Secure IoT begins with Zero-Touch Provisioning at scale

www.infineon.com

EUROTECH

GlobalSign GMO INTERNET GROUP

Microsoft Azure

Infineon

Abstract

The path to secure IoT deployments starts with a hardware root-of-trust at the device level, a simple concept that belies the complexity of managing a chain of trust that extends from every edge device to the core of the network. The solution to this management challenge, based on a coordinated effort of domain experts, is a zero touch “chip-to-cloud” provisioning service for certificates-based identity lifecycle management for connected devices.

Contents

Introduction

What's the largest roadblock to realizing the promise of the Internet of Things? For many organizations, the obstacle delaying widespread deployments is the strategy for onboarding the necessary edge resources for a lifetime of secure operation. Proof-of-concept and pilot systems comprised of dozens and even hundreds of nodes in a controlled setting are simply different than a full-scale roll-out. And while we are well-served today by IoT platforms and a proven, cloud-accessed application infrastructure, the complex task of device onboarding remains a multi-domain problem by nature. Thus, the solution is best addressed through a coordinated effort by domain experts. This paper presents such a solution, delivered by Infineon Technologies, GlobalSign, Eurotech and Microsoft.

Onboarding a new device to a cloud-served IoT network is essentially a two-part process; establishing the initial connection to the cloud-accessed network and then configuring the device to perform its intended task. In any system designed to scale, the process must be automated. Manual onboarding of each device, and subsequent management of each and every device, is simply impractical in terms of labor and time. The goal is Zero Touch Provisioning, where a handshake triggered when a device is powered on initiates onboarding and a subsequent automated provisioning process. Many companies today support elements of Zero Touch Provisioning, but leave the end customer responsible for part of the implementation. The solution presented here leverages the expertise of suppliers addressing each critical step to provide a secure, automated identity chain that extends throughout the operational lifecycle of the device and system.

Device identity is the baseline

A baseline requirement for this type of deployment is Zero Trust; the initial handshake with the network must include authentication of identity and credentialing of trusted certificates that then support subsequent interactions. For this purpose, the lessons learned in implementing Zero Trust inside IT networks are applicable to the Operational Technologies served by IoT systems.

Today, an embedded hardware root-of-trust is the most widely used methodology to meet the goal of allowing only trusted devices to access a network. This proven technology can be applied to IoT systems and, when paired with robust, Public Key Infrastructure (PKI) services, provides the basis for a practically impenetrable IoT security architecture. The combined hardware/software approach provides the strongest possible defense of trusted device identities from point of manufacture throughout the product lifecycle.

PKI, a standard for authentication and encryption identified as a keystone of Zero Trust by the National Institute of Standards, is implemented as X.509 certificates. Documented in IETF RFC 5280, the X.509 certificate standard allows high-level control of certificate management and is well-suited to the full chain authentication methodology of Certificate Authorities.

The optimal root-of-trust used in IoT security implementation is the Trusted Platform Module (TPM), developed by the Trusted Computing Group.[1]

Used extensively for two decades in computing and networking devices, the TPM provides secure, tamper-proof key generation and encrypted storage. The TPM used in this solution is a discrete device with cryptographic algorithms embedded in hardware and with hardened features to protect from side-channel and physical attacks. It contains a unique and signed Endorsement Certificate (ECert) and secret Endorsement Key (EK), which is used by a trusted Certificate Authority (CA) as the basis for authentication.[2] Additionally, persistent storage hierarchies in the TPM provide the flexibility to provision the multiple device identities used over the lifetime of an IoT system deployment.

Designed principally as a cryptographic co-processor, the TPM's internal secret key is the ideal root-of-trust for IoT devices. Closely tying a TPM to the x.509 certificate management services and cloud-based resources of a CA creates a powerful tool for both initial attestation and full life-cycle management of operational device certificates. This chain-of-trust extends from the start of the supply chain when the TPM component is manufactured, proceeding to integration by a device manufacturer, through enrollment, provisioning and operational status, and even onto re-tasking or retirement (Image 1). We'll look at this from a wider perspective after a review of the role of each of the participants in the Zero Touch Provisioning Solution.

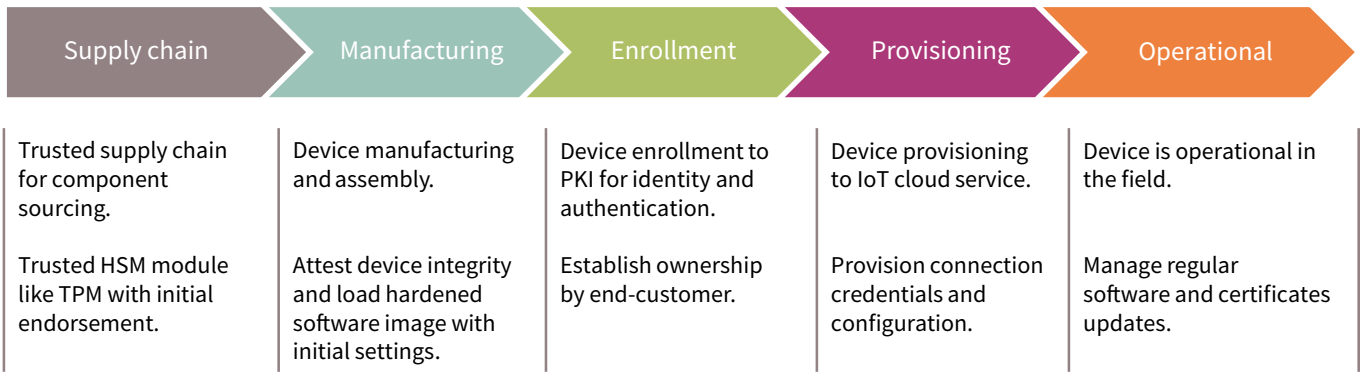


Image 1: The device lifecycle from supply chain to operational

1 https://trustedcomputinggroup.org/work-groups/trusted-platform-module/

2 https://www.globalsign.com/en/blog/new-white-paper-tpm-20-and-certificate-based-iot-device-authentication

Domain experts

The baseline trusted identity of the TPM is provided by Infineon Technologies, a top ten worldwide supplier of semiconductors and long-time leader in hardware-based security. The company's OPTIGA™ TPM family, designed to Trusted Computing Group specifications and manufactured in secure facilities, is certified to Common Criteria CC EAL 4+ security compliance. Supporting root-of-trust and identity assurance tied to digital certificates, these devices have the small footprint and low-power required for securing embedded systems operating on the edge.

As the root of trust in Zero Touch Provisioning, the TPM's unique EK certificate is cross-signed with a GlobalSign IoT root. GlobalSign, a global Certificate Authority and provider of trusted identity and security solutions at scale, uses the EK to attest to the TPM integrity. Subsequently, the TPM protects private keys used for customized X.509 certificates, which act as Secure Device Identifiers (DevIDs) as defined in the IEEE 802.1AR (IETF RFC 5759) standard[3] for unattended autonomous authentication, and provides for full identity lifecycle management of certificated devices.

The Secure Device Identifier (DevID) is a certificate-based identity that is cryptographically bound and uniquely assigned to a device. It facilitates the interoperability of device attestation and secure device authentication use cases. A DevID consists of a unique-per-device secret (private key) capable of creating a signature and an X.509 public key certificate with its certificate chain up to the trust anchor. The DevID certificate is used to identify the supplier of the device, the device type, and the device serial number.

The manufacturer and integrator of secure edge devices, and in most cases the central relationship for enterprise customers and integration partners, is Eurotech. With operations in Europe, North America and Japan, Eurotech provides hardware platforms and edge devices for pervasive computing, with an emphasis on cloud-connected, IoT systems. Eurotech's Edge computers and IoT Gateways are fitted with Infineon TPM 2.0 modules, and the company also provides its IoT Integration Platform (Everyware Cloud) and Edge Device Software (Everyware Software Framework) to manage IoT gateways and devices and connect data from the field to enterprise applications.

This framework pairs with Microsoft Azure and its IoT Services, an open and scalable platform from device to the cloud. Azure IoT assembles managed and platform services, security and operating systems, and data and analytics applications that support robust solutions and flexible service delivery. Collectively, the four companies collaborate to integrate end-to-end-trust in the delivered and operating IoT solution (Image 2).

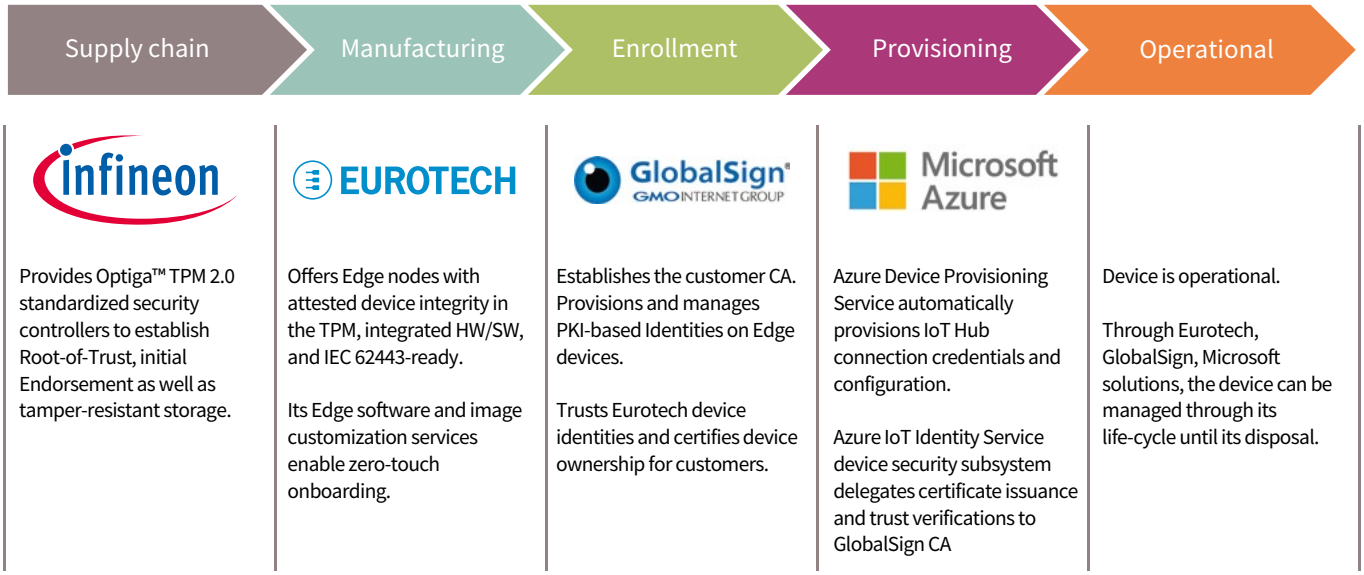


Image 2: Integrated end-to-end trust

3 802.1AR-2018 - IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity | IEEE Standard | IEEE Xplore

High security with low complexity

The collaborative approach to Zero Touch Provisioning is a response to the requirements of enterprise customers that recognize that the challenge of establishing and managing trusted identities is best addressed by specialists. When deployed, systems access the IoT Identity Service security subsystem of Microsoft Azure IoT Edge, which offers flexibility in the customer's engagement and resource allocation and reduces complexity while supporting the strong and comprehensive trusted identity solution.
To facilitate integration of all trust chain elements, the Microsoft Azure IoT Identity Service security subsystem for IoT devices natively implements the standards described in this paper.

A typical project flow (Image 3) begins when an enterprise or its preferred integration partner authorizes a Certificate Authority and receives an intermediate certificate, which it registers to the Azure Digital Provisioning Service (DPS) for device attestation. This establishes the basis for all DevIDs associated with the zero-touch devices in a given project. In turn, the customer engages with Eurotech to supply hardware devices pre-configured for zero-touch onboarding.

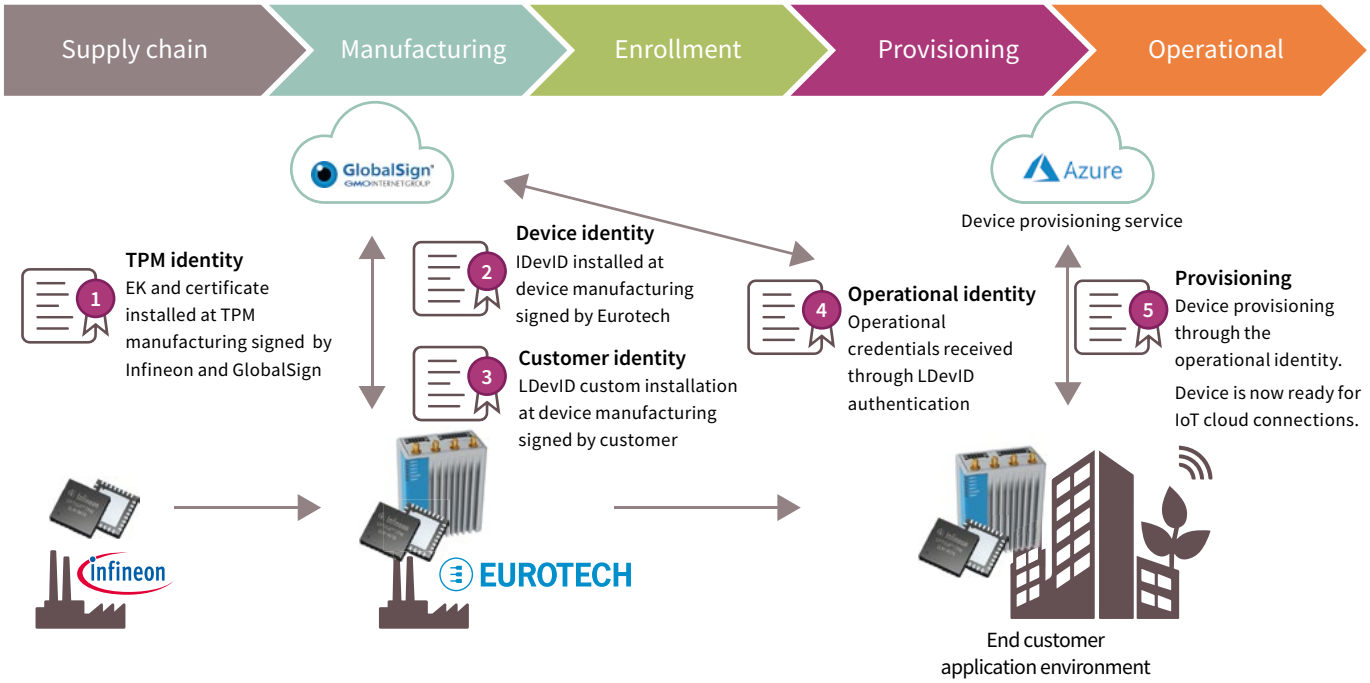


Image 3: Device identities life cycle

Eurotech devices feature device identities based on the 802.1AR standard. At manufacturing time, Eurotech creates and installs an Initial Device Identifier (IDevID). The IDevID certificate, signed by Eurotech, attests the integrity of the platform by identifying it as a genuine Eurotech device and specifying its device type and its serial number. The IDevID key and certificates are respectively stored in the Endorsement and Platform Hierarchy of the TPM 2.0, making them immutable and unmodifiable for the lifetime of the device.

Phase	EST URL	EST Authentication	Enrolled Certificates	Certificate Lifespan	TPM	Azure IDS Mapping
TPM Manufacturing	-	-	EK	Never expiring	EK Key under EH: 0x81010001	-
Manufacturing: Production of Eurotech Device Standard	eurotech.est.globalsign.com	EK HTTPS Header Secret-Value IP White Listing	IDevID	Never expiring	IDevID Key under EH: 0x81020000. IDevID Cert under PH: 0x01C90000.	-
Manufacturing: Zero-touch Provisioning for end Customer	customer-ldevid.est.globalsign.com	IDevID+ HTTPS Header Secret-Value	LDevID (e.g. Customer IDevID)	Long-lived (25y-50y)	Key under SH 0x81000002 azure:ldevid Cert under file system.	est-id
Field: (Re-)enrollment of device-ca	customer.est.globalsign.com	est-id (LDevID)	Azure device-ca	Short-lived	Key under SH azure:device-ca	device-ca
Optional Field: (Re-) enrollment of device-id	customer.est.globalsign.com	est-id (LDevID)	Azure device-id	Short-lived	Key under SH azure:device-id	device-id

Image 4: Trust chain operational blueprint

To enable zero-touch provisioning, Eurotech offers a customization service to install complementary Locally Significant Device Identifiers (LDevIDs) at the point of manufacture time. The LDevID is affiliated to the device owner and signed by its CA. This pre-configuration supplements the IDevID and it is used for authentication and device authorization, as well as the installation/ configuration of the Azure IoT Identity Service (with its own unique LDevID). LDevIDs, which are anchored and stored in the TPM (Image 4), and leverage the owner accessible Storage Hierarchy (Image 5). The creation and management of these identities is controlled through an enterprise class PKI infrastructure and through standards-based protocols.

TPM 2.0 Control Domains and DevIDs		
Endorsement Hierarchy (EH)	Protects keys and certificates installed at TPM manufacturing	Infineon OPTIGA® SLM 9670 is provisioned with Endorsement Key (EK) and Certificate, cross-signed with the GlobalSign TPM Root CA.
Platform Hierarchy (PH)	Owned by Eurotech as platform manufacturer.	Contains IDevID signing and attestation key and an IDevID Certificate signed by Eurotech.
Storage Hierarchy (SH)	Owned by the end-customer for application usages	Contains LDevID and its LDevID certificates signed by customer CA.

Image 5: Secure device identities (DevIDs)

Enrollment over Secure Transport (EST), described in IETF's RFC 7030, is a protocol for X.509 certificate enrollment from a CA. EST's benefits compared to alternative protocols lay in its simplicity and security. The functions of the protocol are straightforward and are operable like many REST API's. At EST's core and most commonly used functions are the /simpleenroll and /simplereenroll endpoints (Image 6). As EST leverages TLS for transport security, mutual certificate-based authentication can be used to verify previously issued identities, such as IDevIDs issued by the device manufacturer.

With delivery of trusted devices to field locations, network attestation, enrollment and device provisioning is fully-automated. Additional Cloud services and other features specific to the device or IoT application are serviced in the same manner. Lifecycle certificate management, which extends to re-purposing of fleet devices, and even eventual decommissioning, ensures that device access and authorizations are always current.

Image 6: EST illustration

A trusted solution

It's no surprise that nearly every enterprise implementing IoT as part of a digital transformation strategy makes security a top consideration (Image 7)[4]. While the specifics vary, many of the most frequently cited concerns revolve around authentication and fleet management issues. Security in depth, starting with each device in the network, addresses these concerns, a fact that makes trusted identity a pre-requisite for successful deployment and lifetime operation.

The standards-based definition, issuance, and lifecycle management of certificate-based IoT device identities described herein is more than the basis for automated, Zero Touch Provisioning. It is the keystone for security by design, applied at the level of every device with network access, that ensures the success and lifetime value of IoT solutions.

While **security** is a low hinderance to IoT adoption, it is a consideration during implementation, with data privacy top of mind for about half of all organizations

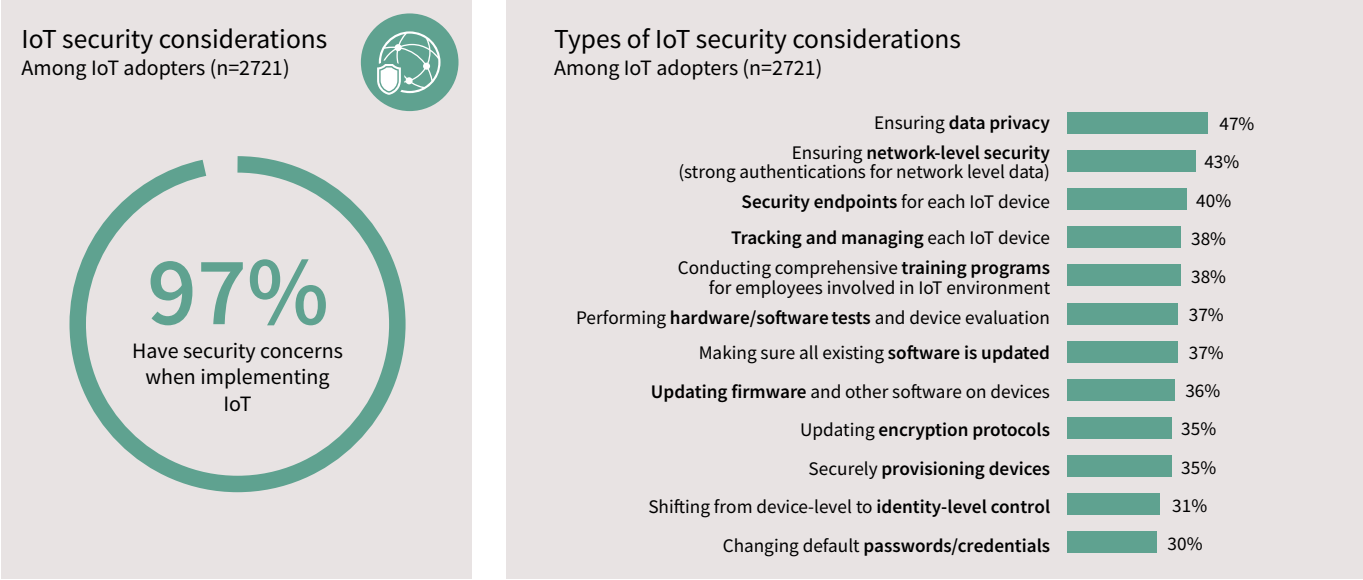
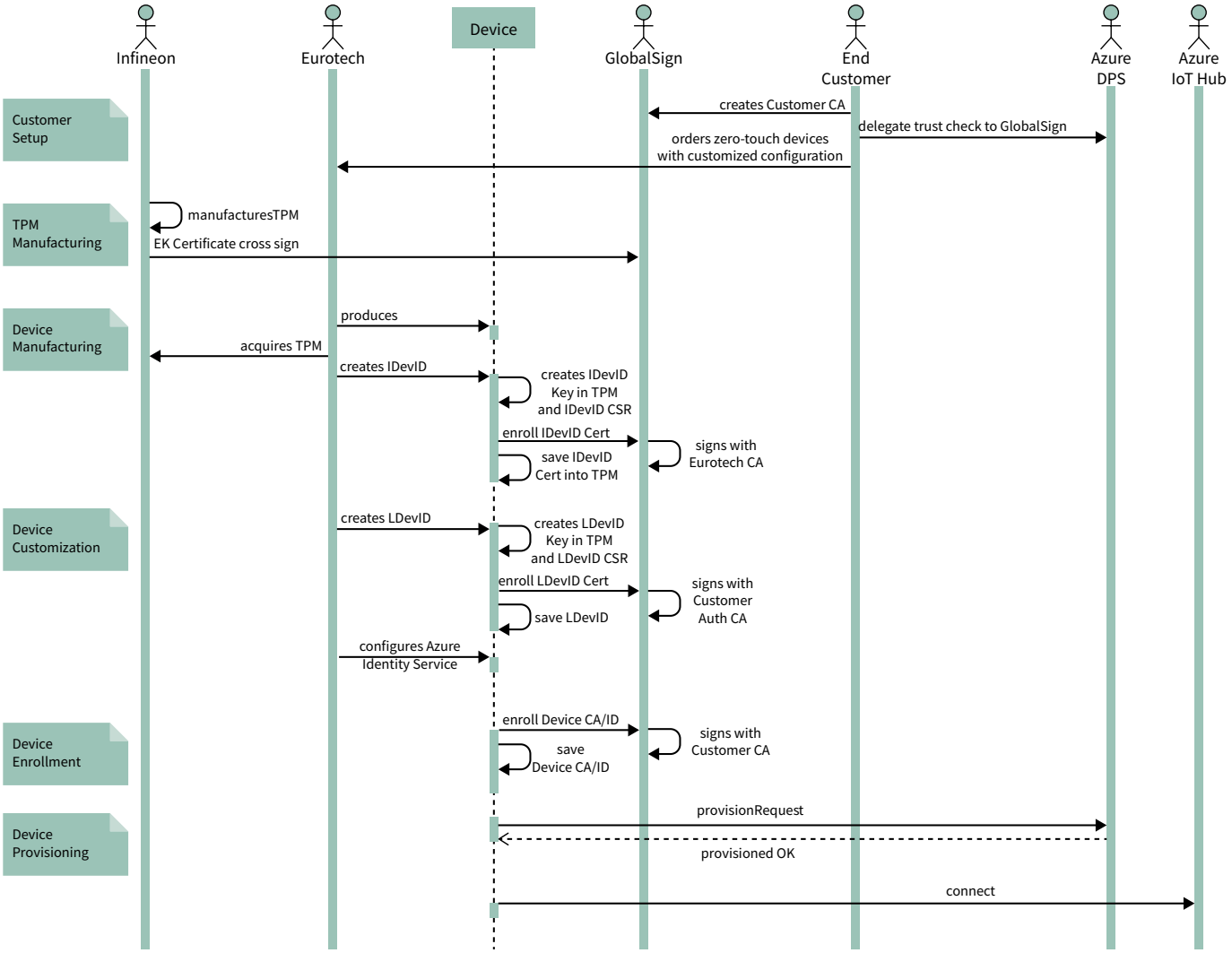
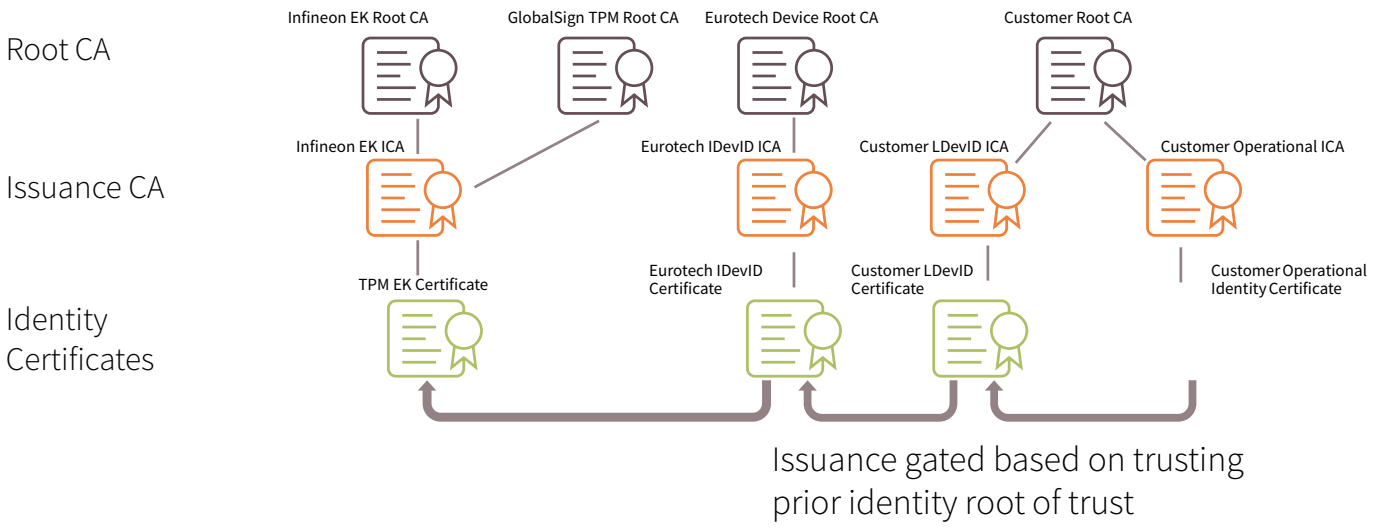


Image 7: IoT security considerations

4 IoT Signals Report: https://azure.microsoft.com/en-us/resources/iot-signals/



Appendix image



Solution PKI hierarchy

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 04/2021

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.