IoT hub connection information to the Device. The Device can now start sending data directly to the IoT hub.
7. The Device connects to the IoT hub.
8. The Device gets the desired state from its device twin in the IoT hub.

The preparation required for setting up the DPS does not consider the challenges involved in the supply chain.

### OPCUA Device Provisioning

OPCUA is a common standard used in the industrial internet of things environment that allows seamless data exchange and interoperability. OPCUA part 10000-21 addresses the secure zero touch provisioning solutions. Reference [10] discusses the investigations into a secure provisioning solution in an industrial environment. The standard is yet unpublished, and the proposals available consider the supply chain and life cycles complexities. Manufacturer provided ticket is a comparable artifact to BRSKI vouchers that serves the purpose of binding the device identity with the network identity. Compound assemblies such as a machine built from individual devices and the Identity of the machine is also considered in the provisioning process.



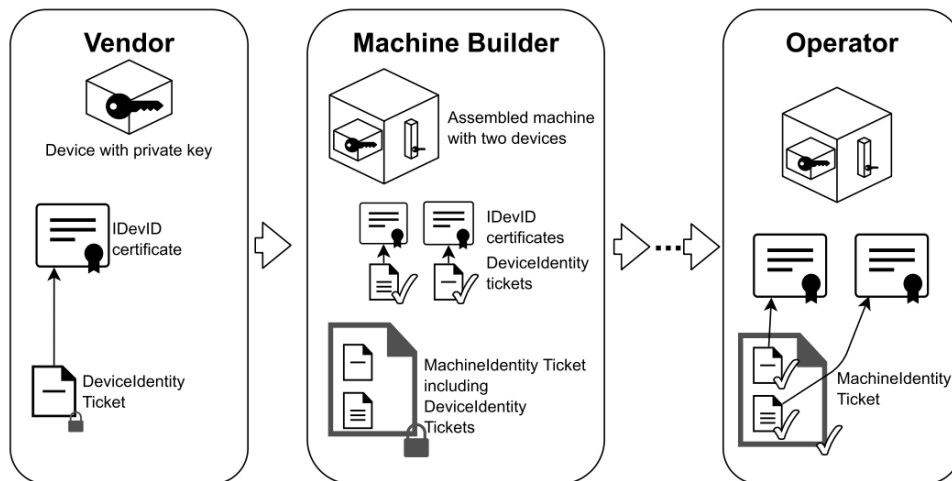


Figure 19: OPCUA Provisioning (Image courtesy[10])

### Wi-Fi Device Provisioning Protocol (DPP)

Wi-Fi DPP is a protocol specifically designed for wireless environments. In DPP, public keys are used to identify and authenticate all devices. The private key associated with a public key should be generated within each Device and protected from disclosure. Devices use public key cryptographic techniques to authenticate peer devices and establish shared keys for further secure communications. Two roles are identified in the protocol, an Enrollee and a Configurator. A Configurator supports the setup of Enrollees. The Configurator and the Enrollee engage in DPP bootstrapping, the DPP Authentication protocol and the DPP Configuration protocol. Either Configurator or Enrollee may perform the role of Initiator in the DPP Bootstrapping protocol and in the DPP Authentication protocol. However, only Enrollees initiate the DPP Configuration protocol and the DPP Introduction protocol. The initial bootstrapping key of the Device is required to start the bootstrapping process. One method for obtaining this is via QR codes placed in the Device. The QR code contains the public key associated with the device identity private key. The length of characters is limited in QR codes, yet it is possible to encode an ECC public key in a QR code.

The protocol provides other facilities such as delegating a configurator role to another configurator.

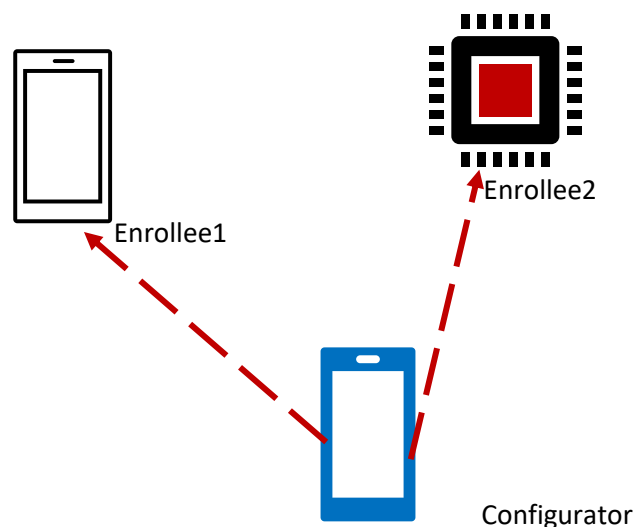


Figure 20: Wi-Fi DPP

## 6TiSCH Constraint Join Protocol

This protocol defines a join protocol in a constrained environment, where a device securely joins a 6TiSCH network. The Device and the join registrar share a symmetric key. CoAP request-response is used for the provisioning. Details of the protocol are available in [19].

## eSIM – Remote SIM provisioning

eSIMs are embedded Subscriber Identity Modules that contain the information that allows a subscriber to access a specific provider's network. Traditional SIMs were pre-programmed, but for eSIMs that can be done remotely by a Remote SIM Provisioning (RSP) system. RSP is a GSMA specification that defines how the process of remote Subscriber Identification Module activation should work. This specification aims to simplify lots of processes in the lifecycle of a mobile service or an M2M service. It also creates new business models where a single user could have multiple operators.

RSP, as defined by GSMA, offers two different architectures. One focuses on Consumer Devices, and the other focuses on M2M.



Figure 21: eSIM operator profile selection (Image courtesy [5])

Reference [5] provides details on eSIM provisioning sequence.

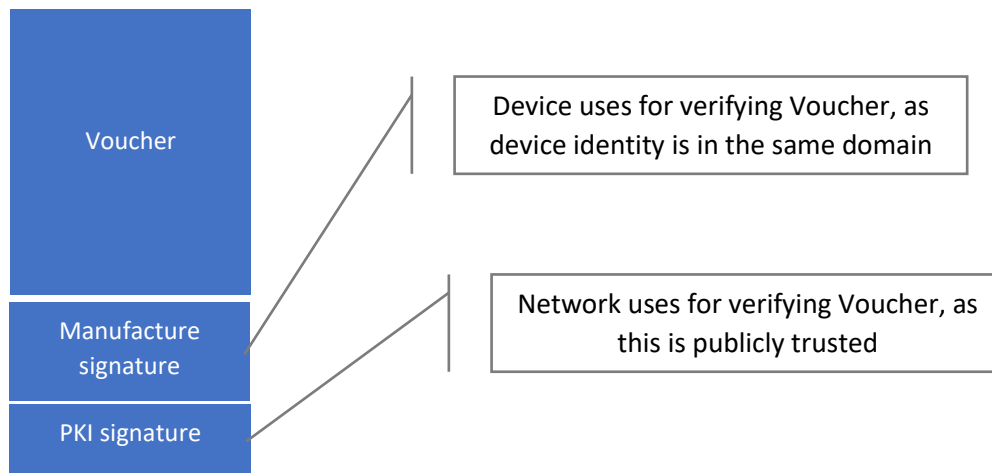
## Discussions

This document discussed the concepts around secure zero touch provisioning of security credentials. This document also discussed the various solutions available and work in progress in different industries and standards groups.

The solutions derive inputs from some of the foundational building blocks such as Device identities, vouchers, onboarding components, internet hosted services. Few solutions for constrained environments are also discussed.

There are specific situations in the context of individual organizations where the approaches discussed may be adapted. An example is the case of mergers and acquisitions where the device ownership changes. Adaptations to facilitate easy ownership transfer is one such specific example. The public Identity of the organization remains at the same time, manufacturer identity of the device changes. Solutions such as counter signatures are methods of such adaptations.

Vouchers have a counter signature. The first signature in the manufacturer domain which the Device uses for establishing authenticity and integrity on the voucher. The counter signature by the PKI system for the network to establish the authenticity and integrity of the voucher.



## Conclusion

The document presented approaches for secure zero touch provisioning for devices. The devices range from resource constrained IoT devices to composite assemblies. While a specific approach may not completely address the specific challenges and risk factors in a given environment, these approaches provide the toolset for designing a solution for a given environment.

The next steps to this analysis are contextualizing and defining specific problems and bringing out specific solutions.

## References

- [1] NIST Draft Whitepaper on Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.09082020-draft.pdf>
- [2] IEEE 802.1AR-2018, IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity
- [3] Hardware Requirements for a Device Identifier Composite Engine, [https://trustedcomputinggroup.org/wp-content/uploads/Hardware-Requirements-for-Device-Identifier-Composition-Engine-r78\\_For-Publication.pdf](https://trustedcomputinggroup.org/wp-content/uploads/Hardware-Requirements-for-Device-Identifier-Composition-Engine-r78_For-Publication.pdf)
- [4] Intel EPID, <https://intel-epid-sdk.github.io/download/enhanced-privacy-id-enhanced-revocation.pdf>
- [5] <https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf>
- [6] Wi-Fi DPP, [https://www.wi-fi.org/download.php?file=/sites/default/files/private/Device\\_Provisioning\\_Protocol\\_Specification\\_v1.1\\_1.pdf](https://www.wi-fi.org/download.php?file=/sites/default/files/private/Device_Provisioning_Protocol_Specification_v1.1_1.pdf)
- [7] RFC 8250, Manufacturer Usage Description Specification
- [8] RFC 8366, A Voucher Artifact for Bootstrapping Protocols
- [9] The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, <https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf>
- [10] F. Kohnhäuser, D. Meier, F. Patzer and S. Finster, "On the Security of IIoT Deployments: An Investigation of Secure Provisioning Solutions for OPC UA," in IEEE Access, vol. 9, pp. 99299-99311, 2021, doi: 10.1109/ACCESS.2021.3096062.
- [11] Intel SDO, Videos and Documents, <https://www.intel.in/content/www/in/en/internet-of-things/secure-device-onboard.html>

- [12] Intel SDO Product Brief, <https://www.intel.com/content/dam/develop/public/us/en/documents/intel-sdo-product-brief.pdf>
- [13] Enhanced Privacy ID from Bilinear Pairing, <https://eprint.iacr.org/2009/095.pdf>
- [14] RFC 8995, Bootstrapping Remote Secure Key Infrastructure
- [15] SICAM Gridpass, <https://assets.new.siemens.com/siemens/assets/api/uuid:b7c3e06c-ca05-448d-b3b1-f1ced0412e9d/sicamgridpassmanualv1.80en.pdf>
- [16] IETF ANIMA, <https://datatracker.ietf.org/wg/anima/documents/>
- [17] RFC 8572, Secure Zero Touch Provisioning (SZTP)
- [18] Azure DPS, <https://docs.microsoft.com/en-us/azure/iot-dps/about-iot-dps>
- [19] <https://datatracker.ietf.org/doc/html/draft-ietf-6tisch-minimal-security#section-8>