
NXP
A new kind of
IoT Security
Easy to Trust. Easy to Use

Contents

A New Kind of *IoT Security*

01

Today's IoT: A Balance of Opportunity and Risk

The Internet of Things (IoT) is now an everyday reality. From utility infrastructures, industrial control applications, and medical equipment to smart-home appliances, fitness bracelets, and bike-sharing services – not to mention smartphones and connected vehicles – today's IoT is all around us.

The IoT is Growing Quickly

The economic impact of the IoT is measured in trillions, and the number of IoT devices is measured in billions. Market analysts report that, in 2017, there were already more than 5 billion connected devices, and anticipate there will be more than 12 billion by 2020 (Gantner, 2017).

To support this rapid expansion, industrial suppliers are moving quickly to broaden their private-cloud offerings, while prominent internet players, including Alibaba, Amazon Web Services, Google, IBM, and Microsoft, are establishing their own cloud services.

Connectivity Creates Significant Vulnerabilities

The unpleasant reality is that connected devices are potential targets for those seeking unauthorized access to the network, malicious control of the device, or theft of IoT-collected data. The increasing complexity of IoT ecosystems compounds these dangers, since devices supplied by many vendors and offering varying levels of security can lead to unexpected weakness, unanticipated results, and unsafe operation.

For example, any type of IoT-connected equipment, be it an air compressor, a washing machine, or a passenger vehicle, can be remotely controlled or triggered to operate in an unsafe manner. What's more, the smart grids that govern the distribution of energy and water can, if tampered with or illicitly accessed, pose a significant threat to human health and our safety as a community.

The people aiming to do harm or steal information move quickly to exploit weaknesses, and continually develop new ways to gain access, hack systems, and grab data. The results can be devastating.

IoT Opportunities	IoT Risks
• Improved asset utilization • Real-time optimization • Greater end-user insight • Enhanced decision-making • More autonomous operation of physical assets • Easier access to information and services	• Cybercrime, cyberwar, and cyberterrorism • Data and privacy breaches • Botnets, ransomware, and other malware • DDoS attacks and other types of sabotage • Product malfunction through remote control • Theft of intellectual property (IP)

The Potential Recovery Costs are Enormous

In the past two years alone, the economic damage of cybercrime topped a trillion dollars. Even a limited malware attack, which hinders operation but fails to retrieve sensitive data, can cost an organization hundreds of millions of dollars in lost business, damaged reputation, temporary work-arounds, product recalls, public relations, and long-term fixes. There is also the potential for legal fees, if personal injury or other types of liability are involved. Other costs, like those relating to ransomware, can extend to end users, too.

No harm done, but a high price to pay

In 2015, Fiat Chrysler recalled 1.4 million cars after a vulnerability in their "connected car" software was uncovered by a security researcher and written up in Wired magazine. In a real-road driving demonstration, the researchers were able to take control of a Jeep Cherokee's onboard computer. They remotely increased the vehicle's speed, controlled its brakes, and, in some cases, controlled its steering. While there were no accidents directly linked to the discovery, and recalling the potentially impacted vehicles was a precautionary step, Fiat Chrysler still paid a high price, in terms of recall and repair costs, damage to the Jeep brand, and potential legal liability.

Choose the Right Kind of Protection

It's one thing to know that every IoT device needs a baseline of protection, but what's the best way to implement that security? After all, not every device faces the same risk profile – a smart action figure, connected to a home WiFi network, is different from a control mechanism in a nuclear plant – and there's the ongoing need to balance the type of protection with the cost of implementing and maintaining that protection.

One place to start, when defining security for IoT devices, is to consider the operating environment. How will devices interact with the systems around them, and what specific risks are associated with those interactions?

For example, which IoT devices will upload data to the cloud, and which cloud service will receive the data? Who will control each device? What hardware will be used to drive devices, and what software will be allowed to run, and when? Is billing associated with the use of the IoT device? Will the IoT device co-exist with potentially sensitive equipment and applications?

By characterizing each device as part of a larger ecosystem, and anticipating the threats within that particular ecosystem, it can be easier to know what kind of protection will work best, and how to deploy it.

02 IoT Devices Need Continuous Protection

Cradle to Grave

IoT security is more than about protecting a device while it's connected to a network. At nearly every point in the IoT ecosystem, and throughout the life of any IoT device, there are opportunities for tampering or abuse – from design and manufacture to the way items are transported within the supply chain, how subcomponents are integrated, how devices are distributed, deployed, and even disposed of.

Manufacturing & Distribution

While in the factory or in the supply chain, ICs and devices are subject to malware injection, counterfeiting, key capture, and the creation of security backdoors.

Deployment & Operation

Once in the field, ICs and devices are susceptible to a wide range of logical attacks, including malware injection, unauthorized connection, theft of unencrypted data, and malicious software updates, as well as physical attacks involving tampering or reverse engineering.

Decommissioning

When ICs and devices are retired or taken out of service, any usage records, personal information, or login credentials they have stored onboard can create a target for physical and logical tampering, to try and access that data.

There are *Dangers* Everywhere

While today's news outlets tend to highlight the exploitation of weak device security (such as unencrypted connections or unreliable access control), and the damage done by things like Distributed Denials of Service (DDoS) attacks, there are many different kinds of sabotage and the list is only getting longer. For example, remote, scalable attacks can now extract information at the physical hardware level or physically alter memory content, which are things that until recently were only possible with a local attack.

Type of Attack	How it Works
Social engineering	Various techniques, including lies, impersonation, tricks, bribes, blackmail, and threats, used by individuals to prompt others to attack information systems.
Weak security	The exploitation of systems that are inadequately protected. This includes a long list of poor security habits, including the use of connections that don't employ encryption, data integrity, or authentication, the use of unreliable access control, involving default passwords or unprotected credentials that are easily or even publicly accessible, the use of systems that can easily be hacked via brute-force or exhaustive attacks, and the use of poorly configured communication stacks, with ports left open, and so on.
Bug exploit	A system vulnerability, such as a software or hardware bug, is taken advantage of to create unintended behavior, including data access arbitrary code execution, and denial of service.
Side-channel attack	By locally or remotely observing and measuring physical aspects of system operation, such as timing sequences, power consumption, electromagnetic leaks, or even sound, certain secrets, including keys, can be inferred and used to compromise or break a system.
Fault injection	Modifications, performed locally or remotely, that change system behavior are introduced into the system's hardware or software. Memory locations can be modified, fuses tampered with, bus values changed, and so on.
Manufacturing attack	Damage done during production, such as stealing intellectual property (IP) or credentials, degrading security levels, adding hidden functions, or changing functionality, including illicitly modifying software or introducing counterfeit components.
Software/hardware reverse engineering	With software, the attacker usually aims to decipher the programmer's attempt to disguise how code operates, and with hardware, the attack typically involves breaking through physical barriers, put in place during manufacturing, that hide the circuit architecture.

What Heartbleed Teaches Us

In 2014, researchers discovered **Heartbleed**, a particularly dangerous bug in the OpenSSL cryptography library that let remote attackers bypass intrusion detectors and leave no trace while gaining access to confidential information, including private keys, logins, passwords, credit-card numbers, emails, and instant messages.

Having been overlooked by the core developers of OpenSSL, and having gone undetected for nearly two years, Heartbleed was likely present on two-thirds of all Internet servers. The OpenSSL community responded quickly with a fix, but deploying such a fix across embedded systems that are already in the field presents a significant challenge.

It's likely that there are still IoT deployments that have yet to be upgraded with the fix. All the more reason why IoT security is, to a large degree, a question of implementation, and why it's so important to properly safeguard the private data used by IoT devices.

A *Strong Defense* Creates its Own Rewards

Protects Vital Infrastructures

The communication networks associated with the generation and distribution of energy and chemicals are potential targets of sabotage. The ISA/IEC 62443 standard series, which defines procedures for implementing electronically secure Industrial Automation and Control Systems (IACS), is designed to protect these networks. Compliance with the standard provides assurance that cybersecurity is an institutionalized part of smart-grid development and operation.

Keeps Communities & Businesses Up and Running

Round-the-clock operation is an essential part of many IoT applications, but especially so in smart cities and Industry 4.0. Whether it's a smart utility grid, precision machinery on the factory floor, automation in the supply chain, or smart urban transportation, a well-designed system architecture – supported by industry-standard methods for strong authentication, effective data protection, and precise command control – provides the protection needed to minimize potential downtime associated with device security.

When properly secured, an IoT deployment is protected throughout its lifecycle, and effectively shelters data, fuels productivity, safeguards operation, and protects people.

Preserves Personal Privacy

An IoT deployment that deals with information relating to people, their personal preferences and behavior, or their purchasing habits, needs to protect that information. As of May 2018, entities operating in the European Community must comply with the General Data Protection Regulation (GDPR), which specifies how data collected from EU residents is to be managed, protected, and processed. The GDPR is a good guide for securing data collection, even in deployments outside the EU, since it specifies several key requirements for maintaining privacy. The GDPR is gaining support, and prompted the EU agency for Network and Information Security (ENISA) to propose baseline requirements for security regulations, with recommendations for testing and certification.

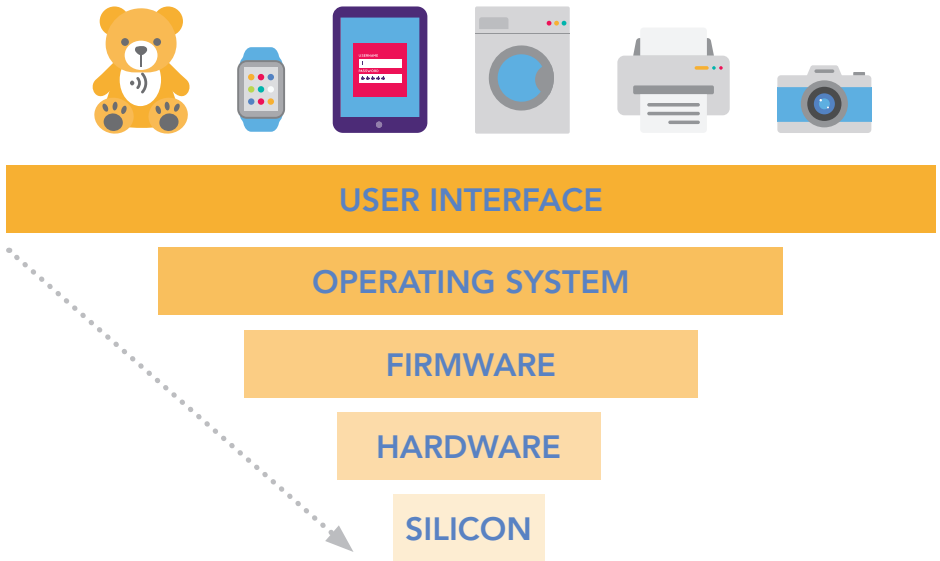
Protects Health and Confidentiality

Malicious programming codes and cyberattacks targeted at medical devices and IT networks can disrupt medical systems and put people's lives at stake. What's more, patient medical records and any health-related information collected by devices needs to remain confidential. The recently published UL 2900-1 standard, which covers software cybersecurity in network-connectable products, calls for evaluation and testing of medical devices and, in the United States, is a guidance model for the Food and Drug Administration (FDA).

03 True Protection Starts with...

Security at the *Silicon Level*

Because there are so many ways to potentially damage in the IoT, connected devices need a comprehensive set of protections. Adding protection at the silicon level is one of the best ways to arm a device with the necessary defenses. Here's why:



01

Silicon is the Heart of the Device

More and more of today's connected devices are complex systems that involve hardware, firmware, and software operating at different layers of abstraction. Each layer relies on the components and operations of the layer beneath it.

The user interface, for example, needs to trust the operating system, the operating system needs to trust the firmware, and the firmware needs to trust the hardware circuits operating in the silicon layer. This creates a hierarchy for security, and the need for a strong foundation on which to build.

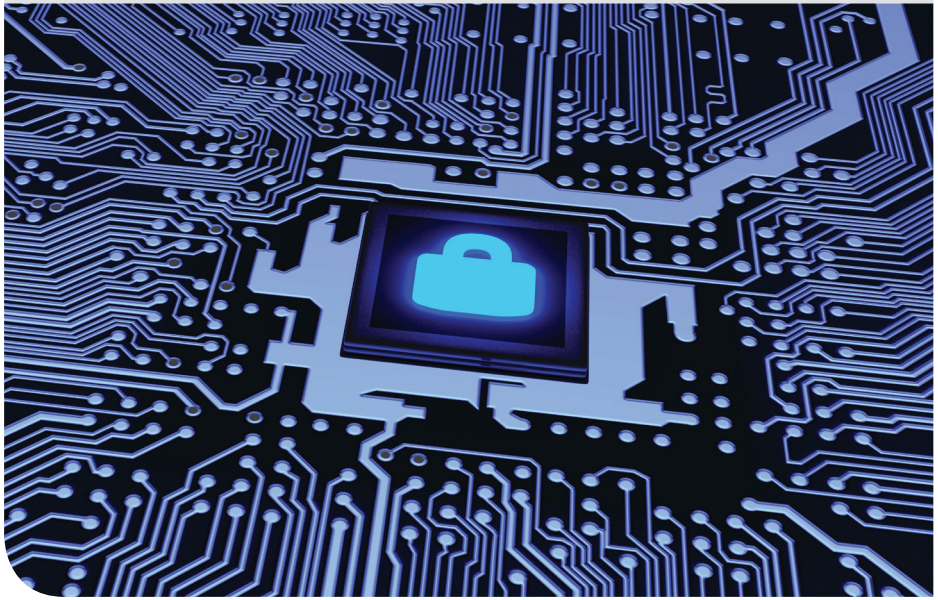
Security begins with the *root of trust*. Silicon is an anchor for a demonstrated, managed root of trust.

02

Silicon is Trustworthy

The starting point for this hierarchy of security – that is, the base that supports the layers of abstraction – is known as the root of trust. The root of trust is something that is inherently trustworthy. It's something that can be relied upon, with a very high degree of confidence, to be risk-free.
The right root of trust creates a firm foundation for security. In the same way that a wall, built with bricks placed in sand, is unstable, an electronic system cannot be secure without a solid root of trust.

Silicon is an ideal source for the root of trust. While lines of code, data stored in memories, operating systems, and user interfaces are relatively easy to alter or damage, physically isolated programs and data in silicon, or programs and data kept safe in immutable silicon, are highly stable and resistant to change.



03

The Implementation Matters

Security is a matter of getting the details right. Even the smallest of errors, made at any point in the implementation, can eventually create weaknesses and put the overall design at risk.

Effective security solutions are the result of a strict development process, with clearly defined design rules, multiple iterations of careful review, and full control over the many sub-components involved in the design.

Developing security also requires system-level thinking, so as to identify a more comprehensive risk profile, and benefits from multi-layer mitigation strategies and validation procedures, to strengthen the defense.

What's more, as consumers and service providers seek greater assurance that IoT products are adequately protected, it becomes increasingly important to have third-party evaluations that certify implementations for compliance with security claims.

04 Plug & Trust

Supporting the *'Plug & Trust'* Approach to IoT Security

At NXP, We believe strong security doesn't have to be hard to work with.

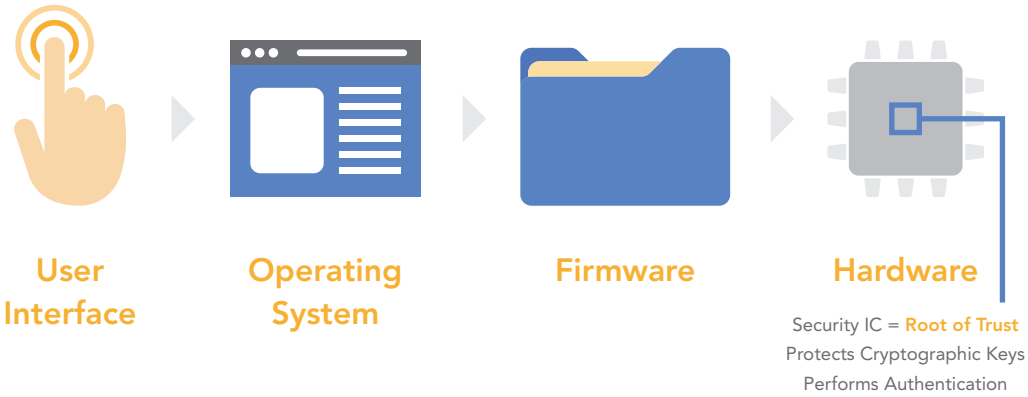
We also recognize that the most effective security solutions deliver simplicity as well as peace of mind. We're taking a fresh look at IoT security, and creating new ways for developers to add protections while streamlining the design process.

Our silicon-based security solutions have been part of the IoT since it began, and we continually build on that pioneering work to refine our algorithms and evolve our architectures. In the same way that the "plug and play" approach simplified the configuration of early computer setups, our "plug and trust" approach simplifies the implementation of strong security mechanisms in today's IoT devices.

An Exceptionally Strong *Root of Trust*

Our standalone security ICs are designed to provide a safe, self-contained environment for staging and executing the authentication tasks that are essential to safe operation in the IoT. The ICs are designed to create a barrier that isolates critical security processes from IoT application software and its associated complexity, so processes can run in a protected, "sandboxed" environment.

We secure this isolated environment with banking-grade protections for the security keys, using more than a hundred hardware and software countermeasures that target a broad spectrum of attack scenarios. We integrate secure, nonvolatile memory into the IC, so keys are securely transported and managed, and we offer specialized key management processes supported by silicon injection in a secure manufacturing environment.



As a result, security credentials are protected from device creation to decommissioning. The origin of uploaded data can be trusted, the source of commands used by real-time automation systems can be considered reliable, and any private information exchanged with a device stays protected while in transit. Communications remain authentic and confidential, and data remains unaltered and fully intact.

Securing the Connection

Connectivity is a basic ingredient for IoT operation, and when it comes to securely integrating an IoT device to a network, an infrastructure, or a service in the cloud, the first order of business is to protect the credentials that ensure the integrity of that connection and keep data confidential.

We isolate the protection of credentials, so the task of securing the connection remains separate from the rest of the system. The result is a stronger, more robust way to safeguard connectivity.

Our self-contained solutions are designed to establish a secure connection to the IoT platform, and to support just-in-time registration to services, right out of the box.

Easy to *Trust*

In keeping with our philosophy that developing security requires discipline and attention to detail, we consider the entire device lifecycle, anticipate the associated threats, and create comprehensive protections that work on many levels to ensure safe, trustworthy operation. Our solutions have been recognized for their security innovations, and our portfolio of Common Criteria certified products is one of the broadest in the industry.

Attested Device Origin

Products of questionable origin can have built-in backdoors that attackers use later, and can impact reliability in ways that lead to system failures, physical damage, and even personal harm. Our device-origin solution lets IoT devices confirm their authenticity at any point in their lifecycle. Origin data remains private throughout the lifetime of the device, even after decommissioning, so there's one less way for hackers to repurpose the information.

Safer Over-the-Air Updates

The wireless delivery of firmware, in what's referred to as "Over The Air" or OTA updates, is a way to upgrade functionality and keep security functions up to date, but the process needs to be done carefully to avoid introducing risks. Our silicon-based security provides a convenient way to protect OTA updates, with secure deployment, in the field, of a trusted repository of data related to firmware access and validation. The setup supports access control to the code, supports verification of the origin and integrity of code, particularly on legacy or resource-constrained platforms, and prevents firmware rollbacks.

Increased Security at the Edge

The arrival of complex, processor-intensive IoT devices, including industrial robots, new consumer devices, and increasingly autonomous vehicles, is transitioning processing from the cloud to the edge of the network, in the device itself. Edge computing prevents cloud connections from being overwhelmed by data, and supports faster operation, especially in real-time systems, by reducing latency. It can also boost efficiency and privacy, since only aggregated information, scrubbed of sensitive details, needs to be uploaded.

Our security ICs are designed to protect edge devices. In standalone environments, without connections to the cloud, the IC securely manages interactions with other nodes, and if there's a need to make external connections, the IC manages those interactions, too.

Easy to *Use*

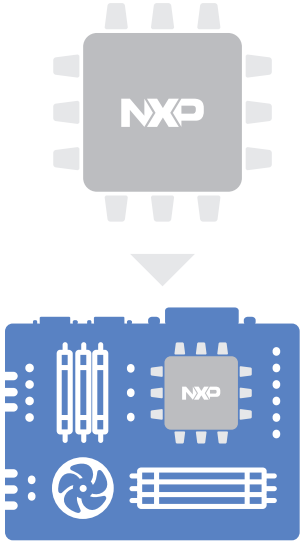
Our security solutions save time without cutting corners. We provide the mechanisms needed to prevent unauthorized access and protect data, and pre-integrate functionality so there are fewer steps involved.

Simple as 1-2-3

Because our security ICs can contain the necessary keys for the device to connect securely to a public or private cloud, it takes just three steps to establish a connection. A pre-integrated, on-chip application already includes the necessary security code for secure access.

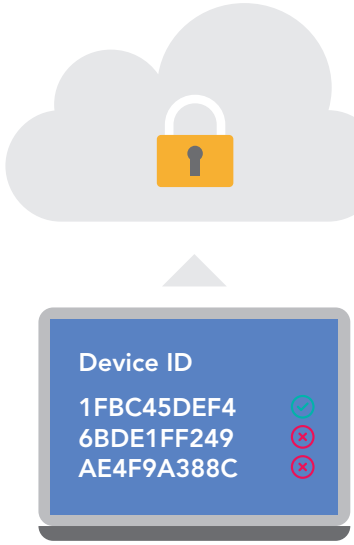
IDC forecasts that, as early as 2021, *43% of IoT computing* will occur at the edge.

1.



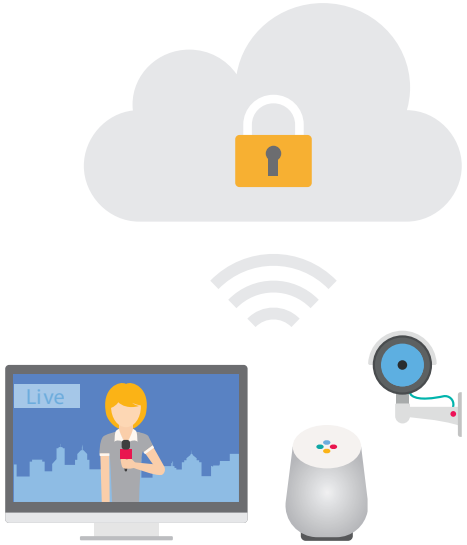
Drop NXP **Security IC** on the board

2.



Upload **Certification Authority's** certificate or select Device Identifiers on Cloud Dashboard

3.



Turn on IoT Device and onboarding will be **automatic** and **secure**

Zero-Touch Key Management

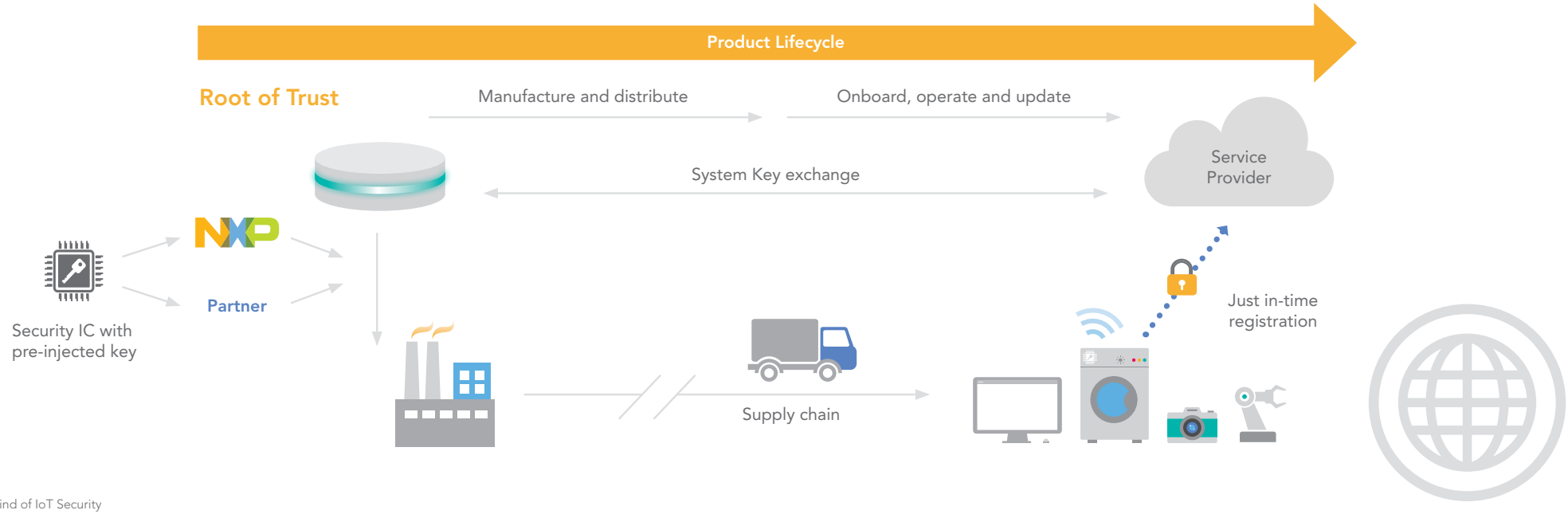
Generating the keys and credentials needed for secure access is a relatively complex process, and can introduce vulnerabilities if not done properly. Manual provisioning lends itself to errors, and is difficult to scale when more devices are needed. Also, to ensure keys are kept safe, injection should take place in a trusted environment, in a facility with security features like tightly controlled access, careful personnel screening, and secure IT systems that protect against cyberattacks and theft of credentials. Our Secure Trust Provisioning service, implemented at the chip level, offloads the cost of ownership and complexity of key management from OEMs, and is designed to create smooth onboarding of IoT devices. Through partnerships with programming centers, NXP supports IoT deployments of any size. Also, the provisioning can be applied to multiple third-party OEM devices connecting to the same service without having to coordinate key sharing with the service provider.

Quick to Integrate

We kick-start the design process by providing integration into connectivity stacks, along with sample code for major use cases, extensive applications notes, and compatible development kits for i.MX and Kinetis microcontrollers. Debug versions and easy access to sample applications simplify the final system integration.

Through our collaborations with cloud providers, we're able to offer comprehensive security solutions, from the edge to the cloud. Our pre-integrated solutions, purpose-built to work with specific cloud providers, minimize complexity, reduce development time for secure IoT devices, and deliver protection throughout the extended ecosystem.

NXP Security Solutions Deliver Protection at the Ecosystem Level

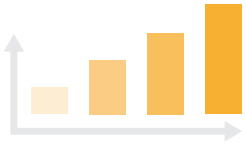


Multi-Faceted Security in One Place

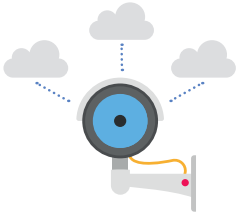
Easy-to-integrate, zero-touch solutions

Pre-integrated security and system-level performance

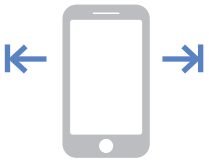
Proven robust, award-winning approach



Quick scaling for every rollout, small or large



Multi-application platforms that enable new business models



End-to-end security: from device to edge to cloud

Product Highlights	
Secure Connectivity to Cloud, Services, and Edge Computing Platforms	EdgeLock™ SE050
Proof of Device Origin	A1006
Metering Infrastructure	A80SM (Germany)

The NXP Difference

We understand that IoT security is about more than one thing, and that no two IoT deployments are exactly alike. That's why we go beyond device operation to address security at every stage in the IoT lifecycle, and for every type of IoT ecosystem. Our IoT portfolio combines high-quality processing with cutting-edge connectivity and robust security, making us a "one-stop shop" for IoT development. What's more, as a provider of security solutions across a wide range of industries, we've developed long-standing relationships with key ecosystem players, including third-party developers, OEMs, system integrators, and service providers. Our solutions are designed to protect what they contribute to the ecosystem, and we use the experience gained from each new challenge to create tailored solutions for today's IoT.

- **Security leadership with very broad portfolio of Common Criteria certified products**
- **Technology leadership in secure microcontrollers**
- **One supplier for comprehensive solutions**
- **Extensive ecosystem relationships**
- **Quick scaling for small and large rollouts**
- **Multi-application platforms that support new business models**

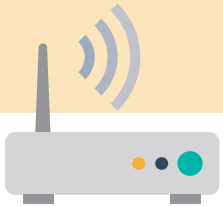
05 NXP Security

Security in the Real World

Our **silicon-based security solutions** are used in a very wide variety of IoT applications, from smart cities and smart energy to home automation, personal care, Industry 4.0, and smart mobility, including telematics. Here are just some of the ways IoT deployments are using our solutions to protect connectivity and keep data private.

"Building NXP security into our smart gateway helped us achieve the goal of maintaining the security and privacy of customer data, and brings us a step closer to ***GDPR compliance***."

Dr. Neuhaus Telekommunication



Smart Home

Secure Access Control with ENTR Smart Lock

The **ENTR Smart Lock Solution** from Mul-T-Lock, a worldwide provider of high-security locking and access-control solutions, lets you open your front door using a smartphone, fingerprint, personal code, or remote control. Homeowners can manage access by creating and revoking keys at virtually any time, and can cancel access even when the credentials are lost. The battery-powered system is protected by a low-power NXP security solution that supports Bluetooth Low Energy (BLE) connection over a secure channel, thereby building trust with mobile devices in an offline environment.

Smart Cities

Certified Security for Germany's Smart Energy Gateways

NXP worked with providers of **smart metering gateways**, including Dr. Neuhaus Telekommunikation and Power Plus Communication, to develop security solutions that meet the strict guidelines for the Security Protection Profile as issued by BSI, Germany's Federal Office of Information Security. NXP's embedded security module is designed to deliver the protection needed for secure access to the consumer metering data reported by energy and service providers, and the privacy-compliant transfer of measured data. The setup prepares the deployment to comply with the GDPR.

Utility Metering

Secure, Zero-Touch Commissioning in the UK

As part of a multi-year rollout, the UK smart-grid infrastructure will include more than 100 million devices, with residential communication hubs, gas and electricity meters, and in-home displays working together to optimize energy management. NXP technology is being used to protect a significant part of the infrastructure, with secure connectivity chipsets that provide authenticated, zero-touch commissioning of hubs and meters to the national data communication center. Simple, quick installation is key, since every minute spent on set-up is expensive. Our groundbreaking approach was recognized for its unique combination of security and simplicity, and gained broader industry recognition when the Smart Metering Europe and UK Summit of 2014 awarded their prestigious Innovation of the Year for Cyber Security to NXP.

Take the Next Step

To learn more about NXP's innovative solutions for IoT security, visit

www.nxp.com/iotsecurity