保护物联网从大规模的零接触供应开始

Marco Carrer，欧洲技术公司首席技术官
Lancen LaChance，GlobalSign物联网身份解决方案主管
Eustace Asanghanwa，微软首席项目经理
Josef Kohn，Infineon嵌入式安全营销总监

EUROTECH　GlobalSign GMO INTERNET GROUP　Microsoft Azure　infineon

摘要

安全物联网部署的路径始于设备级的硬件信任根，这一简单概念掩盖了管理从每个边缘设备延伸到网络核心的信任链的复杂性。这一管理挑战的解决方案基于领域专家的协同工作，是一种零接触的“芯片到云”供应服务，用于基于证书的连接设备身份生命周期管理。

目录

简介

实现物联网承诺的最大障碍是什么？

对于许多组织来说，延迟广泛部署的障碍是为终身安全运营提供必要的边缘资源的策略。概念验证和在受控环境中由数十个甚至数百个节点组成的试点系统与全面推出完全不同。尽管物联网平台和经验证的云访问应用基础设施为我们提供了良好的服务，但设备注册的复杂任务本质上仍是一个多领域问题。

因此，解决方案最好通过领域专家的协调努力来解决。本文介绍了由Infineon Technologies、GlobalSign、Eurotech和Microsoft提供的解决方案。

将新设备安装到云服务物联网网络基本上是两部分过程；建立初始值连接到云访问网络，然后配置设备以执行其预期任务。在任何按规模设计的系统中，流程必须自动化。在人工和时间方面，手动安装每个设备以及随后管理每个设备都是不切实际的。目标是零接触供应，整个过程在设备通电时触发的握手会启动运行和随后的自动配置。

如今，许多公司支持零接触资源调配的基本部分，但最终客户也需负责部分实施。此处提供的解决方案利用供应商的专业知识解决每个关键问题，提供安全可靠的自动化身份链的步骤并扩展到设备和系统。

设备标识基线

此类部署的基线要求为零相信与网络的初始握手，必须包括身份认证和可信身份认证，然后支持后续交互的证书。为此，在实施零排放的过程中吸取的经验教训 IT 网络内部的信任适用于运营物联网系统服务的技术。

如今，嵌入式硬件的信任根是最重要的且广泛使用的方法，来实现允许只有受信任的设备才能访问网络。这项技术已被证实可以应用于物联网系统与健壮的公钥基础设施（PKI）服务配对，为几乎无法穿透的物联网提供了基础安全架构。硬件/软件相结合的方法在整个产品生命周期中从制造点为可信设备身份提供了最强有力的保护。

PKI是一种认证和加密标准，被国家标准协会认定为零信任的基石，它被实现为X.509证书。记录在IETF RFC 5280中的X.509证书标准允许对证书管理进行高级控制，并且非常适合证书颁发机构的全链认证方法。

物联网安全实施中使用的最佳信任根是由可信计算集团开发的可信平台模块（TPM）[1]。

TPM在计算和网络设备中广泛使用了20年，它提供了安全、防篡改的密钥生成和加密存储。此解决方案中使用的TPM是一个离散设备，其加密算法嵌入硬件中，并具有增强的功能，以防止侧通道和物理攻击。它包含唯一且签名的背书证书（ECert）和秘密背书密钥（EK），可信证书颁发机构（CA）将其用作身份验证[2]的基础。此外，TPM中的持久存储层次结构提供了灵活性，以提供在物联网系统部署的整个生命周期中使用的多个设备标识。

TPM的内部密钥主要设计为密码协处理器，是物联网设备的理想信任根。将TPM与x.509证书管理服务和CA的基于云的资源紧密结合，为操作设备证书的初始认证和全生命周期管理创建了一个强大的工具。这种信任链从TPM组件制造时的供应链开始延伸到设备制造商的集成，再到注册、供应和运行状态，甚至到重新分配任务或退役（图1）。在回顾了零接触供应解决方案中每个参与者的角色之后，我们将从更广泛的角度来看待这一点。

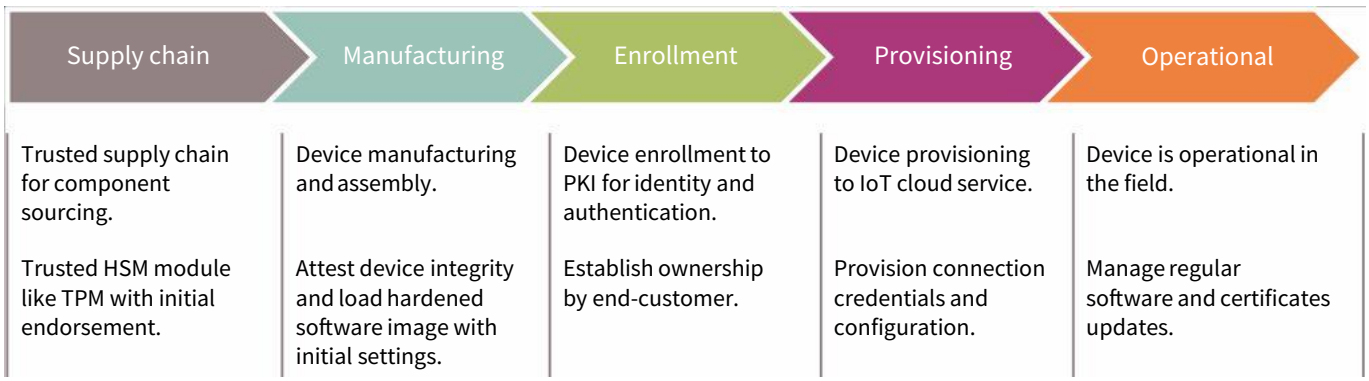


图1：从供应链到运营的设备生命周期

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

领域专家

TPM的基线可信身份由Infineon Technologies提供，该公司是全球十大半导体供应商，也是硬件安全领域的长期领导者。公司的OPTIGA™ TPM系列是根据可信计算集团规范设计的，在安全设施中制造的，通过了通用标准CC EAL 4+安全合规性认证。这些设备支持与数字证书相关的信任根和身份保证，占地面积小，功耗低，可确保在边缘操作的嵌入式系统的安全。

作为零接触供应的信任根，TPM的唯一EK证书与GlobalSign IoT根交叉签名。GlobalSign是一个全球证书颁发机构和大规模可信身份和安全解决方案提供商，它使用EK来证明TPM的完整性。随后，TPM保护用于定制X.509证书的私钥，这些私钥充当IEEE 802.1AR（IETF RFC 5759）[3]标准3中定义的用于无人值守自主认证的安全设备标识符（DevID），并提供认证设备的完整身份生命周期管理。

安全设备标识符（DevID）是一种基于证书的身份，以加密方式绑定并唯一分配给设备。它促进了设备认证和安全设备认证用例的互操作性。DevID由一个能够创建签名的设备并且具备唯一密钥（私钥）和一个X.509公钥证书组成，其证书链一直到信任锚点。DevID证书用于标识设备的供应商、设备类型和设备序列号。

欧洲技术公司是安全边缘设备的制造商和集成商，在大多数情况下是企业客户和集成合作伙伴的中心关系。Eurotech在欧洲、北美和日本开展业务，为普及计算提供硬件平台和边缘设备，重点是云连接物联网系统。Eurotech的边缘计算机和物联网网关配备了Infineon TPM 2.0模块，该公司还提供了物联网集成平台（Everyware Cloud）和边缘设备软件（Every ware Software Framework），以管理物联网网关和设备，并将现场数据连接到企业应用程序。

该框架与Microsoft Azure及其物联网服务（一个从设备到云的开放和可扩展平台）配对。Azure IoT组装托管和平台服务、安全和操作系统，以及数据和分析应用程序，支持强大的解决方案和灵活的服务交付。四家公司共同合作，在交付和运营的物联网解决方案中整合端到端的信任（图2）。

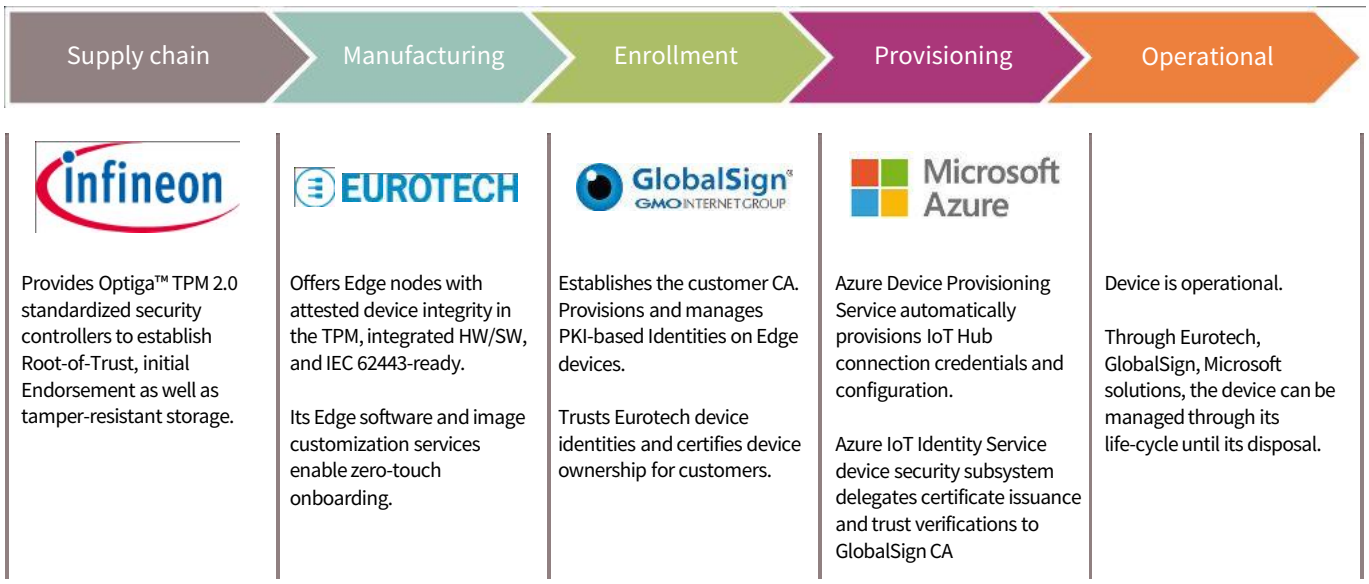


图2：集成端到端的信任

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

高安全性和低复杂性

零接触资源调配的协作方法是对企业客户需求的回应，企业客户认识到建立和管理可信身份的挑战最好由专家来解决。部署后，系统可访问Microsoft Azure IoT Edge的IoT身份服务安全子系统，该子系统可在客户参与和资源分配方面提供灵活性，并降低复杂性，同时支持强大而全面的可信身份解决方案。为了促进所有信任链元素的集成，用于物联网设备的Microsoft Azure物联网身份验证服务安全子系统，实现了本文中描述的标准。

典型的项目流程（图3）始于企业或其首选集成合作伙伴授权证书颁发机构并接收中间证书，然后注册到Azure数字供应服务（DPS）进行设备认证。

这为给定项目中与零接触设备相关联的所有DevID奠定了基础。反过来，客户与Eurotech合作，提供预先配置的零接触登录硬件设备。

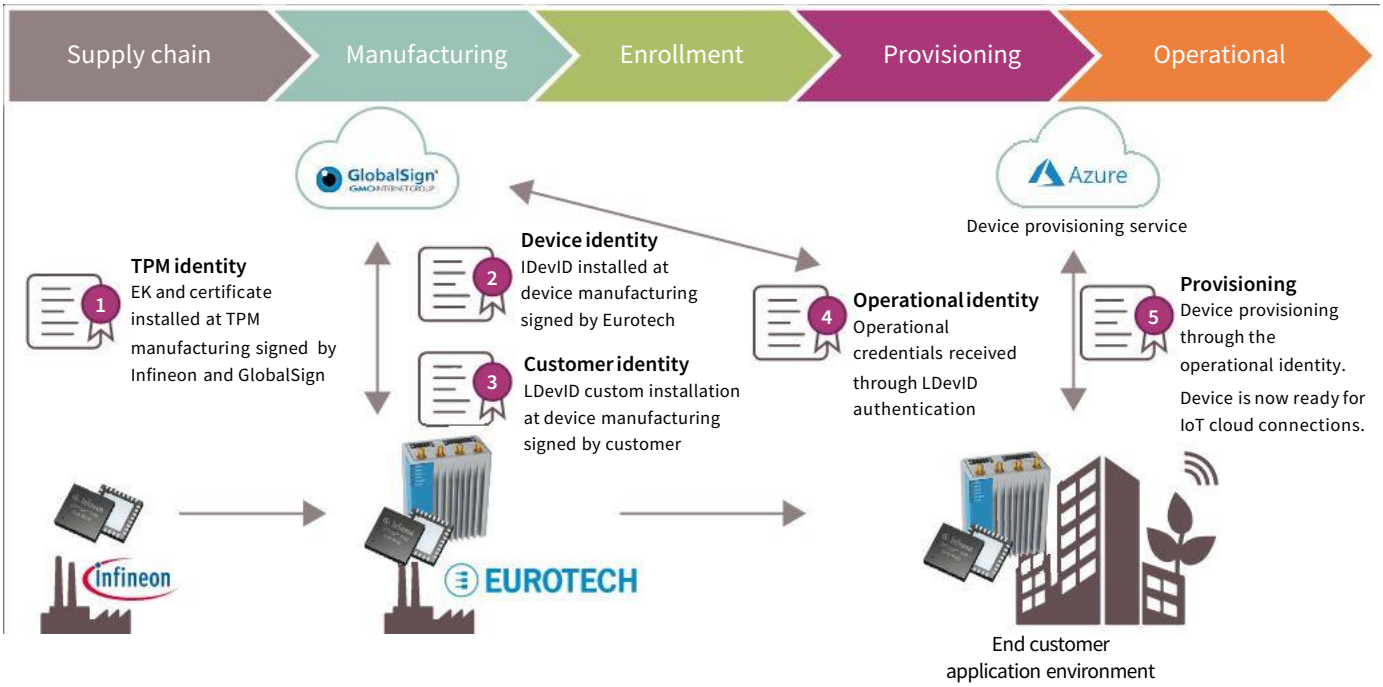


图3：设备标识生命周期

Eurotech设备是具有基于802.1AR标准的设备标识。在制造时，Eurotech创建并安装初始设备标识符（IDevID）。由Eurotech签署的IDevID证书通过将其识别为真正的Eurotec设备并指定其设备类型和序列号来证明平台的完整性。

IDevID密钥和证书分别为存储在TPM 2.0，有效保护它们在设备的使用寿命内不被篡改。

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	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

图4：信托链运营蓝图

为了实现零接触供应，Eurotech提供定制服务，在制造时安装补充的本地重要设备标识符（LDevID）。LDevID隶属于设备所有者并由其CA签名。此预配置补充了IDevID，用于身份验证和设备授权，以及Azure IoT身份服务的安装/配置（具有其唯一的LDevID）。

锚定和存储的LDevID在TPM中（图4），并利用可访问的所有者存储层次结构（图5）。这些身份的创建和管理通过企业级PKI基础设施和基于标准的协议进行控制。

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.

图5：安全设备标识（DevID）

IETF的RFC 7030中描述的安全传输注册（EST）是一种用于从CA注册X.509证书的协议。与其他协议相比，EST的优势在于其简单性和安全性。该协议的功能很简单，可以像许多REST API一样操作。EST的核心和最常用的功能是/simpleenroll和/simplerenroll端点（图6）。由于EST利用TLS实现传输安全，基于相互证书的身份验证可以用于验证以前颁发的身份，例如设备制造商颁发的IDevID。

通过将可信设备交付到现场位置，网络认证、注册和设备供应完全自动化。其他云服务和设备或物联网应用程序特有的其他功能以相同的方式提供服务。生命周期证书管理可扩展到全部设备的更新使用，设备的最终退役，并且确保设备访问和授权始终是最新的。

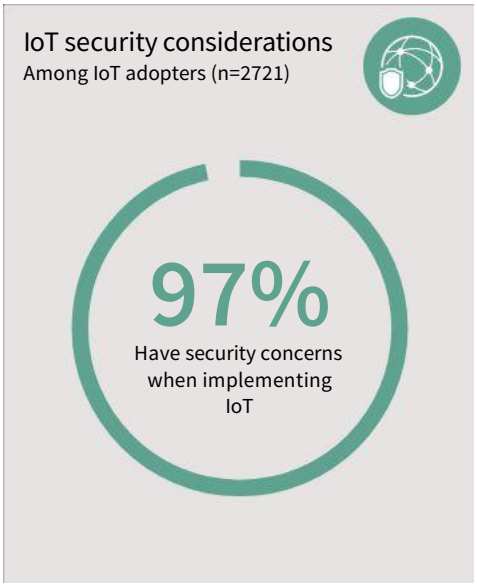
图6:EST插图

值得信赖的解决方案

毫不奇怪，几乎所有实施物联网作为数字化转型战略一部分的企业都会将安全作为首要考虑因素（图7）[4]尽管具体情况各不相同，但许多最常被提及的问题都围绕着认证和批量管理问题。从网络中的每个设备开始实施深度安全，解决了这些问题，这一事实也使可信身份成为成功部署和终身运行的先决条件。

本文描述的基于证书的物联网设备标识，并且基于标准的定义、发布和生命周期管理，不仅仅是自动化、零接触供应的基础。它是设计安全性的基石，应用于每个具有网络访问能力的设备，为物联网解决方案提供了成功和终身价值。

虽然安全性对物联网的采用是一个低阻碍，但它是实施过程中的一个考虑因素，大约一半的组织将数据隐私放在首位



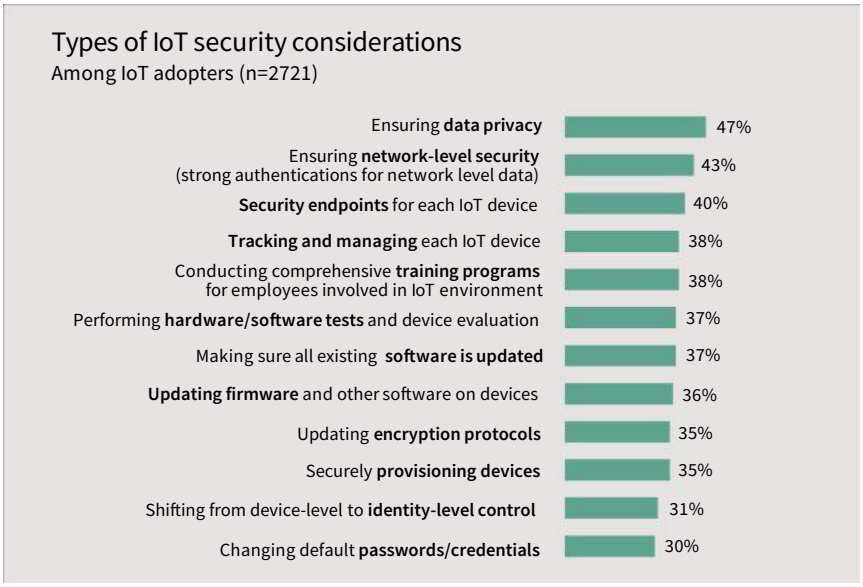
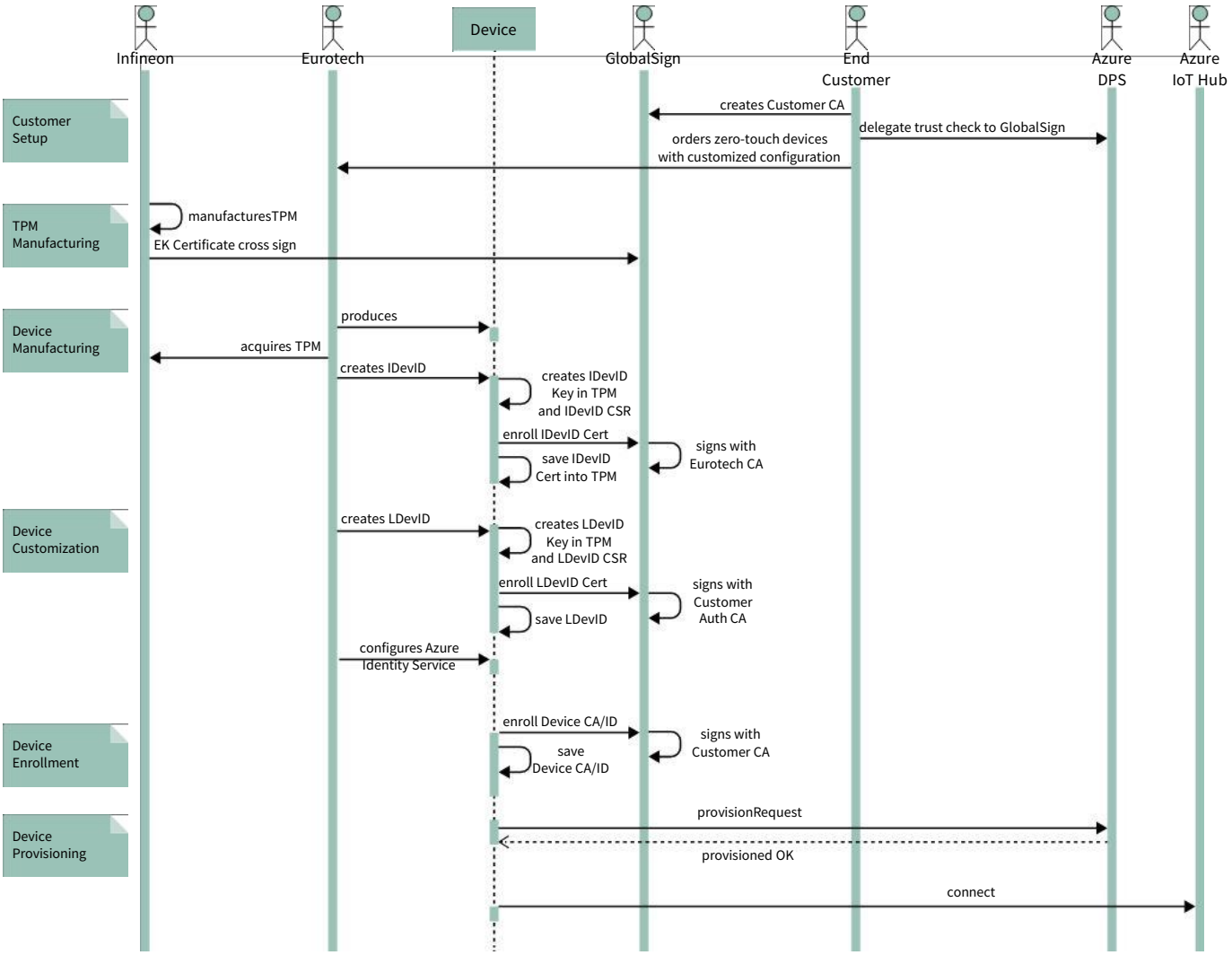
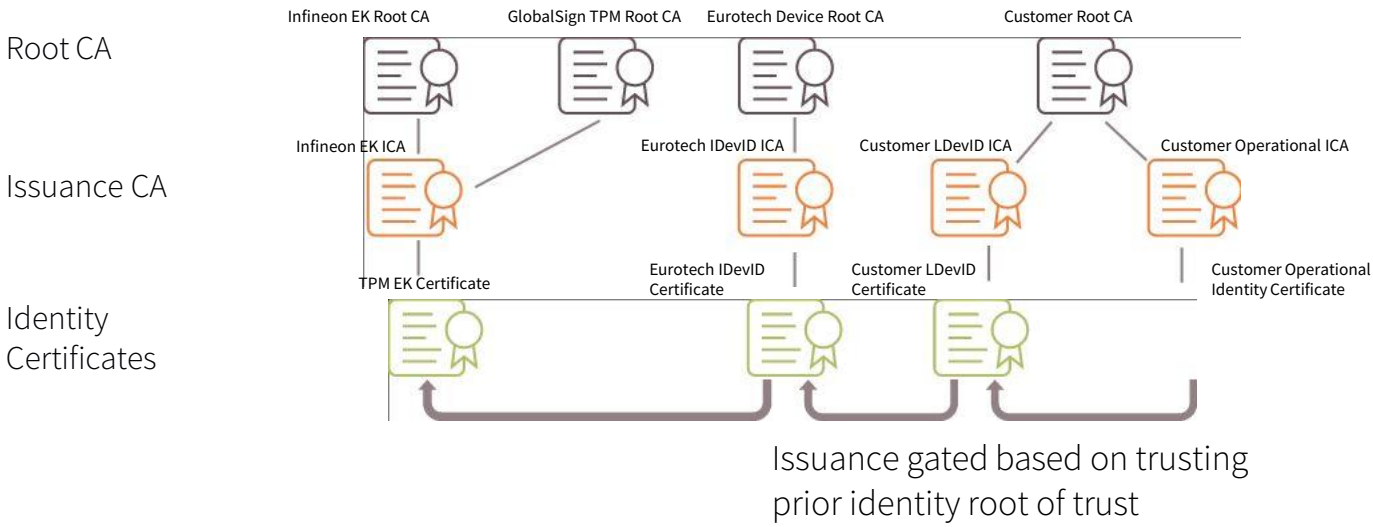


图7：物联网安全注意事项

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



附录图像



PKI解决方案层次结构

www.infineon.com/cloud-security
www.globalsign.com/en/internet-of-things
https://azure.microsoft.com/overview/iot/
www.eurotech.com/en/products/iot

发布信息：
Infineon Technologies AG
81726 Munich, Germany

Date: 04/ 2021

特别注意：

本文件仅供参考，本文件中提供的任何信息在任何情况下均不得被视为对我们产品的任何功能、条件和或质量或特定用途的任何适用性的保证或描述。关于我们产品的技术规格，请参考我们提供的相关产品数据表。我们的客户及其技术部门需要评估我们的产品对预期应用的适用性。

我们保留随时更改本文件和/或此处提供的信息的权利。

其他信息：

有关技术、产品、产品应用、交付条款和条件和/或价格的更多信息，请联系您最近的Infineon technologies办公室（www.Infineon.com）

警告：
由于技术要求，我们的产品可能含有危险物质。有关问题类型的信息，请联系您最近的Infineon Technologies办公室。除非我们在Infineon技术授权代表签署的书面文件中明确批准，否则我们的产品不得用于任何危及生命的应用，包括但不限于医疗、核、军事、生命关键或产品故障或使用后果可能导致人身伤害的任何其他应用。