



Build **Trust** and Ensure **Privacy** in the Industrial and Consumer IoT

A Developer's Guide to NXP EdgeLock®
secure elements and authenticators

Trust is Everything

A World of Potential

In today's industrial and consumer Internet of Things (IoT), billions of connected devices collect data and add automation in ways that have already brought dramatic changes to the way we live, work and play.

Now, with the arrival of artificial intelligence (AI), industrial and consumer IoT devices promise to accelerate this transformation of daily activities, with even more ways to generate value, gain insights, increase efficiency and enhance everyday experiences.

Given this sustained momentum, the industrial and consumer segments of the IoT remain areas of remarkable potential – well within reach. However, to fully capitalize on these opportunities, we must first address one of the biggest challenges in present-day IoT applications: reducing risk.

Risk is Everywhere

Throughout the IoT, cybersecurity events, such as data breaches, malware attacks, ransomware attacks and other manipulations of network vulnerabilities, have become daily occurrences.

IoT devices of all kinds, but especially those operating in the consumer and industrial sectors, are now a favorite target of attack, even more so than desktop computers and mobile devices like smartphones and laptops.

Why the focus on IoT devices? Because any device that connects to a network is a potential launch point for mounting an attack. Any single vulnerability, if exploited, can lead to unwanted consequences, ranging from costly disruptions to catastrophic harm. Multiply these vulnerabilities across billions of devices, many of them working autonomously and using 24/7 connections to the network, and you have an operating environment that is simply too attractive for cybercriminals to overlook.

Hackable Points of Entry

Weak authentication and unsecured connections to the network are easy to bypass. So are inappropriate device configurations, weak passwords, and known vulnerabilities that have been left unpatched. Software bugs, present in communication stacks, the operating system, or application software, can lead to unexpected device behaviors that attackers can manipulate. Running unverified firmware and software code can also create opportunities that hackers turn to their advantage.



When the IoT
is protected,
investment
and innovation
follow

Cybercrime is a Roadblock to Success

The statistics show just how pervasive cybercrime has become in the IoT. The European Commission (EC) reports that, in 2021, cybercriminals launched around 10 million Distributed Denial of Service (DDoS) attacks worldwide. That's more than 25,000 per day.

The EC also reports that, in 2021, ransomware attacks occurred every 11 seconds, for an estimated annual cost of roughly €20 billion.¹ Since then, poorly protected IoT devices have continued to come online, and there is growing awareness in the hacker community that IoT devices are attractive targets.

As the frequency and cost of IoT cybercrime continues to increase, so does anxiety about operating in the IoT. The fear of loss, damage and privacy associated with IoT deployments can erode trust and deter investment. That lack of confidence can, in turn, slow innovation and prevent progress.

The Way Forward

The picture begins to change when industrial and consumer IoT devices are protected by strong, effective and up-to-date security mechanisms. Stronger security mechanisms don't, in and of themselves, eliminate the problem. There will always be a race to stay ahead of hackers, but cybercriminals tend to avoid well-protected platforms because more effort is needed to compromise them. Having stronger protection in place helps reduce the risk of cybercrime overall.

As the chance of attack goes down, people begin to view the IoT as a safe, protected space. At the same time, as strong IoT security becomes standard, every stakeholder – from manufacturers and developers to investors, consumers and government agencies – has reason to trust the IoT. Investment and innovation build on that trust, and help the IoT reach its full potential.

Developers of industrial and consumer IoT devices can accelerate this process of building trust by thinking about security from the beginning, and by using proven techniques to protect devices. Building on the concept of "secure by default," the IoT can become a place of trusted security and digital privacy, and can begin living up to its promise of increasingly seamless experiences, deeper insights, higher levels of autonomy and greater efficiency.

Your Guide to IoT Security

The good news is that IoT developers already have a proven roadmap to follow when implementing security. Using trusted techniques for reducing risk, and leveraging ready-made solutions for device protection, developers can quickly and efficiently add strong, effective, updatable protections to their devices.

To help developers navigate their security options, and start unlocking the full potential of the IoT, we've put together this guide.

It begins with a look at some of the regulatory guidelines and certifications, aimed at minimizing vulnerabilities in IoT devices, that developers need to be aware of. It then introduces the NXP approach to establishing trust in the IoT, which builds on a broad portfolio of optimized products, complemented by security-focused services, and provides the scalability to address varying security needs. Across the security spectrum, our solutions also offer the value and differentiation that comes from using innovative technologies, proven architectures and time-saving strategies.




This brochure focuses on NXP's industry-leading portfolio of EdgeLock secure elements and authenticators, which are backed by EdgeLock 2GO, a cloud service that ensures high-level security over the lifetime of each IoT device.



The Regulatory and Certification Landscape for Trust in the IoT

In recent years, a number of industry and government organizations around the world have developed standards, regulations, guidelines and certification programs aimed at increasing security, combating cybercrime and building trust in digital systems, including those operating in the industrial and consumer IoT. This section describes the regulatory certification framework relevant to IoT developers.



Cybersecurity regulations and certifications build on best practices and are good starting points for establishing trust

As you review the following list of cybersecurity regulations, keep these key points in mind to ensure thorough understanding.

1 Different Origins

The many regulations and certifications relating to industrial and consumer segments of the IoT are developed and maintained by very different organizations and differ in their scope and audience. For example, some address cybersecurity in general, with recommendations for best practices in a wide range of product categories, while others are required for use in certain geographical regions or intended for certain use cases. Also, some of these items are legal requirements necessary for doing business in a particular market, while others are simply guidelines that, if followed, give customers an added level of assurance. Some have been in place for quite a while, others are quite new. For this reason, it's important to do a bit of research before making a final selection for a given development effort.

2 Common Themes

You'll notice that despite the variations in scope and audience, there are several common themes. From an operational standpoint, for instance, regulations and certifications tend to require transparent processes for evaluating risk, monitoring vulnerabilities and quickly responding to issues as they arise. Similarly, when it comes to the specific security mechanisms to be supported by products they tend to recommend a fairly standard list of items, such as secure authentication and encrypted communication.

3 Best Practices

The reason why there's so much overlap in these guidelines and requirements is that they focus on best practices and support the idea of standards-based security. Standards-based security is a systematic process for identifying, assessing and mitigating risks. Developed by security experts and recognized globally as a best practice, standards-based security emphasizes transparency, established concepts and regulatory compliance. It increases the effectiveness of security, by helping to ensure products are secure by design, and lowers the cost of developing security by using proven solutions that are tailor-made for quick integration.

4 A Good Place to Start

Most industrial and consumer IoT products need to conform to one or more of these regulations, or will benefit from one or more of these certifications, so this list can be a good place to start when defining how a given IoT product will operate. In general, though, having a high-level understanding of what these directives and certifications look for can help guide the development of secure IoT solutions.

General Cybersecurity

CC EAL 6+ Certification	<p>The Common Criteria for Information Security Evaluation, referred to simply as Common Criteria or CC, is an international standard (ISO/IEC 15408) for security certification. What began as a program for computers has become an internationally recognized standard for certifying a wide range of IT assets.</p> <p>The Evaluation Assurance Level (EAL) indicates the depth and rigor of certification tests, ranging from the lowest, EAL 1, to the highest, EAL 7. EAL 7 is typically applied only to critical national infrastructure and highly sensitive military applications. EAL 6+, which is used for highly critical systems where security breaches could have catastrophic consequences, is widely considered the benchmark for IoT security.</p> <p>The Assurance Vulnerability Analysis (AVA_VAN) indicates the level of rigor applied to identify and mitigate potential flaws within the system being evaluated. On an increasing scale from 1 to 5, the lower VAN levels check for obvious vulnerabilities, while the higher VAN levels involve in-depth assessments considering sophisticated attack scenarios.</p>
FIPS 140 Certification	<p>Issued by the U.S. National Institute of Standards and Technology (NIST), the Federal Information Processing Standard (FIPS) 140 defines security requirements for cryptographic modules. It is required by federal departments and agencies in the U.S. but is internationally recognized as a best practice and is used as one of the selection criteria in other instances, too. FIPS-compliant modules have been closely examined by a federally accredited lab and given a Cryptographic Module Validation Program (CMVP) certificate. The latest version of the standard, FIPS 140-3, broadens its coverage to include non-invasive physical requirements, to protect against side-channel attacks, and refines the process for destroying security data should it be somehow disclosed or modified. Depending on the application, if an embedded FIPS-certified module is used to run all the critical cryptography in an end product, a separate FIPS certification at the product level may not be required. For example, if an end product contains a FIPS 140-3 validated module, customers may be able to claim the following phrase for their product: "FIPS 140-3 Inside [SE052F certificate #]."</p>

Regional Cybersecurity

Cyber Resilience Act (CRA) – European Union	<p>This EU-wide legislation, the first of its kind, describes the cybersecurity requirements for hardware and software products with digital elements. All products with digital elements sold in the EU, regardless of their place of origin or date of introduction, must comply by December 11, 2027. The CRA requires products to be 1) secure by default, 2) equipped with mechanisms that mitigate the effect if a vulnerability is found and exploited, and 3) covered by processes that ensure a security incident is addressed professionally and resolved quickly. The CRA requirements also span the design, development and maintenance of products. Details of the conformance process and product categories continue to evolve, making it important to check specifics before starting a design.</p>
AI Act – European Union	<p>Put in place in August 2024, this is the world's first concrete initiative for regulating artificial intelligence. It aims to make the EU a global hub for trustworthy AI by specifying rules for the development, marketing and use of AI in the EU. The aim is to ensure AI systems are safe and respect fundamental rights and values, while fostering investment and innovation in AI. All parties involved in the development, usage, import, distribution, or manufacturing of AI systems will be held accountable. The Act defines four levels of risk, from minimal to unacceptable, and prohibits those in the unacceptable category. Systems of minimal, limited and high risk are permitted, but must comply with requirements and may require a conformity assessment.</p>
PSTI Bill – United Kingdom	<p>Passed in 2022, the UK's Product Security and Telecommunications Infrastructure (PSTI) Act is a regulatory framework to enhance the security of consumer internet-connected devices. It ensures that devices are protected against cyber threats and vulnerabilities by setting out minimum security standards that manufacturers must adhere to. For example, the PSTI framework establishes security guidelines for secure product implementation, requires clear information about schedules for security updates, mandates a mechanism for vulnerability reporting, and requires periodic regulatory reviews. The Office for Product Safety and Standards (OPSS) is responsible for enforcement of the Act.</p>



Consumer IoT Cybersecurity

Matter Specification (Smart Home)	First published in 2022, Matter is a freely available connectivity standard for smart home and IoT devices. It is developed and maintained by the Connectivity Standards Alliance (CSA) and backed by a certification program that ensures smart devices are secure and work together reliably. Matter is one of the first device specifications to make security a foundational part of operation. The specification requires the use of unique device identities, strong cryptographic protocols, device authentication and verification, robust data encryption, strict access control mechanisms and secure firmware updates – all built on an open standard for transparency and scrutiny by the security community.
US Cyber Trust Mark (Wireless Consumer)	Introduced by the U.S. Federal Communication Commission (FCC) in 2024, the U.S. Cyber Trust Mark is a voluntary labelling program for wireless consumer IoT products. The program includes compliance testing by accredited labs that result in a logo, accompanied by a QR code that links to a registry of information with easy-to-understand details about the security of the product. Based on the NIST 8425 standard for cybersecurity in consumer IoT products, the U.S. Cyber Trust Mark covers all other components necessary for a product to operate, such as a cloud server or a companion app on a smartphone. It also addresses the entire life cycle of the product and provides development guidelines that help ensure security. Manufacturers outside the U.S. are eligible to apply for product testing.
ETSI EN 303 645 (Consumer IoT)	Developed as a globally applicable standard by the European Telecommunications Standards Institute (ETSI), EN 303 645 covers all consumer IoT devices, establishing a good security baseline for connected devices. It's intended to be complemented by other standards defining specific provisions, but includes its own set of 13 recommendations, with the top three being no default passwords, implement a vulnerability disclosure policy and keep software updated. The 13 recommendations are used to establish 68 provisions, of which 33 are mandatory and 35 are optional. ETSI EN 303 645 was originally developed to provide the foundation of “basic-level” IoT assurance under the EU Cyber Resilience Act (CRA).



Industrial and Medical IoT Cybersecurity

ISA/IEC 62443 (Factory Automation)	<p>Addressing cybersecurity for operational technology (OT) in industrial automation and control systems (IACS), this set of standards provides cybersecurity reference architectures as well as direction of security processes, requirements, technology, controls, security acceptance and factory testing, product development, security lifecycles and a cybersecurity management system (CSMS). The standards, which are applicable to manufacturing and processing plants and facilities, include five Security Level (SL) grades, ranging from SL 0, the minimum, to SL 4, the “most vulnerable” level, so developers can find the suitable level of protection for uptime, safety and intellectual property.</p>
ISO 15118 (Electric Vehicles)	<p>Specifies a secure communication interface for electric road vehicles, for interactions between electric vehicles (EVs), including battery EVs and plug-in hybrid EVs, and the EV supply equipment (EVSE) infrastructure. In addition to defining the communication between an EV and a charging station, the protocol also addresses smart charging, which optimizes energy management based on grid conditions, user preferences and pricing, as well as vehicle-to-grid (V2G) communication, for bidirectional energy flow, which allows EVs to supply power back to the grid. Built-in security mechanisms include authentication, authorization, data encryption and regular security audits.</p>
IEC 62056 (Smart Meters)	<p>Establishes an international standard for various communication protocols used to exchange data with metering equipment. It combines the Device Language Message Specification (DLMS), a standardized communication protocol that facilitates communication between utility control centers, data concentrators and smart meters and the Companion Specification for Energy Metering (COSEM), which defines the transport and application layers of the DLMS protocol. The security mechanisms of IEC 62056 protect meter data during transmission and storage, and include authentication, encryption and integrity verification to ensure confidentiality and the completeness of metering data.</p>
IEC 62541 (Sensor Networks)	<p>Defines the information model of the Open Platform Communications (OPC) Unified Architecture (UA), which covers the data exchange from sensors to the cloud. The focus is on sensors used to automate manufacturing, and the need to keep their communications with the cloud confidential. The standard ensures secure, reliable and manufacturer-neutral transport of raw data and pre-processed information from the manufacturing level into the system for enterprise resource planning (ERP). Security mechanisms include authentication and authorization, encryption and data integrity via signatures.</p>
IEC 81001-5-1 (Healthcare)	<p>As an optimized version of ISA/IEC 62443 (which specifies the process for secure development of industrial automation and control systems), IEC 81001-5-1 specifically addresses healthcare. It covers software in medical devices, software as part of hardware intended for health use, and software-only products for health use. It is relevant to practically any organization, anywhere in the world, developing medical equipment that contains software, to ensure the safety of their embedded systems. By going beyond the medical device itself, though, the standard extends beyond things like heart monitors, insulin pumps and smartwatches to include software-only products such as yoga apps, nutrition software and care-planning software.</p>
FDA 510k (Medical Devices)	<p>The 510k regulatory pathway is a submission process, defined by the U.S. Food and Drug Administration (FDA), that manufacturers of medical devices use to get clearance to market eligible products in the U.S.. 510k clearance is required for network-enabled medical devices, and for medical devices that include a software function, use firmware, or integrate programmable logic. Manufacturers must demonstrate that their device meets cybersecurity standards and that they have processes in place to minimize cybersecurity risk, such as the performance of risk assessments, the provision of a software bill of materials (SBOM), post-market surveillance to monitor for cybersecurity issues and to release patches or updates as needed, and transparency in managing cybersecurity risks.</p>

The Common Denominator: A Root of Trust

Although there are numerous regulations, guidelines and certifications programs with relevance to the industrial and consumer segments of the IoT – the dozen-plus list in the previous section is far from complete. There is one thing they all have in common – they all recommend widely trusted security mechanisms, based on internationally recognized standards, that are applicable to just about any IoT device.

Look over the list and you'll find that certain operations are common themes across regions, industries and applications. Operations, like secure authentication to confirm the legitimacy of a device and its access rights, and secure onboarding, to ensure only authorized devices join the network, are nearly universal recommendations. So are encrypted communication, to protect data transmissions, and the ability to make ongoing security updates to keep protections current.

All these security-related IoT activities – authentication, onboarding, communication, updates and the like – have their basis in one thing: the so-called root of trust. In a digital system, the root of trust is the single source that can always be trusted. It's the essential building block on which all the secure operations of a system depend and, as a result, is a place to start when creating a secure IoT solution.

What's also true is that the root of trust – that is, the starting point for all the recommended security mechanisms – can be built using a single IC, known as a secure element. In other words, there may be lots of regulations and certifications relevant to the IoT and lots of security mechanisms to be implemented to conform to those requirements, but just one IC is all that's needed to create the foundation on which all the other items rest.

Secure Elements and the Challenge of Post-Quantum Security

Computing is undergoing a dramatic change. We are rapidly approaching a new era, defined by the ability to harness the unique qualities of quantum mechanics to solve problems beyond the ability of even the most powerful of today's classical, binary-driven computers. But the arrival of quantum computing also threatens the ability of present-day encryption to protect data. NXP is part of the industry-wide effort to develop new cryptography algorithms, standards and migration paths, so we can secure IoT devices against emerging threats from quantum computing.

Security Starts Here

In the industrial and consumer segments of the IoT, the two most widely used hardware roots of trust are secure elements and secure authenticators.

1 Secure element

A tamper-resistant IC, produced in a certified-secure environment, that acts as a vault within the system, securely stores the credentials such as keys and certificates, and protects the cryptographic functions that are essential for secure operation. It's where an IoT device's unique identity is safely stored, and where secure authentication, which confirms device identity during onboarding and other activities, takes place. It's also where encryption keys, needed for secure communication, are either generated or securely injected, and where security-critical algorithms are executed.

In some secure elements, the security mechanisms supported by the IC can be remotely updated using a secure cloud connection, so protections remain current over time, even after devices are deployed in the field.

Using a secure element helps with certification, since so many certification programs require the use of a hardware root of trust. It helps with scalability, too, because a single IC can be used across many device types, and because secure elements simplify onboarding while ensuring safe deployment.

2 Secure authenticator

A type of secure element, designed expressly for authentication purposes, that provides a protected hardware environment for storing and managing the cryptographic keys used to verify identity and authorize transactions.

NXP's EdgeLock Discrete portfolio includes secure elements and secure authenticators that are optimized for use in a range of IoT use cases. We take a closer look at the portfolio in the next section.

TPMs vs TEEs vs SEs

Hardware roots of trust come in several forms

Trusted Platform Module (TPM) – a standalone or embedded IC that provides dedicated, hard-ware-based protection of PCs, laptops, networking equipment and other computing equipment, usually in accordance with the Trusted Computing Group (TCG) certification program.

Trusted Execution Environment (TEE) – A secure area, in the main processor of a device, that guarantees the confidentiality and integrity of code while also ensuring data is executed and protected in an isolated environment.

Secure Element (SE) – A standalone, tamper-resistant IC, often with integrated security software, that provides a hard-ware-based root of trust in IoT systems.

NXP EdgeLock Discrete Solutions

NXP is a recognized leader in digital security. Our solutions are used in many of the world's most sensitive applications, including electronic passports and payment cards. We also helped define a number of protocols, specifications and standards that address security, including the new Matter protocol for smart home. Our deep engineering expertise, proven processes and advanced support for emerging trends, are just a few reasons why we're a trusted partner for IoT security.

Our EdgeLock portfolio of secure elements and authenticators includes a wide range of options optimized for use in the industrial and consumer segments of the IoT. Just about any device that's going to operate in the IoT – no matter what it's intended function – can benefit from the security provided by our EdgeLock Discrete portfolio. From cloud onboarding and secure communication to the protection of data, late-stage parameter configuration, Wi-Fi credential protection and other IoT-related security operations, our EdgeLock secure elements and authenticators deliver security tailored to the IoT.

EdgeLock secure elements and authenticators are certified, state-of-the-art solutions that deliver strong protection against the most recent attack scenarios. Dedicated features enable a wide range of use cases and serve multiple IoT applications, including industrial and consumer.

EdgeLock IoT Security and Authentication

We begin with enhanced security certified to CC EAL 6+ AVA_VAN.5 and, in some cases, to FIPS 140-3 as well. Then we add flexibility to simplify integration and make it easy to implement the cryptographic algorithms and protocols used in IoT and authentication applications.

Our Plug and Trust approach to security also means EdgeLock secure elements and authenticators are supported by a full range of development tools, from a pre-integrated and fully updatable IoT applet and middleware to software examples, development boards, access to an extensive design community, comprehensive documentation and more.

Tailored Options

The EdgeLock Discrete portfolio includes options tailored for specific use cases, such as the protection of devices that use Ultra Wideband (UWB) for secure ranging. We also offer a dedicated solution for smart home devices that require secure, efficient protection for authentication and anti-counterfeit protection.

EdgeLock 2GO IoT Service Platform

Every EdgeLock secure element and authenticator is backed by NXP's cloud-based **EdgeLock 2GO management service**, a dedicated platform for provisioning and managing IoT devices. You can use EdgeLock 2GO to securely install keys and certificates into IoT devices, either during manufacture or in the field, and then use it to keep credentials up to date during the device life cycle.

EdgeLock 2GO leverages the security capability of each EdgeLock security solution for optimal levels of security across the entire IoT fleet, and makes it easy to safely deploy and maintain devices in the IoT. EdgeLock 2GO also simplifies the delivery of end-to-end security from chip to cloud based on a certified root of trust. It protects the entire device life cycle, from day one of deployment, and simplifies security management independent of device manufacturing and the supply chain. This flexible, easy-to-use service is even approved for Matter, offering secure injection of device attestation keys into silicon and multiple options for delivery of device attestation certificates.

EdgeLock Discrete for the IoT

Device	Description
EdgeLock A30	Certified EdgeLock secure authenticator supporting multiple authentication use cases and new regulatory requirements, including digital product passports
EdgeLock A5000	Certified EdgeLock secure authenticator with symmetric and asymmetric crypto for authentication use cases
EdgeLock SE050	Certified EdgeLock secure element family with extended crypto functionality for multi-IoT use cases
EdgeLock SE051	Certified EdgeLock secure element family with support for applet updatability
EdgeLock SE051H	Certified EdgeLock secure element with integrated NFC functionality to simplify secure onboarding of Matter devices in smart homes
EdgeLock SE051W	Certified EdgeLock secure element for secure UWB ranging in the IoT (for use with NXP Trimension™ SR150)
EdgeLock SE052F	Certified EdgeLock secure element for out-of-the-box FIPS compliance (first with FIPS 140-3 Level 3 certification)



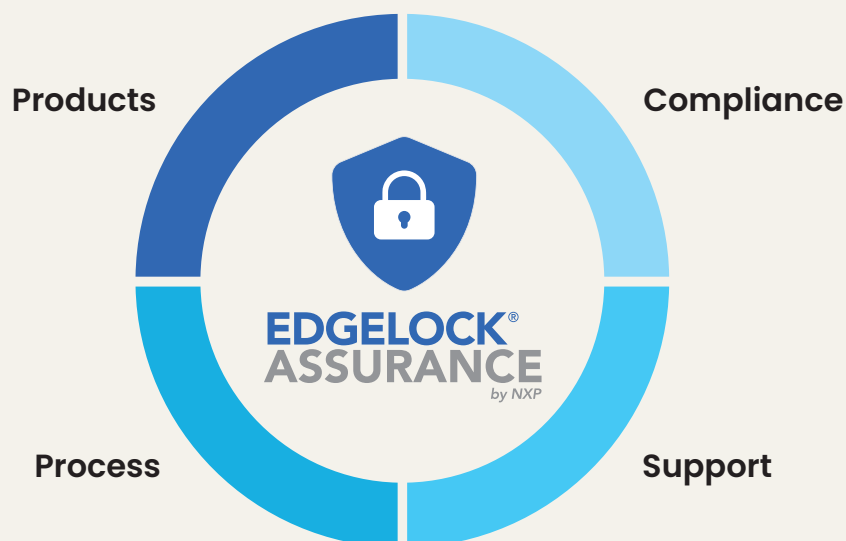
EdgeLock secure elements and authenticators provide a root of trust at the IC level and deliver true end-to-end security from edge to cloud

One Solution. So Many Ways to Use It.

The EdgeLock Discrete portfolio – including the EdgeLock SE05x family of secure elements and the EdgeLock A5000 and EdgeLock A30 secure authenticators – is designed to deliver what the IoT needs. That includes support for a remarkably broad range of use cases, spanning everything from manufacturing, healthcare and other specialized industrial applications to smart city and smart home applications that consumers interact with every day. Security is a requirement for all these use cases, whether it's protecting data collected on the factory floor, authenticating access or transactions at an EV charging station, installing an IP camera as part of a retail outlet's security system, or using a new, cloud-connected gaming device. There's an EdgeLock Discrete solution for each of those situations and more.

EdgeLock Assurance Program

All our EdgeLock secure elements and authenticators are part of NXP's EdgeLock Assurance program, which offers measurable proof of our secure-by-design process. Every product that carries an EdgeLock Assurance logo has been built to our proven security processes, is designed to meet industry standards for security, and is supported by our extensive partner ecosystem for end-to-end security.



Get a Head Start on Design

Our development teams use their security expertise and extensive knowledge of the IoT to create sample designs and development tips for some of the most widely deployed use cases. The following tables provide an overview of each use case, explaining how the EdgeLock secure elements and authenticators address specific design requirements.

For more on each use case, including block diagrams, application notes, webinars and videos, go to our dedicated page on the nxp.com/iotsecurityusecase.



Cross-Segment Use Cases

Use Case	What The EdgeLock Discrete Portfolio Lets You Do
<u>Secure Cloud Onboarding</u>	<p>Ensure end-to-end security, from chip to cloud, with secure, zero-touch connections to public and private cloud services, edge computing platforms and infrastructures.</p> <p>EdgeLock secure elements and authenticators make it possible to establish a trusted and secure Transport Layer Security (TLS) connection with different cloud service providers. They also come pre-provisioned with security credentials for use with cloud onboarding.</p>
<u>Secure Device Communication</u>	<p>Use a toolbox of crypto algorithms and communication protocols to protect the integrity, authenticity and privacy of every communication with cloud, edge and server platforms, and other IoT devices.</p> <p>EdgeLock secure elements and authenticators enable secure Plug & Trust communication with cloud, edge and server platforms. At the same time, they simplify the deployment of common communication protocols, including TLS and GlobalPlatform's Secure Channel Protocol 03 (SCP03), which secures device communication between the host and a secure element in the communication interface or between a secure element and other external entities, such as the cloud. EdgeLock Discrete products can also be used to support binding and secure boot, and can secure network communications by running NXP's Plug & Trust middleware or the developer's own TLS algorithms.</p>
<u>TPM Functionality for the IoT</u>	<p>Replace a traditional Trusted Platform Module (TPM), designed for use in powerful PCs and tablets, with a small-footprint IC intended for use in lightweight, battery-powered IoT environments.</p> <p>The EdgeLock SE05x secure element family is available with a pre-installed applet for optimized TPM functionality in the IoT, so everything from tiny sensors to robots and industrial PLCs can perform secure cryptographic processing, secure key storage, unique ID generation and storage, device attestation, and even Platform Configuration Register (PCR) issuance to remotely verify device health and ensure trust.</p>
<u>Wi-Fi Credential Protection</u>	<p>Simplify network onboarding and protect networks from unauthorized access by using certificate-based authentication and government-grade encryption in gateways and routers equipped with Wi-Fi.</p> <p>The EdgeLock SE05x secure element family provides the IoT device with a secure identity, which is then used for authentication to Wi-Fi networks. The IC supports the latest WPA-EAP-TLS security protocols as well as cryptographic functions, such as HKDF, PBKDF2 and SCP channel protection.</p>
<u>Late-Stage Parameter Configuration</u>	<p>Quickly and securely configure generic IoT devices, without powering them on, by using a standard NFC-enabled smartphone or reader to transfer final settings in the factory, before shipment, or in the field.</p> <p>Some of the EdgeLock SE05x variants include an ISO/IEC 14443-compliant passive contactless interface. In the factory, multiple profiles can be securely managed with ease, and specific parameters can be transferred to generic devices with a simple tap. In the field, one-touch customization enhances the end-user experience and saves time during installation. Furthermore, the contactless interface can be used to perform smart diagnostic of end devices.</p>
<u>Protection of Sensor Data</u>	<p>Safeguard a distributed sensor network from manipulation and unauthorized access, so the backend operation is safer and more reliable.</p> <p>The EdgeLock SE05x secure element family, located between the host controller and its associated sensors, acts as a gatekeeper, verifying that all connected sensor data is locally generated and encrypted within the IC's secure environment.</p>

Segment-Specific Use Cases

Use Case	What The EdgeLock Discrete Portfolio Lets You Do
<u>ISA/IEC 62443-Compliant Industrial Operation</u>	<p>Meet the strict requirements of ISA/IEC 62443 compliance in the Industrial IoT (IIoT) by adding protections that guard against unauthorized access and data manipulation.</p> <p>The EdgeLock SE05x secure element family is available with a pre-installed, feature-rich security applet designed to satisfy the ISA/IEC 62443 requirements relating to device identity, crypto functionality, secure provisioning and secure protocols. The family also issues a secure identity that the IIoT device uses with mutual authentication, sensor authentication, cloud onboarding and other IIoT tasks.</p>
<u>IEC 62056-Compliant Energy Management</u>	<p>Leverage comprehensive, third-party certified solutions that protect smart meters and are tailored to local regulations, such as the Smart Meter Gateway (SMGW) in Germany.</p> <p>EdgeLock secure elements and authenticators prevent unauthorized access to meter data and ensure secure communication and authenticated transactions, in accordance with IEC 62056 (DLMS/COSEM), the German SMGW, and other regional requirements. They also work seamlessly with the EdgeLock 2GO cloud service to securely manage the credentials of already-deployed meters, manage the contracts and authenticate transactions, address new security requirements and/or respond to a security incident.</p>
<u>ISO 15118-Compliant EV Charging</u>	<p>Use a turnkey solution for secure Electric Vehicle Source Supply Equipment (EVSE) to enable quick deployment and rapid scaling of compliant chargers in residential and commercial environments.</p> <p>The EdgeLock SE05x secure element family is part of our turnkey solution for EV charging, which implements all the security requirements for ISO 15118-2 and part of the requirements for ISO15118-20. The family also simplifies key management, accepts over-the-air updates, authenticates energy-usage and billing data, supports charger production at third-party facilities and enables EV charger authentication with multiple entities.</p>
<u>FIPS-Compliant IP Cameras</u>	<p>Integrate a ready-made solution for IP cameras that turns what would otherwise be a serious risk into a trusted asset for video monitoring.</p> <p>The EdgeLock SE05x secure element family protects the essential steps in IP camera operation, including secure cloud onboarding, device-to-device authentication and attestation and late-stage parameter configuration. The EdgeLock SE052F is FIPS 140-3 Level 3 certified.</p>
<u>Matter-Compliant Home Security</u>	<p>Create truly smart home-security devices by delivering Matter-enabled secure connectivity and seamless interoperability.</p> <p>EdgeLock secure elements and authenticators extend Matter's connectivity security to provide the kinds of additional protections – such as secure device administration and device management, support for device integrity and secure storage of user data – that OEMs and consumers need. The EdgeLock SE051H is a turnkey solution, designed to meet the security requirements of Matter (up to version 1.3) by supporting all the specified algorithms and cryptographic functions.</p>
<u>Medical IoT (MIoT)</u>	<p>Deploy comprehensive, FIPS-compliant protection that safeguards privacy, secures data and enables innovation in connected medical devices.</p> <p>The EdgeLock SE052F is the industry's first hardware secure element validated for FIPS 140-3. It offers fast certification with other efforts, too, including FDA submissions. The EdgeLock secure authenticator family, with its CC EAL6+ certification, meets the medical industry's standards for authentication use cases.</p>
<u>Secure Access</u>	<p>Deliver a higher level of protection in Smart City applications that use physical or logical access and enable advanced features for multi-user/multi-session management.</p> <p>The EdgeLock SE05x secure element family works seamlessly with MIFARE® DESFire® EV2/EV3 for authentication, session key generation and key rotation. It's a flexible approach applicable to everything from smart door locks to specialized machinery in industrial environments.</p>
<u>Wireless Charging</u>	<p>Enable safe wireless charging and create better consumer experiences by integrating a dedicated solution for the authentication of Qi 1.3 wireless charging.</p> <p>NXP is a designated Wireless Power Consortium (WPC) Approved Manufacturer CA Service Provider, and EdgeLock secure elements and authenticators are WPC-compliant ICs. That means we offer a turnkey solution for Qi charging with 1.3 authentication so it's easy to deliver Qi-compliant devices that enable safe, satisfying charging experiences</p>



nxp.com/iotsecurity

NXP, the NXP logo, EdgeLock, MIFARE and DESFire are trademarks of NXP B.V. All other product or service names are the property of their respective owners.
© 2025 NXP B.V.

Document Number: IOTSECBRA4 REV 1

