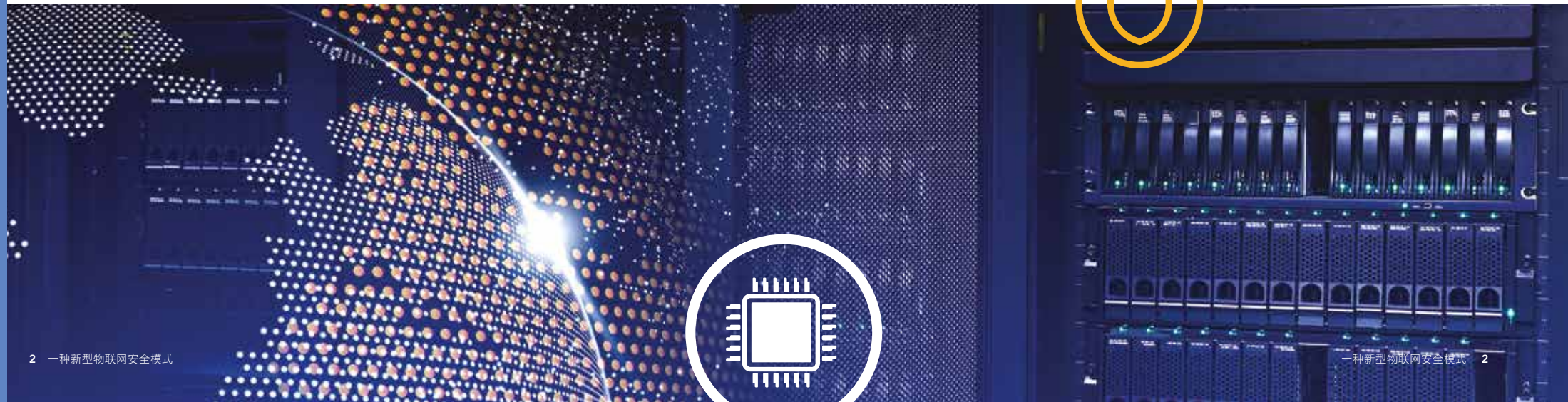

NXP
一种新型物联网
安全模式
易信任，易使用

目录

一种新型*物联网安全模式*



01 当今的物联网

机遇和风险的微妙平衡

物联网(IoT)现已成为一种日常现实。从公用事业基础设施、工业控制应用、医疗设备到智能家用电器、健身手环和自行车共享服务，更不必说智能手机和联网车辆，今天的物联网随处可见。

物联网发展迅速

物联网的经济影响以数万亿计，而物联网设备的数量则以数十亿计。市场分析人士称，2017年，互联设备已经超过50亿台，预计到2020年将超过120亿台（Gartner，2017年）。

为了支持这种快速扩张，企业供应商正在迅速扩大其私有云产品，包括阿里巴巴、Amazon Web Services、Google、IBM和Microsoft在内的知名互联网公司正在建立自己的云服务。

连接造成严重的漏洞

严峻现实是，互联设备是那些寻求未经授权访问网络、恶意控制设备或窃取物联网收集数据的人员的潜在目标。物联网生态系统的日益复杂加剧了这些危险，因为许多供应商提供的设备以及提供不同程度的安全可能导致意外的漏洞、意外的结果和不安全的操作。

例如，任何类型的物联网连接设备，无论是空气压缩机、洗衣机还是客车，都可以远程控制或触发，以不安全的方式运行。更重要的是，如果掌管能源和水分配的智能电网被篡改或非法访问，会对人类健康和社会安全构成重大威胁。

那些企图伤害或窃取信息的人通常迅速利用漏洞，并不断开发新的方法来获得访问、对系统发起黑客攻击和攫取数据。这样的后果会是毁灭性的。

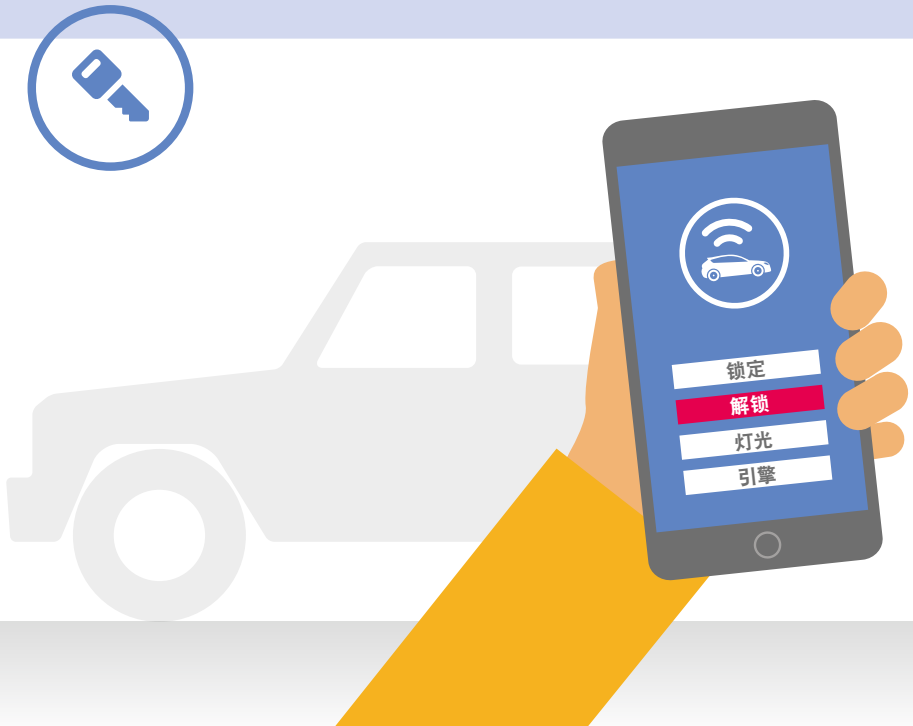
物联网机遇	物联网风险
• 改进的资产利用率 • 实时优化 • 对最终用户更深入的了解 • 增强的决策能力 • 对实物资产更多的自主操作 • 更轻松地访问信息和服务	• 网络犯罪、网络战争和网络恐怖主义 • 数据和隐私侵犯 • 僵尸网络、勒索软件和其他恶意软件 • DDoS攻击和其他类型的破坏 • 产品远程控制故障 • 盗窃知识产权(IP)

潜在的回收成本巨大

仅在过去两年，网络犯罪造成的经济损失就超过了1万亿美元。即使是阻碍操作但无法检索敏感数据的有限恶意攻击，也会让一个组织在丢失生意、商誉受损、临时解决办法、产品召回、公共关系和长期解决方案方面蒙受数亿美元的损失。如果涉及人身伤害或其他类型的赔偿责任，也有可能产生法律费用。最终用户还可能需要承担其他费用，如与勒索软件有关的费用。

没有伤害，但代价高昂

2015年，菲亚特克莱斯勒召回了140万辆汽车，而此前一名安全研究人员发现了其“互联汽车”软件中的漏洞，并在《连线》杂志上就此撰文。在一次真实的道路驾驶演示中，研究人员能够控制Jeep切诺基车型的车载计算机。他们远程提高了车辆的速度，控制了它的刹车，并在某些情况下，控制了车辆的转向。虽然没有与这一发现直接相关的事故，召回可能受到影响的车辆也只是一个预防措施，但菲亚特克莱斯勒仍然付出了高昂的代价，包括召回和修理费用、对Jeep品牌造成的损害以及潜在的法律责任。



选择正确的保护方式

知道每个物联网设备都需要基本的保护是一回事，但是实现这种安全最好的方法是什么呢？毕竟，并非每一种设备都面临同样的风险状况，与家庭WiFi网络连接的智能人偶就与核电站的控制机制不同，而且目前仍有必要在保护类型与实施和维护这种保护的成本之间达到平衡。

在定义物联网设备的安全性时，首先要考虑的是工作环境。设备将如何与其周围的系统交互？与这些交互相关的具体风险是什么？

例如，哪些物联网设备会向云端上传数据，而哪些云服务将接收数据？谁来控制每台设备？哪些硬件将用于驱动设备，哪些软件将获许运行，以及何时运行？账单是否与物联网设备的使用有关？物联网设备会与潜在的敏感设备和应用共存吗？

通过将每个设备作为一个更大的生态系统的一部分，并预计该特定生态系统内的威胁，就可以更容易地知道哪种保护最有效，以及如何部署它。

02 物联网设备需要持续保护

由始至终

物联网的安全性不仅仅是保护连接到网络的设备。在物联网生态系统的几乎每一个点上，在任何物联网设备的整个生命周期，都有篡改或滥用的机会——从设计和制造到供应链内货品的运输方式、子组件的集成方式，以及设备的分布、部署甚至是销毁的方式，无一例外。

制造和分销

在工厂或供应链中，IC和设备受到恶意软件注入、伪造、密钥捕获和安全后门创建的影响。

部署和运营

一旦实地运行，IC和设备就容易遭受各种逻辑攻击，包括恶意软件注入、未经授权的连接、窃取未加密数据和恶意软件更新，以及涉及篡改或逆向工程的物理攻击。

设备退役

当IC和设备退役或被停止使用时，它们存储在板上的任何使用记录、个人信息或登录凭据都可能成为尝试和访问该数据的物理和逻辑篡改的目标。

*危险*无处不在

虽然今天的新闻媒体倾向于强调针对薄弱设备安全漏洞的利用（如未加密的连接或不可靠的访问控制），以及分布式拒绝服务(DDoS)攻击等所造成的破坏，但破坏类型多种多样，而且只会越来越多。例如，远程、可扩展的攻击现在可以在物理硬件级别提取信息或以物理方式更改内存内容，而这些内容直到最近才能通过本地攻击实现。

攻击类型	工作原理
社会工程学	被个人用来提示他人攻击信息系统的各种技术（包括谎言、冒充、欺骗、贿赂、勒索和威胁）。
弱安全性	对未得到充分保护的系统的利用，这包括大量不良安全习惯，包括使用不采用加密、数据完整性或身份验证的连接、使用不可靠的访问控制（涉及默认密码或易于甚至可公开访问的未受保护的凭据）、使用通过暴力攻击或穷举攻击很容易被黑客攻击的系统，以及使用配置欠佳的通信协议栈，保持通讯端口开放等等。
错误利用	利用系统漏洞（如软件或硬件错误）执行意外操作，包括数据访问、任意代码执行和拒绝服务。
旁路攻击	通过本地或远程观察和测量系统操作的物理方面，如时序、功耗、电磁泄漏，甚至声音，可以推断出某些机密（包括密钥）并用来操控或破坏系统。
故障注入	在本地或远程，通过系统的硬件或软件会更改系统行为。还可以修改内存位置、篡改保险丝、更改总线值等。
制造攻击	在生产过程中造成的损害，如窃取知识产权(IP)或密钥证书、降低安全级别、增加隐藏功能或改变功能，包括非法修改软件或引入假冒组件。
软件/硬件逆向工程	对于软件，攻击者的目标通常是破译程序员掩饰代码运行方式的意图；而对于硬件，攻击通常涉及突破制造过程中设置的隐藏电路结构的物理屏障。

我们从Heartbleed中学到了什么

2014年，研究人员发现了**Heartbleed**，这是OpenSSL密码库中一个特别危险的漏洞，它让远程攻击者绕过入侵检测器，在访问机密信息（包括私钥、登录信息、密码、信用卡号码、电子邮件和即时消息）时不留下任何痕迹。

由于被OpenSSL的核心开发人员所忽视，并且在将近两年的时间里没有被发现，有三分之二的互联网服务器上可能出现了Heartbleed。OpenSSL社区使用一个补丁快速做出响应，但是在已经投入运行的嵌入式系统中部署这样的补丁是一个极大的挑战。

可能仍有一些物联网部署还需要使用该补丁进行升级，这也是为什么物联网安全在很大程度上是一个实现的问题，以及为什么正确保护物联网设备所使用的隐私数据是如此重要。

*强大的防御措施*自会带来回报

保护重要的基础设施

与能源和化学品的产生和分配有关的通信网络是潜在的破坏目标。ISA/IEC 62443标准系列定义了实施电子安全工业自动化和控制系统(IACS)的程序，旨在保护这些网络。遵循此标准提供了网络安全是智能电网开发和运行的制度化部分的保证。

保持社区和企业持续运营

24小时运营是许多物联网应用的重要组成部分，尤其是在智能城市和工业4.0中更是如此。无论是智能公用电网、车间的精密机械、供应链中的自动化，还是智能城市交通，采用行业标准方法为实现强大的身份验证、有效的数据保护和精确的命令控制而精心设计的系统架构，都能提供最大限度地减少与设备安全相关的潜在停机时间所需的保护。

在适当安全的情况下，物联网部署在其整个生命周期内都受到保护，并能有效地保护数据、提高生产力、保障运营和保护人员。

保护个人隐私

处理与人员、他们的个人偏好和行为或他们的购买习惯有关的信息的物联网部署需要保护这些信息。从2018年5月开始，在欧共体运营的实体必须遵守通用数据保护条例(GDPR)，该条例规定如何管理、保护和处理从欧盟居民收集的数据。GDPR是确保数据收集安全的良好指南，即使在欧盟以外的部署中也是如此，因为它规定了维护隐私的几个关键要求。GDPR正得到支持，并促使欧盟网络与信息安全局(ENISA)提出安全法规的基准要求，以及测试和认证的建议。

保护健康和机密

针对医疗设备和IT网络的恶意编程代码和网络攻击可能破坏医疗系统，危及人们的生命。更重要的是，病人的病历和设备收集的任何与健康有关的信息都需要保密。最近发布的UL 2900-1标准涵盖了可连接网络的产品中的软件网络安全，要求对医疗设备进行评估和测试，该标准是美国食品药品监督管理局(FDA)的指导模式。

03 真正的保护始于...

*芯片级*的安全

由于在物联网中有很多潜在的破坏方式，因此互联设备需要一套全面的保护措施。在芯片级加强保护是为设备提供必要防御措施的最好方式之一。主要有以下原因：

01

芯片是设备的核心

现在越来越多的互联设备是复杂的系统，有硬件、固件和软件在不同的抽象层运行。每个层都依赖于其下面层的组件和操作。

例如，用户界面需要信任操作系统，操作系统需要信任固件，而固件需要信任在芯片层运行的硬件电路。这就创建了一个安全层次结构，并且需要建立一个坚实的基础。

安全始于*信任根*。芯片是经过验证，受管理的信任根的锚点。

02

芯片值得信赖

这种安全层次结构的起点，即支持抽象层的基础，被称为信任根。信任根天生就值得信赖。它可以依赖，具有很高的可信度，没有风险。正确的信任根为安全奠定坚实的基础。就像在沙滩中用砖砌的墙不稳定，没有坚实的信任根，电子系统就不可能安全。

芯片是信任根的理想来源。虽然代码行、内存中的数据、操作系统和用户界面相对容易更改或损坏，但芯片中物理隔离的程序和数据，或安全保存在不可变芯片中的程序和数据，都是高度稳定的，难以更改。

03

实施很重要

安全是一个弄清细节的问题。即使是在实施中的任何一点上犯的最小的错误，最终也会造成漏洞，使整个设计处于危险之中。

有效的安全解决方案来自于严格的开发过程，具有明确定义的设计规则，经过仔细检查的多次迭代，以及对设计中涉及的许多子组件的全面控制。

开发安全性还需要系统层面的思考，以便确定更全面的风险状况，并从多层缓解战略和验证过程中获益，以加强防御。

更重要的是，随着消费者和服务提供商寻求对物联网产品得到充分保护的更大保证，进行验证实施是否符合安全要求的第三方评估变得越来越重要。

04 即插即信

支持*“即插即信”*的方式以保障物联网安全

在恩智浦，我们相信强大的安全性并非难以实现。

我们还认识到，最有效的安全解决方案既能提供简便性，又能免除后顾之忧。我们正在重新审视物联网的安全性，并为开发人员创造新的方式，以在简化设计流程的同时加强保护。

我们基于芯片的安全解决方案从一开始就成为物联网的一部分，我们不断地在这一开创性工作的基础上改进我们的算法，发展我们的架构。就像“即插即用”方法简化了早期计算机设置的配置一样，我们的“即插即信”方法简化了在当今物联网设备中实现强大的安全机制。

无比坚固的*信任根*

我们的独立安全IC旨在提供一个安全、独立的环境，用于准备和执行对物联网中的安全操作至关重要的身份验证任务。IC旨在建立一个屏障，将关键安全进程与物联网应用软件及其相关复杂性隔离开来，以便进程能够在受保护的“沙盒”环境中运行。

我们通过对安全密钥的银行级保护来保护这个孤立的环境，针对各种攻击场景采用100多个硬件和软件对策。我们将安全的非易失性存储器集成到IC中，以便安全地传输和管理密钥，并在安全制造环境中提供往芯片注入密钥的的专用密钥管理流程。

因此，安全凭据从设备创建到停用一直受到保护。上传数据的来源可以信任，实时自动化系统使用的命令源可以被认为是可靠的，与设备交换的任何私人信息在传输过程中都会受到保护。通信仍然是真实和保密的，数据保持不变，完好无损。

确保连接安全

连接性是物联网操作的基本要素，在要安全地将物联网设备集成到网络、基础设施或云中的服务时，首要任务是保护确保该连接完整性和数据的保密性。

我们隔离了对密钥证书的保护，因此保护连接安全的任务仍然与系统的其他部分是分开的。结果是可以用更强大、更可靠的方法保护连接性。

我们的独立解决方案旨在建立与物联网平台的安全连接，并支持开箱即用的即时注册服务。

易*信任*

按照我们开发安全性需要遵循原则和关注细节的理念，我们关注整个设备生命周期，预测相关的威胁，并建立在多个层面起作用的全面保护，以确保安全、可靠的操作。我们的解决方案因其安全创新而得到认可，我们经过通用评估准则(Common Criteria)认证的产品组合是业内最丰富的产品组合之一。

经过验证的设备来源

来源可疑的产品可能有攻击者随后可以利用的内置后门，并可能影响可靠性，导致系统故障、身体损伤，甚至人身伤害。我们的设备来源解决方案允许物联网设备在其生命周期的任何时刻确认它们的真实身份。在设备的整个生命周期，即使在停用之后，原始数据仍然是保密的，因此黑客就少了一个重新使用这些信息的方式。

更安全的无线更新

在无线(OTA)更新中，固件的无线传输是一种升级功能和保持安全功能更新的方法，但是需要小心操作以避免引入风险。我们基于芯片的安全性通过在现场安全地部署与固件访问和验证相关的可信数据存储库，可以便捷地保护OTA更新。安装程序支持对代码的访问控制，支持验证代码的来源和完整性（特别是在遗留或资源受限的平台上），并防止固件版本降级。

加强网络边缘的安全性

处理器密集型的复杂物联网设备的出现，包括工业机器人、新消费电子设备和越来越多的自动驾驶汽车，正在将处理过程从云端转移到设备本身的网络边缘。边缘计算可防止云连接被数据压垮，并通过减少延迟来支持更快的操作，特别是在实时系统中。它还可以提高效率和增强隐私，因为只需要上传删除了敏感细节的汇总信息。

我们的安全IC旨在保护边缘设备。在独立的环境中，没有与云的连接，IC可安全地管理与其他节点的交互，如果需要建立外部连接，则IC也管理这些交互。

易*使用*

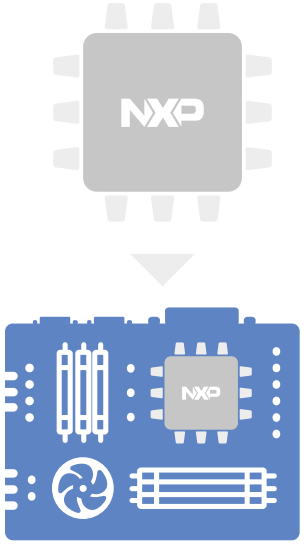
我们的安全解决方案节省时间而不走捷径。我们提供防止未经授权的访问和保护数据所需的机制，并预集成功能，因此所涉及的步骤更少。

就是简单三步

因为我们的安全IC可以包含设备安全连接到公共或私有云所需的密钥，所以只需三个步骤即可建立连接。预集成的片上应用已包含安全访问所需的安全代码。

IDC预测，最早在2021年，*43%的物联网计算*将在网络边缘。

1.

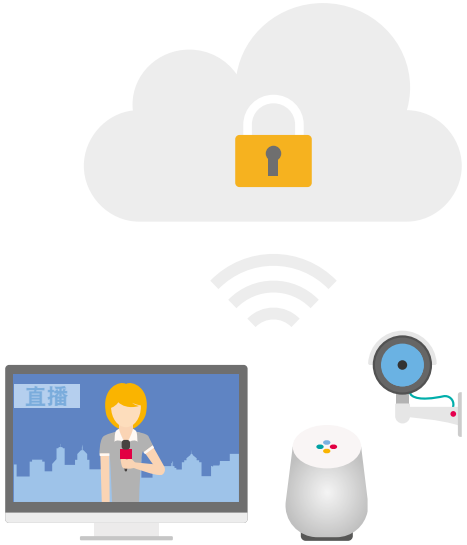


把恩智浦**安全IC**放到PCB板上

2.

上传**证书颁发机构的**证书或在云仪表板上选择设备标识符

3.



打开物联网设备并接入将是**自动**而且**安全**的

全自动密钥管理

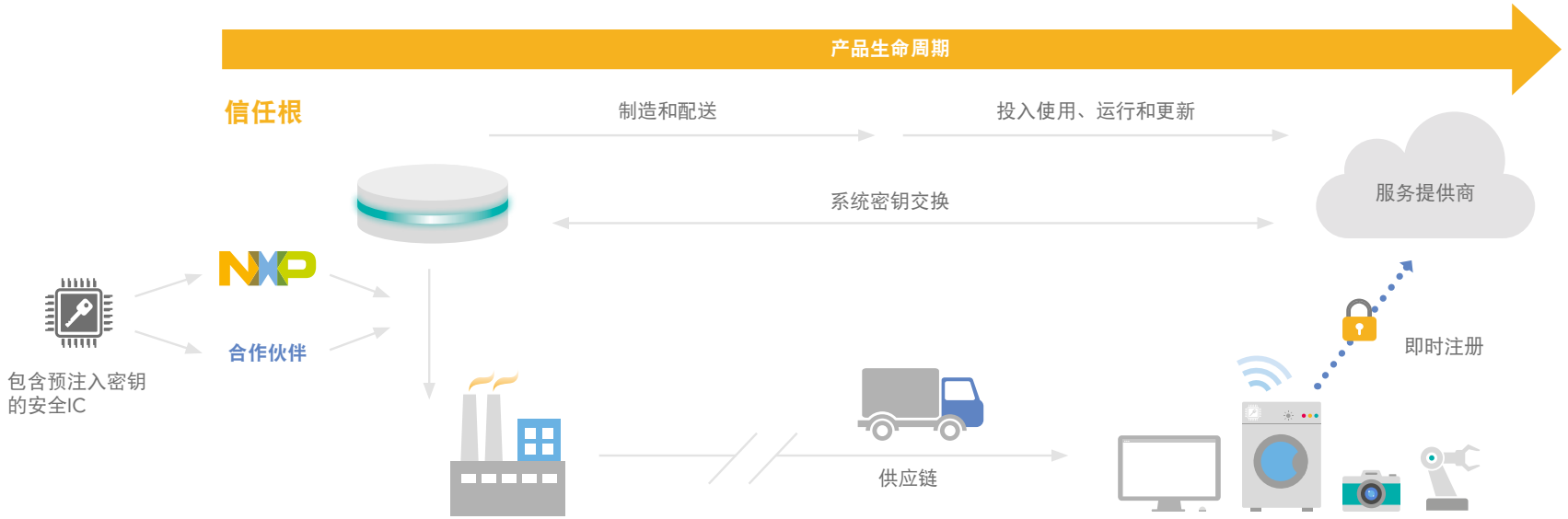
生成安全访问所需的密钥和证书是一个相对复杂的过程，如果操作不当，可能会产生漏洞。手动配置会导致错误，在有更多设备时很难进行扩展。此外，为了确保密钥的安全，密钥注入应该在可信的环境中进行，在具有严格控制的访问、仔细的人员筛选和保护IT系统以防止网络攻击和证书被盗等安全特性的场所中进行。我们在芯片级实现的安全信任配置服务，旨在顺利接入物联网设备，同时无需OEM投资拥有这种场所，还消除了他们密钥管理的复杂性。通过与编程中心合作，恩智浦支持任何规模的物联网部署。此外，不必与服务提供商协调密钥共享，安全信任配置服务还可以应用于连接到同一服务的多个第三方OEM设备。

快速集成

通过集成通讯协议栈，提供用于主要应用场景的示例代码、广泛的应用说明以及用于i.MX和Kinetis微控制器的兼容开发套件，我们就可以启动设计。调试版本以及对示例应用程序的轻松访问简化了最终的系统集成。

通过与云提供商的合作，我们能够提供从边缘到云的全面安全解决方案。我们的预集成解决方案专为特定的云提供商而构建，可将复杂性降到最低，减少安全物联网设备的开发时间，并在整个扩展的生态系统中提供保护。

恩智浦安全解决方案提供生态系统级别上的保护

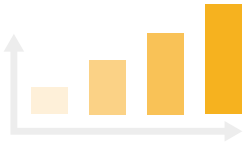


多元化安全

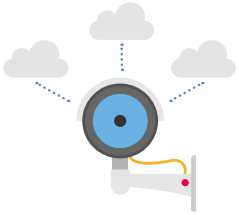
易于集成的全自动解决方案

预集成安全和系统级性能

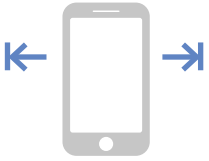
成熟可靠、屡获殊荣的方法



可针对每次实施（无论大小）快速扩展



支持新业务模式的多应用程序平台



端到端安全：从设备到边缘到云

亮点产品	
与云、服务和边缘计算平台的安全连接	A710xCH（Amazon Web Service和私有云） A710xCL（中国的阿里云服务）
设备来源证明	A1006
计量设备基础设施	A70CU（英国） A80SM（德国）

恩智浦的优势

我们知道物联网安全性不仅仅是一方面的，而且没有两个物联网部署是完全相同的。这就是为什么我们在设备运行之外，在物联网生命周期的每一个阶段，为每种类型的物联网生态系统解决安全问题的原因。我们的物联网产品组合将高质量的处理能力与先进的连接和强大的安全性结合在一起，使我们为物联网开发提供“一站式”服务。此外，作为跨广泛行业的安全解决方案提供商，我们已经与重要生态系统公司建立了长期的关系，包括第三方开发人员、OEM、系统集成商和服务提供商。我们的解决方案旨在保护它们对生态系统的贡献，我们利用从每一个新挑战中获得的经验，为今天的物联网创建量身定制的解决方案。

- **通过非常广泛的经过通用评估准则(Common Criteria)认证产品组合建立的安全领导地位**
- **在安全微控制器方面的技术领先**
- **一个提供全面解决方案的提供商**
- **广泛的生态系统关系**
- **针对大小实施快速扩展能力**
- **支持新业务模式的多应用程序平台**

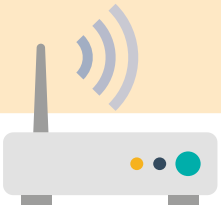
05 恩智浦安全

现实世界中的安全性

我们基于芯片的安全解决方案广泛应用于各种物联网应用，包括智能城市和智能能源、家庭自动化、个人护理、工业4.0和智能移动（包括远程信息处理）。下面是物联网部署使用我们的解决方案来保护连接和对数据保密的一些例子。

“在我们的智能网关中运用恩智浦安全技术帮助我们实现了维护客户数据的安全性和隐私的目标，并使我们朝*遵守GDPR*的方向更近了一步。”

Dr. Neuhaus Telekommunication



智能家居

使用ENTR智能锁实现安全访问控制

通过全球高安全性锁具和门禁解决方案提供商Mul-T-Lock提供的**ENTR智能锁解决方案**，您可以使用智能手机、指纹、个人代码或遥控器打开大门。业主几乎随时可通过创建和撤销密钥来管理访问，甚至在密钥证书丢失时也可以取消访问。电池供电系统由低功耗恩智浦安全解决方案保护，该解决方案支持安全通道上的蓝牙低能耗(BLE)连接，从而在脱机环境中建立与移动设备的信任关系。

智慧城市

德国智能能源网关的认证安全

恩智浦与**智能计量网关**提供商合作，包括Dr. Neuhaus Telekommunikation和Power Plus Communication，共同开发符合德国联邦信息安全办公室BSI发布的安全保护规定严格准则的安全解决方案。恩智浦的嵌入式安全模块旨在提供安全访问能源和服务提供商报告的消费者计量数据所需的保护，以及符合隐私要求的测量数据传输。这样的设置让服务部署准备好以符合GDPR要求。

公用事业仪表

英国的安全、全自动入网启动

作为多年实施计划的一部分，英国智能电网基础设施将包括1亿多台设备，并配合使用住宅通信集线器、煤气表和电表，以及家用显示屏，优化能源管理。恩智浦技术正被用于保护大部分的基础设施，通过安全连接芯片组向连接国家数据通信中心的集线器和仪表提供经身份验证和全自动入网启动。简单快捷安装是关键，因为花在设置上的每一分钟都是昂贵的。我们的开创性方法以其安全性和简便性的独特组合而获得认可，并且恩智浦网络安全在2014年的欧洲与英国智能计量峰会上荣获了著名的年度创新奖，因而获得更广泛的业界认可。

实现新的突破

要了解有关恩智浦物联网安全创新解决方案的更多信息，请访问

nxp.com/internet-of-things

发布日期：2018年2月