Protecting the Edge at scale with NXP Security Solutions

Technology Six Pack

January 2025

Overview

The digital transformation and paradigm shift: threats & risks at the Edge

Security protections offered by NXP Edge Processing portfolio

NXP Security Technologies

Security Assurance by NXP

Protecting the Edge at scale with NXP


Then
Digitalization, complexity, exposure to cyber risk
Now

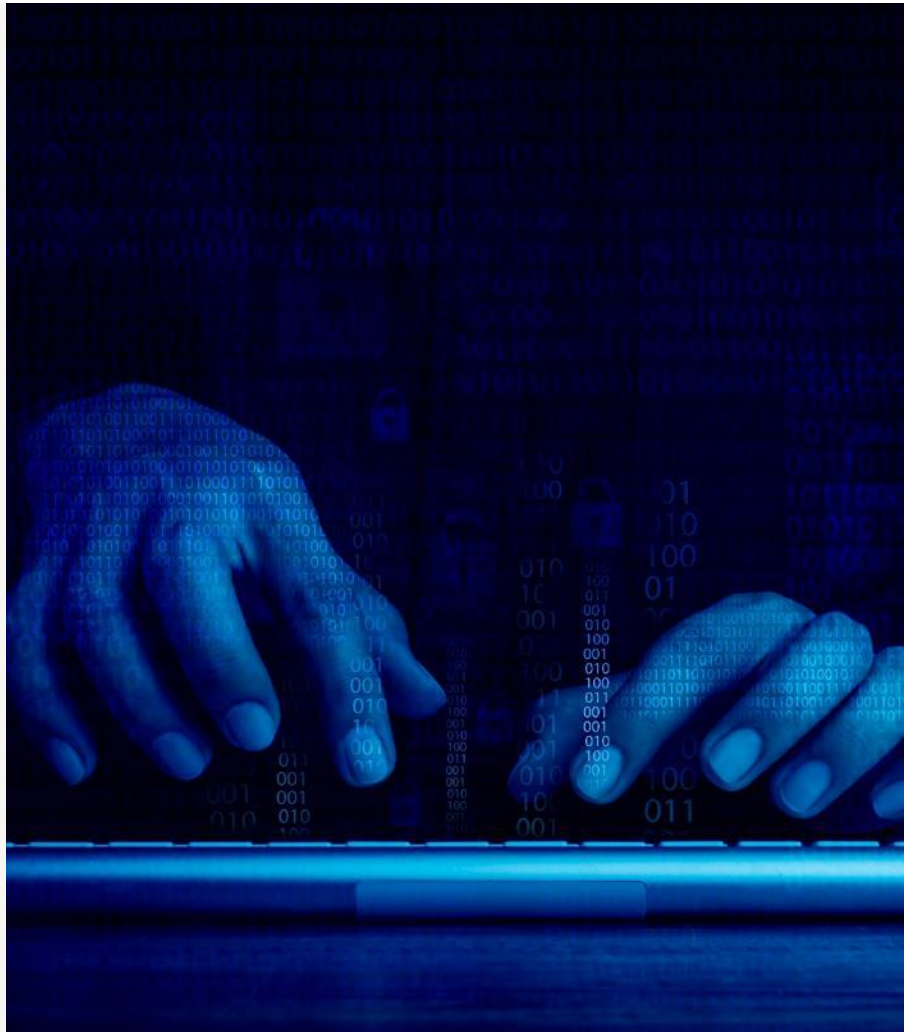
Then

Digitalization, complexity, exposure to cyber risk

Now

A paradigm shift

- Security agencies worldwide report a significant increase in both the variety and quantity of cyberattacks
- Ransomware and denial of service ranked at the top
- Public sector, individuals, health, digital infrastructure, manufacturing, finance and transport targeted
- Device manufacturers exposed to recovery costs, product recalls & warranty costs, indemnifications, IP theft, reputation loss
- Regulations emerge to foster a more secure cyber space & allow consumers to make informed purchase decisions



Attacks on edge

Remote

Local

Network to edge

Manufacturing

Field

Tap to network(s)

- Capture poorly protected/unprotected sensitive data
- Inject fake data
- Disrupt connections

Break into the device through its network interface

Exploit a vulnerability on device or interface protocol to:

- Take control of device, install malware
- Modify data or steal stored sensitive data
- Spy activity and traffic
- Brick the device, block until ransom paid
- Steal device identity
- Damage hardware

Tamper devices in field locally

- Unlock debug port or admin port and extract SW,
- Get device admin or access passwords
- Reprogram device with modified, malicious SW
- Steal device identity, (keys) with side channel analysis and local attacks

Compromise supply chain

- Replace genuine devices/components (including SW) by compromised ones
- Install (sub-contractor or component provider) malware/backdoors
- Misconfigure device
- Collect device identities
- Steal SW IP
- Overproduce, clone, counterfeit

Multiple mitigations can be put in place to counter various attacks

Edge device

Attacks on data of networks

- Secure commissioning of devices
- Secure access to network
- Data encryption
- Device & data authentication
- Use of state-of-the art cryptography
- Regular update of cryptographic keys and digital certificates

Attacks on device software in field

(often remote but also local)

- Device hardening (e.g. disabling of unused network ports, setting file permissions, configuring user account with strong access credentials…)
- Device integrity protection mechanisms (e.g. verification of executed firmware)
- Isolation of sensitive assets and security functions within the device
- Authentication on physical ports for admin & debug (JTAG, USB, etc.)
- Use of state-of-the art cryptography
- Device (remote) integrity verification

Attacks on device hardware in field

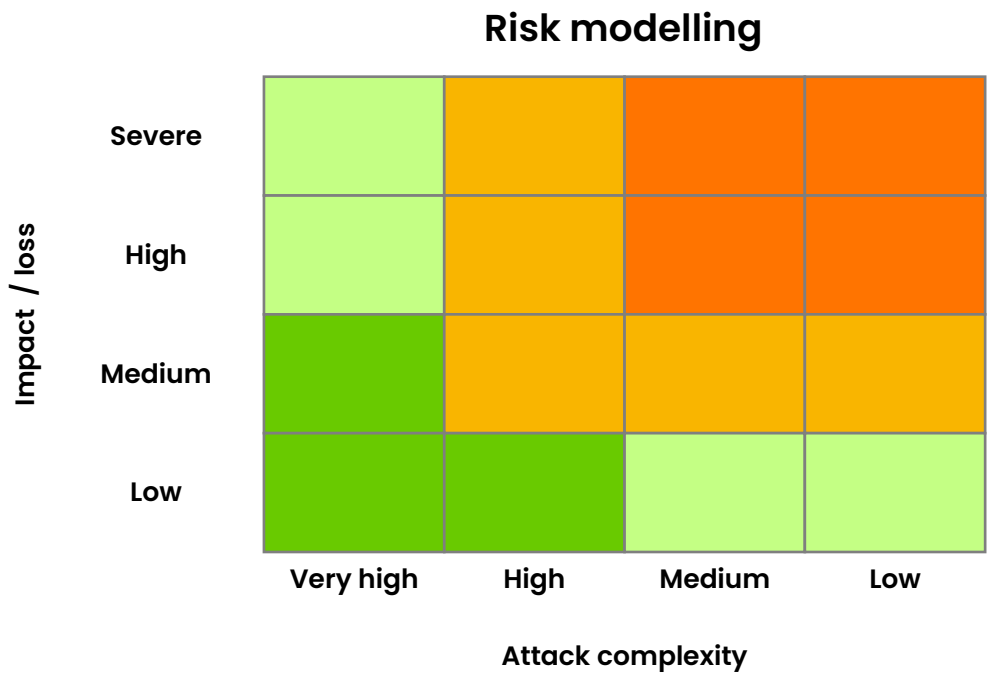
(often local but also remote)

- Detection of tampering and malicious activity with erase of sensitive data
- Tamper resistance of security functions
- Secure access to device location

Attacks in manufacturing

- Procurement of secure components (HW, SW)
- Secure manufacturing sites, Zero Trust infrastructure
- Encrypted install of FW/SW and credentials
- Monitoring of production
- Overproduction control
- Secure key management (generation, usage)
- Use of state-of-the art cryptography

The required type, number and resistance level of security countermeasures depend on exposure to threats & impact of attacks



The various threats associated with target applications must be identified, analyzed and prioritized in terms of complexity of attack and impact

The complexity of attacks can be measured in terms of required attacker's **equipment, time, window of opportunity, expertise and knowledge, but also reachability** of the device (type of exposure: remote, local).

The impact depends on the **type of application** and is naturally higher for critical infrastructures (such as nuclear plant or power grid), medical application (safety) or manufacturing & industrial facilities (downtime) for example.

Impact depends also on **scalability** of an attack, i.e., ability to (easily) replicate the same attack(s) on many devices of same type.

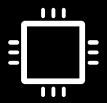
Deployment at scale of security on edge devices is a challenge

Secure networking

- Encryption performances: high speed networks, time sensitive networks (TSN)
- Management of keys over device lifecycle
- Multiple standards and diversity of cryptographic suites to comply with

Security against SW attacks in field

- Vulnerabilities in SW: any single bug in SW is a potential entry point for hackers, while SW stacks are getting increasingly complex & large
- Management of fixes and updates in field
- Management of keys over device lifecycle
- Detection and recovery of compromised devices
- Process for signing SW with access & usage control of SW signing keys



Security against HW attacks in field

- Availability of tools on market lowers required knowledge, time and financial means to tamper devices

Secure supply chain

- Confidentiality of device and OEM credentials in global supply chains and multi-site manufacturing
- Multiplicity of HW and SW components with various origin
- Correctness and integrity of security configuration especially in untrusted manufacturing sites

Security is fundamental to the solutions we create

NXP is uniquely positioned to address various risk levels at the edge

Protection

Security capabilities built on-chip to support protect of end products

Resistance

Robustness of implemented security functions against various attacks

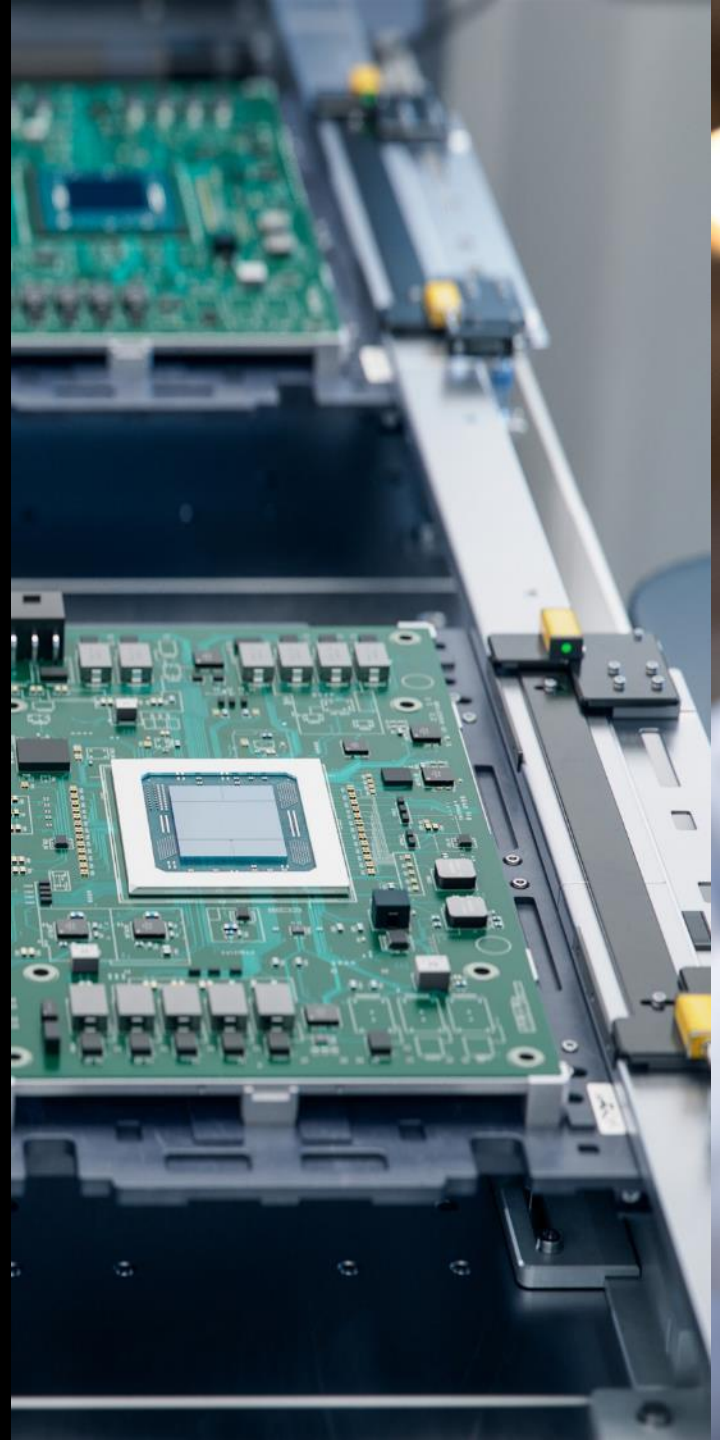
Assurance

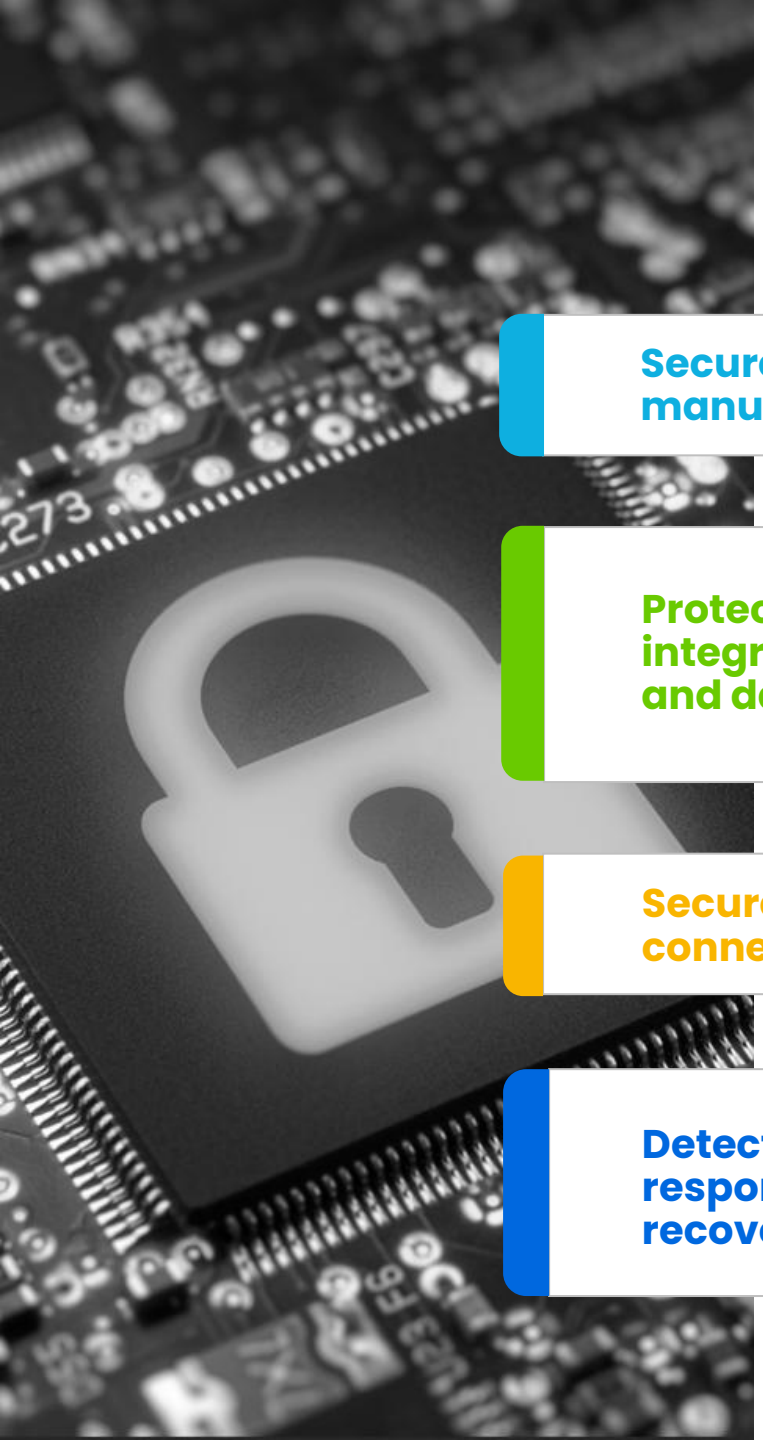
Proven processes and validation assessments help ensure NXP delivers trusted solutions

NXP EdgeLock® Security

Section 2

Security protections offered by NXP Edge Processing portfolio





Leverage EdgeLock® security to build protections over device lifecycle

Securely manufacture

- Encrypted install of firmware
- Encrypted install of keys
- Secure debug & config
- Remote key install

Protect integrity and data

- Secure boot and initialization
- Secure update
- TrustZone® SW Isolation
- Integrated enclave isolation
- Encrypted internal memory
- Encrypted external memory
- Disk encryption

Securely connect

- Device origin attestation
- Secure communication
- Accelerated networking
- Remote key management

Detect, respond, recover

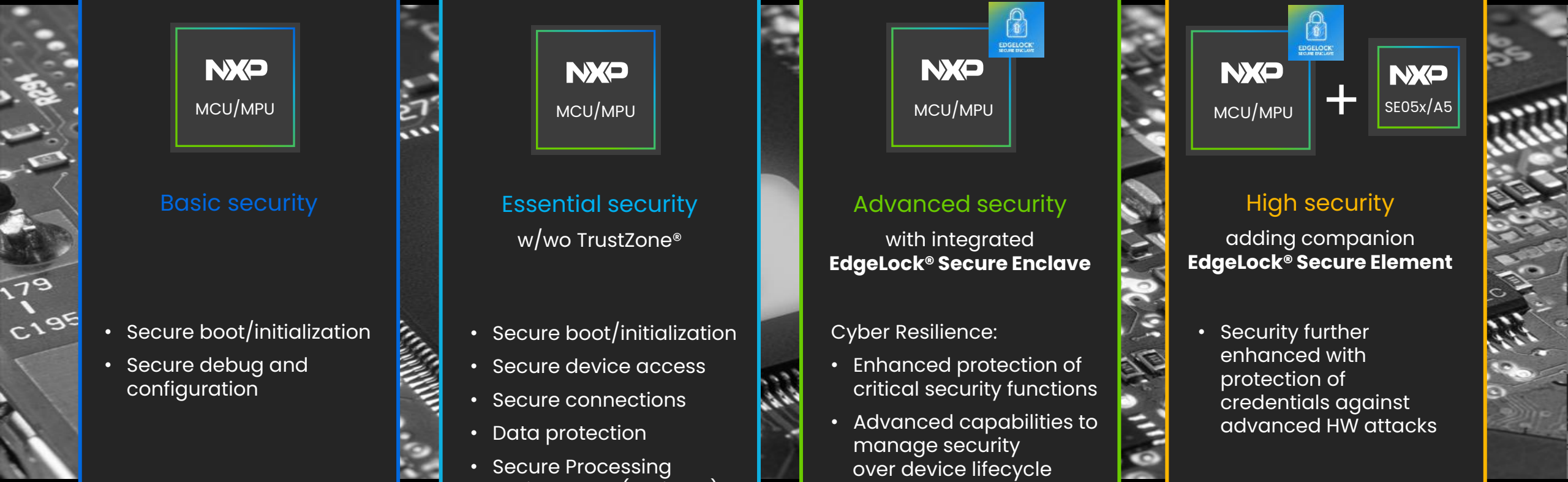
- Measured boot
- SW attestation at runtime
- Tamper detection
- Battery backed monitoring
- Cyber Resilience Recovery

- IP Protection

Section 3

NXP Security Technologies

NXP offers a portfolio of scalable solutions to address various risk & security levels at the edge



NXP MCU/MPU

Basic security

- Secure boot/initialization
- Secure debug and configuration

NXP MCU/MPU

Essential security

w/wo TrustZone®

- Secure boot/initialization
- Secure device access
- Secure connections
- Data protection
- Secure Processing Environment (optional)

NXP MCU/MPU

Advanced security

with integrated **EdgeLock® Secure Enclave**

Cyber Resilience:

- Enhanced protection of critical security functions
- Advanced capabilities to manage security over device lifecycle

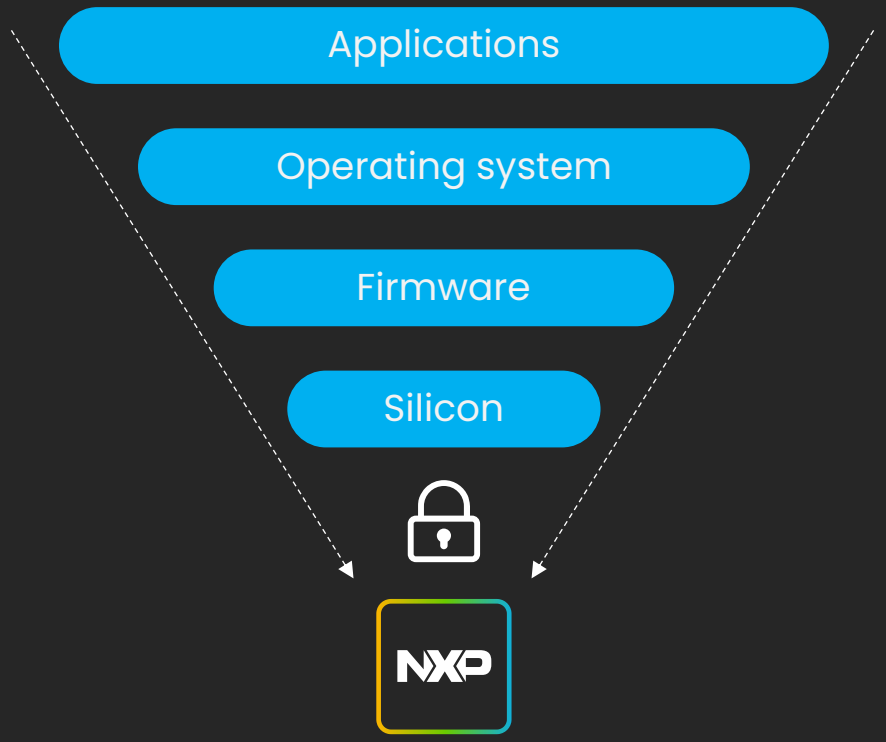
NXP MCU/MPU + NXP SE05x/A5

High security

adding companion **EdgeLock® Secure Element**

- Security further enhanced with protection of credentials against advanced HW attacks

Silicon-based trust anchors to implement & protect security functions



Hardware as foundation

Security starts with HW, and minimum HW foundations are required to further build security protections.

Security functions must be protected and anchored

Security functions protecting data and devices (such as encryption, authentication and device integrity verification) must be isolated from complex SW stacks and be anchored in resilient, root silicon.

Implementation matters for a silicon trust anchor

To be a Root of Trust, silicon must result from a strict development process, with clearly defined design rules & multiple iterations of careful review.

Hardware roots of trust scales across NXP edge processing portfolio

	Basic Security	Essential Security		Advanced Security	High Security
Secure boot capability	✓	✓	✓	✓	✓
Secure debug & Test, Lifecycle Management	✓	✓	✓	✓	✓
Memory/resource access protections	✓	✓	✓	✓	✓
Cryptographic HW support (TRNG, crypto engine)	-	✓	✓	✓	✓
Process/task isolation, Secure Proc. Environ. (incl. for secure key store or application)	-	-	TrustZone®	Enclave[2] + TrustZone	Enclave[2] + TrustZone + Secure Element
Secure boot rooted in ROM as immutable memory type	-	Optional[1]	Optional[1]	✓	✓
HW Tamper detection	Optional[1]	Optional[1]	Optional[1]	✓	✓
Factory programmed Unique Keys or PuF	-	Optional[1]	Optional[1]	✓	✓
Remote Key management (EdgeLock 2GO ready)	-	-	-	✓	✓
Runtime device protection	-	-	-	Optional[1]	Optional[1]
Personalization with custom credentials at NXP manufacturing	-	-	-	-	✓
Protections against advanced HW attacks	-	-	-	-	✓
Assurance Level (Note: some products also feature NIST CAVP, CMVP & ESV)	-	-	Up to SESIP/PSA L2	SESIP/PSA L2-L3 + Secure Enclave	SESIP/PSA L2-L3 + Secure Enclave with Secure Element (CC EAL6+ HW/OS, FIPS 140-3 Level 3)
MCU	MCX A13x/A14x/ A15x		LPC55S6x/2x/1x/0x	LPC 55S3x, K32W148 MCX N9x/N5x/W7x, RW61x	MPUs/MCUs with EdgeLock Secure Enclave (Advanced Security category) + SE05x/A5x
Crossover MCU	-	i.MX RT10xx, i.MX RT116x/7x,	i.MX RT500/600	i.MX RT700, i.MX RT1180	
MPU	-		i.MX 6/7/8M/8/8X	i.MX 8ULP, i.MX 9x	

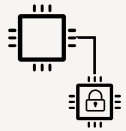
1. optional means chip dependent 2. Enclave type of isolation covers both Core and Advanced capability profiles of EdgeLock Secure Enclave 3. ISP = In-System Programming

NXP offers key technologies facilitating security deployment & maintenance over device lifecycle

EdgeLock Secure Enclave

Integrated security unit

- Ease of use for developers (dedicated HW security unit)
- Secure manufacturing
- Cyber resilience, device integrity protection



EdgeLock SE05x/A5x

Discrete secure element

- Personalization with custom OEM/service provider credentials (pre-build)
- Scalable security & key management across OEM product portfolio

EdgeLock Accelerator

Integrated crypto-co-processor

- High performance encryption/authentication for high speed and time sensitive networking
- Fast & secure boot

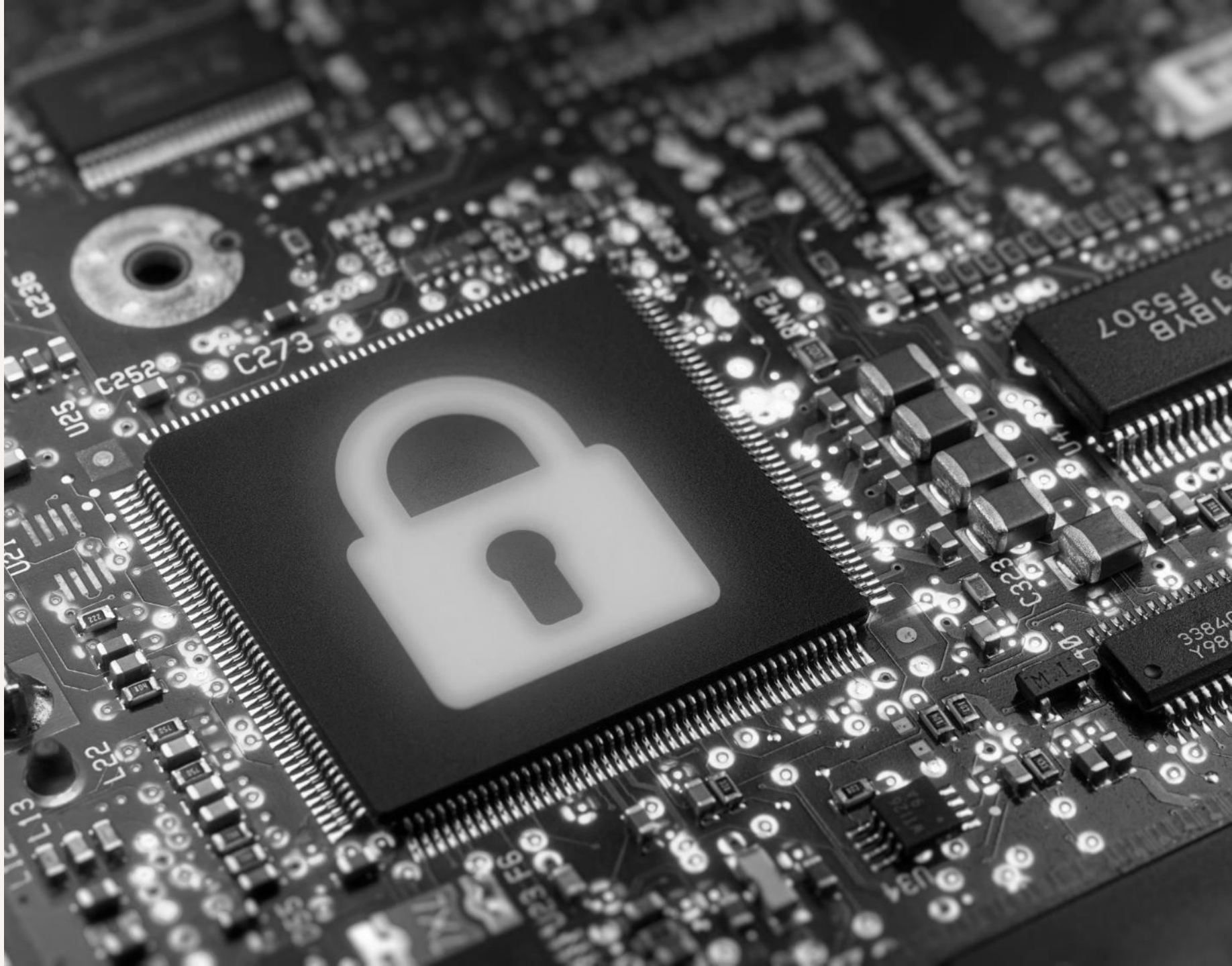
EdgeLock 2GO

Key management platform

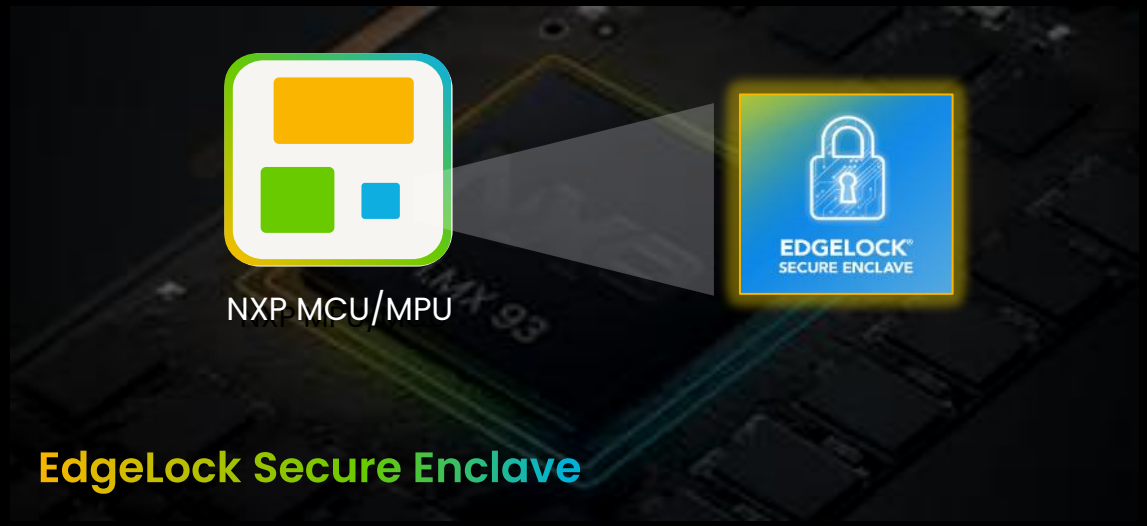
- Secure manufacturing
- Overproduction control
- Management of device access & authentication in factory and in field

Integrated EdgeLock Secure Enclave and discrete EdgeLock Secure Element:

Complementary Root of Trust technologies



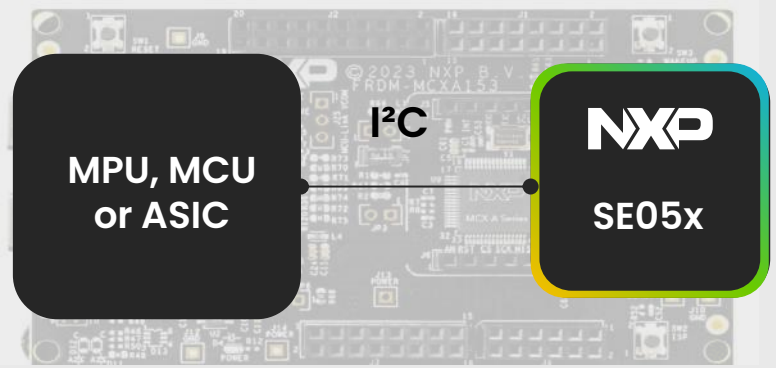
Integrated



EdgeLock Secure Enclave

- Dedicated security unit, with its own CPU core, immutable memory (ROM) and other memories, physically isolated from the rest of SoC
- Protects SoC integrity and prevents application cores from gaining direct access to sensitive data
- Provides enhanced isolation for execution of critical & sensitive security functions. It prevents attacks exploiting shared processing/ storage resources typical to some Trusted Execution Environments

Discrete



EdgeLock Secure Element/Authenticator

- Plugs into any type of processors and provides the host processor with a companion for cryptographic operations, as well as a secure & certified vault for keys and digital certificates
- Security IC featuring tamper resistance to advanced physical attacks, securely transporting & hosting applications with their confidential and cryptographic data (e.g. cryptographic keys)
- Certified Common Criteria at EAL6+ level and FIPS level 3

EdgeLock Secure Enclaves is delivered in 2 capability profiles (Core & Advanced), providing scalability across NXP Edge Processing Portfolio

	Core	Advanced
Crypto Services, TRNG	■	■
Secure Key Store	■	■
Device Unique Identity & Keys	■	■
Device Attestation	■	■
Secure Connections	■	■
Key MNGT OTA (EdgeLock 2GO)	**(optional)**[1]	■
Enclave FW/Crypto Updatability	**(optional)**[1]	■
Runtime Device Protection		■
Integrated typically on:	Arm® Cortex®-M Core MCUs (constrained & lightweight devices)	Crossover MCUs Applications Processors
Supported devices (Examples):	LPC55S3x, MCX N, MCX W7x RW61x, K32W148	i.MX RT1180, i.MX8ULP i.MX9x

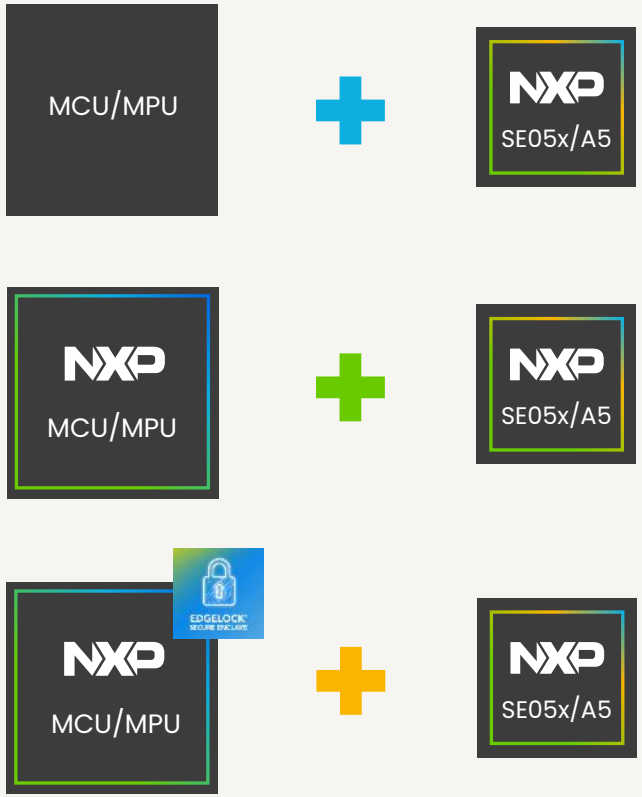
1. optional means chip dependent

Dedicated security cores (integrated or discrete) for Cyber Resilience

Supported Use Cases	EdgeLock Secure Enclave (Core Profile)	EdgeLock Secure Enclave (Advanced Profile)	EdgeLock Discrete SE05x/A5x
Crypto Services, TRNG	Limited set of crypto options	Wide set of crypto options	Wide set of crypto options
Isolated key store	✓	✓	✓
Device Unique Identity & keys	✓	✓	✓
Secure boot/update	✓	✓	-
Secure debug	✓	✓	-
Memory encryption	✓	✓	-
Device SW attestation at boot	✓	✓	-
Runtime Device integrity Protection	-	✓	-
Key mngt OTA (EdgeLock 2GO ready)	Optional	✓	✓
Injection of keys thru NFC interface (passive mode, unpowered board)	-	-	✓
Personalization with custom credentials at NXP manufacturing	-	-	✓
Personalization with custom credentials at programming centers (chip level)	Possible for MCUs with internal FLASH	-	✓
FW/Crypto Updatability	Optional	✓	✓
Programmability (applets)	-	-	SE051P only
Tamper resistance	Protection against SW and basic HW attacks	Protection against SW and basic HW attacks	Protection against SW and advanced HW attacks
AVA.VAN Level (vulnerability assessment as defined by SESIP and Common Criteria)[1]	Up to 3	Up to 3	5
Certification	Up to SESIP L3	Up to SESIP L3	CC EAL6+, FIPS 140-3 L3 (SE052F), IEC62443-4-2

1. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

Usage scenarios of EdgeLock Discrete



Enhancement of non-NXP MCU/MPU with secure key storage and tamper resistant cryptography, harmonizing key management across OEM portfolio

Enhancement of NXP MCU/MPU featuring Essential security, with HW isolation of key storage and tamper resistant cryptography

High security for sensitive applications, combining SW integrity protection (EdgeLock Secure Enclave) & high tamper resistant cryptography & key storage (SE05x/A5000)

Integrated EdgeLock Accelerators

A solution for each type of application

Dedicated cryptographic accelerators for best performances

Accelerator type	Description[1]	Updatable	Integrated Key store	Wrapping for key injection	Typical Use Cases (non exhaustive list)
EdgeLock Accelerator (CAAM)	Family of accelerators with extended cryptographic support, covering RSA, ECC, AES and SHA-1/2, (3)DES. Also includes protocol offload for some variants.	-	✓	✓	TLS, IPsec
EdgeLock Accelerator (V2X)	Accelerator optimized for high speed ECDSA authentication, SHE/Evita support (automotive)	✓	✓	✓	Automotive V2X, Fast boot
EdgeLock Accelerator (Prime)	Multi-engine accelerator optimized for high speed ECDSA authentication, AES and SHA-2	✓	✓	✓	Time Sensitive Networking, Fast boot, Disk encryption, TLS, networking, IPsec, DRM, V2X
EdgeLock Accelerator (PKC)	Mathematical co-processor used for RSA and ECC operations	✓ (host processor SW)	-	-	TLS, IPsec, Matter
EdgeLock Accelerator (Casper)	Mathematical co-processor used for RSA and ECC operations	✓ (host processor SW)	-	-	TLS
EdgeLock Accelerator (SGI)	Hardware engine integrating acceleration for AES, HMAC/CMAC and SHA-2 operations	-	✓	✓	Fast boot (AES based), key wrapping to mass storage
EdgeLock Accelerator (HASH-CRYPT)	Accelerator AES , SHA-1 and SHA256	-	-	-	Secure boot, TLS
EdgeLock Accelerator (DCP)	Accelerator AES-128/SHA256	-	✓	-	Fast boot, Disk encryption, TLS

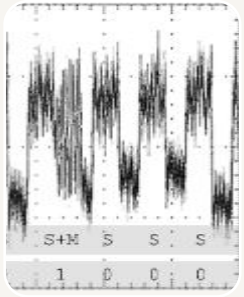
1. Please check specific product datasheets for exact list of supported cryptographic algorithms

Resistance against physical & logical attacks

NXP has developed tamper resistance technologies to mitigate physical attacks

- **Tamper resistance** mitigates or withstands **physical attacks**, such as
  - Disabling FW authentication at boot by applying a power glitch on supply at a precise time (“fault injection”)
  - Probing signals emitted by equipment to extract information (e.g., key encrypting a connection)
- The goal of tamper resistance is to **make it difficult to bypass security protections, and** for unauthorized individuals to **access, modify or disable devices and systems**, based on physical attacks
- Depending on the target applications specific to each MCU/MPU, NXP implements various **countermeasures at chip level** complementing or avoiding the need for other mechanisms applied at equipment level such as
  - Secure facilities protected by access controls, surveillance systems, alarms
  - Tamper-evident seals or coatings to detect if a device or enclosure has been tampered with

The spectrum of physical attacks is broad, from invasive to unnoticed, non-destructive ones

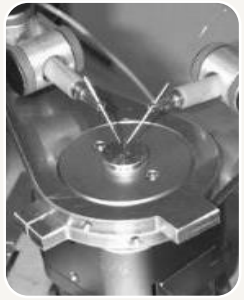


Side-channel attacks

- Power analysis (SPA, DPA)
- Electromagnetic analysis (SEMA, DEMA)
- Timing Analysis
- Photo-emission microscopy (high-end)
- Profiled, unprofiled and ML-assisted variants

Fault injection attacks

- Voltage or clock glitching
- Electromagnetic fault injection (EMFI)
- Body bias injection
- Laser fault injection
- Single and multi-shot scenarios



Invasive attack

- Focused Ion Beam (FIB) modifications
- Micro/Nano-probing of internal signals
- Signal forcing
- Delayering
- Reverse-engineering

NXP has also developed resistance against logical attacks

- Logical attacks exploit logical errors, SW bugs and flaws in decision-making processes
- They only rely on messages sent to the device to cause damage
- They can be based on fuzzing on device interface and/or reverse engineering
- Logical and physical attacks can be combined to downscale attacks in overall complexity, while still fully automated & deployed remotely

NXP offers a range of countermeasures, from prevention of attacks to detection of tampering attempts and response

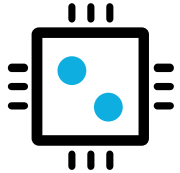
Hardening of HW/FW implementations

Sensitive code fully audited, security tested using static and dynamic test methods

Cryptographic implementations featuring constant execution time and masking of operations

Encryption of memories, hiding of secrets at rest (e.g. with Physically Unclonable Functions -PUF)

Protection of code execution flow: complex pattern for decision information, double checks, double executions, flow verification, etc.



On chip sensing

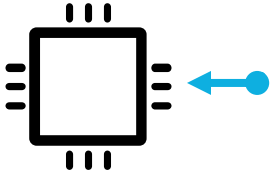
On-chip intrusion detection with sensors, with monitoring of clock frequency, supply (level and glitch), temperature

Active shielding at IC level

Code watchdog

Abnormal behavior on Random Number Generator, unauthorized access on keys or specific memory locations

Zeroing of keys or disabling of functions in case of attack detection



External sensing

Connection to external tamper detection sensors, such as opening switch on casing.

Tamper pins are either passive (input signal to chip) or active (alteration of a stream of bits sent by the chip)

Zeroing of keys or disabling of functions in case of attack detection

(Non-exhaustive list of countermeasures implemented on various NXP solutions)

The resistance level and diversity of countermeasures on NXP products are profiled to meet targeted applications

NXP offers a **range of solutions** adapted to various types of applications:

- From resistance against logical, and basic to intermediate hardware attack with NXP MCU/MPUs
- Up to advanced hardware attack resistance with dedicated companion plug-in: EdgeLock Secure Elements and Authenticators

The resistance level is **measured** in terms of the required

- Cost & complexity of equipment to tamper a device
- Expertise and knowledge of the attacker (about the device)
- Devices availability to the attacker
- Time to identity and exploit vulnerabilities

The **achieved** level of resistance is reflected in certifications results (Common Criteria, SESIP, PSA Certified or FIPS), more precisely in:

- The certification level and related criteria
- The associated Security Target or Protection Profile (specifying a.o. on which functions is the Physical Attacker Resistance claimed)

Security resistance level: assurance & typical use cases

Vulnerability Assurance (AVA_VAN level)[1]	Level 1-2	Level 3	Level 4-5
SESIP[2] certification at chip Level	1-2	3	4-5
Typical Use Cases:	Suited for end products: • Not easily accessible in their operating environment by skilled adversaries • Or for which the likelihood of a more elaborated attack is relatively low (e.g. when expected potential attacker is a layman) • Or for which a security incident has low/acceptable impact • Or for which other security countermeasures exist at the equipment or system level (e.g. tamper detection, sealing, resistant casing, active monitoring, controlled physical access to premises, etc.) • Or for which there are deterrence controls of a technical or operational nature: contractual or legal obligations & penalties (e.g. with contract manufacturer) active monitoring, etc.	Suited for end products: • With adversary access In their operating environment, but limited in time or limited in time without detection • Or for which complementary security countermeasures exist at equipment or system level • Or for which a security incident has a controlled impact (limited damages, no or limited scalability of attack, limited exploitability of a vulnerability, etc.)	Suited for end products: • With (extended) exposure to adversaries without detection in their operating environment • And for which no complementary security countermeasures exist at equipment or system level • And for which a security incident has potentially a significant impact (damages, scalability, difficult deployment of mitigations, etc.)

1. Tolerance or resistance against attacks, as measured at chip level by Common Criteria standard (ISO 15408)
2. SESIP: Security Evaluation Standard for IoT Platforms (EN 17927)

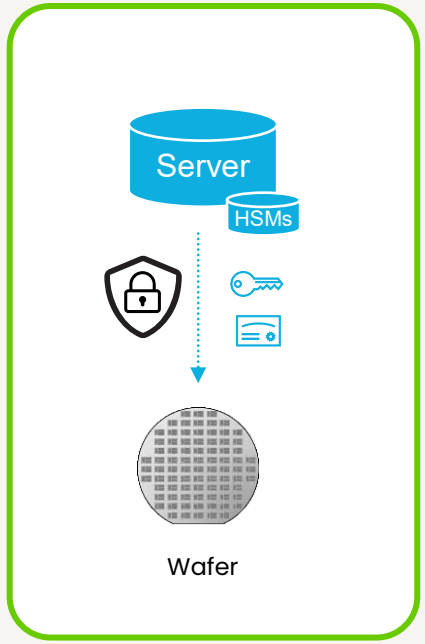
Injection of root of trust keys on NXP Edge Processing platforms

For secure install & execution of applications at the edge

Trust provisioning

NXP runs a trust provisioning service capable of provisioning any credential or secret data at NXP silicon manufacturing

- Certified data creation, processing & injection
- On chip key generation, data harvesting
- Uniqueness assurance of chip individual data like root of trust device key
- NXP FW Signing
- Specifically, for EdgeLock Secure Elements & Authenticators:
  - Personalized product configuration and injection of custom credentials
  - Secure data intake and data delivery to OEM



Example: injection of keys for device authentication, device attestation, secure connections, FW encryption, etc.

Bootstrapping at scale the chain of trust in IoT and Industrial supply chain

- NXP Infrastructure initially developed for banking and eGovernment applications, now used for IoT & Industrial
- Proven in 500+ product types and 35+ billion parts

- Secure manufacturing sites including access protection
- Resilient IT infrastructure with a farm of load-balanced secure servers (HSM)
- Multiple security domains

- Certified & audited facilities, processes, flows and software elements

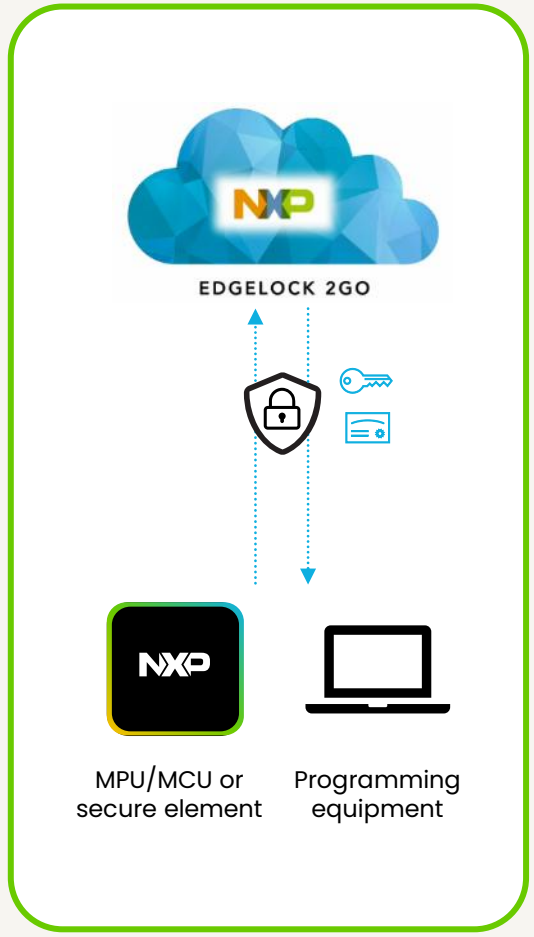
EdgeLock 2GO

NXP cloud services for remote credential management on IoT & Industrial devices

Easy deployment of device & application credentials on devices without upfront investment in infrastructure
(device origin certificates, credentials to access cloud services, FW decryption keys, etc.)

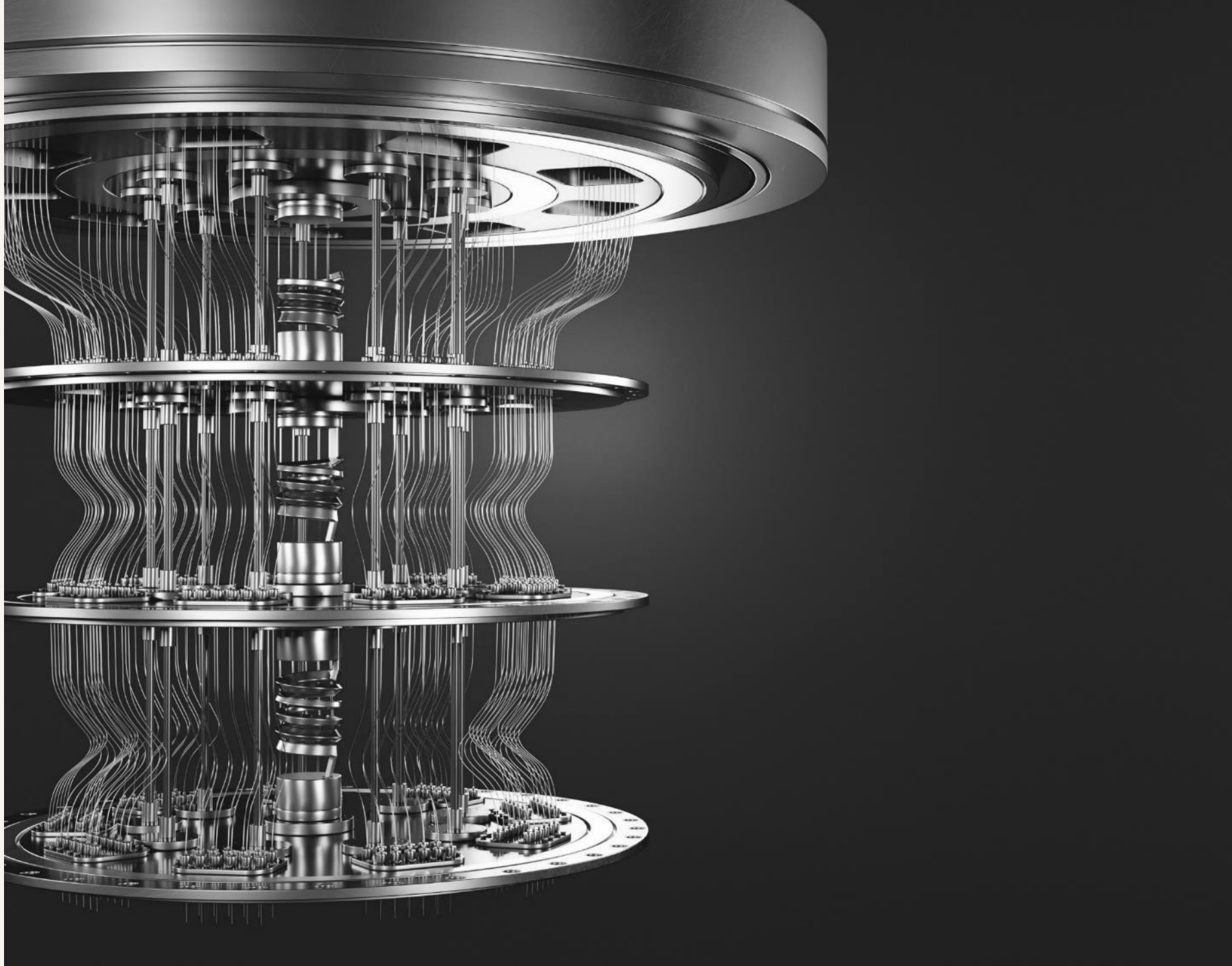
Management of credentials over-the-air and over device lifecycle for a maintained security

Native integration on EdgeLock Secure Enclave, Secure Elements & Secure Authenticators for seamless and end-to-end secure key management solution



Post Quantum Cryptography

A migration for resilience



NXP has started deployment of post-quantum cryptography on Edge Processing Platforms

- Cryptography is the security foundation for equipment integrity, secure communications, secure transactions and protection of assets
- Contemporary PKI crypto in use for more than 20 years can be broken by quantum computers
- Quantum-safe PKI replacement is needed, key length of symmetric crypto must be increased
- NXP co-authored world-wide post-quantum secure standard
- NXP has build strong expertise in enabling PQC for embedded, with more than 10 patent families on high-assurance / high-performance PQC implementation & integration
- NXP announced at Electronica 2024 its first application processor (i.MX 94) with integrated post-quantum cryptography (PQC), including support for secure boot, update and debug access

Section 4

Security Assurance by NXP

EdgeLock® Assurance

Security is fundamental to the solutions we create. When you see EdgeLock Assurance, you'll know it's designed to meet industry standards. Proven processes and validation assessments help ensure we deliver trusted solutions for your security challenges. Together, we can advance the world securely with confidence.

EDGELOCK® ASSURANCE by NXP

NXP provides evidences of conformance to emerging cyber security standards with EdgeLock Security

Security foundation to access global markets

- EU Cyber security Act
- Cyber Resilient Act
- NIS2
- Radio Equipment Directive (RED)

- AI Act (trustworthy AI)

- ISA/IEC 62443
- OPC UA
- FDA Cybersecurity

- ETSI 303 645
- Matter
- Cyber Trust Mark, NIST 8425
- Product Security Verified Mark (Connectivity Standards Alliance)

NXP is evaluating & measuring security of MPU/MCUs with in-house lab and certifies them thru third-party assessment

SESIP™

NXP applies SESIP (Security Evaluation Standard for IoT Platforms), a security evaluation methodology standard (EN 17927)

SESIP Assurance Level 1 is a self-declaration assessed by independent evaluators.

SESIP Assurance Level 2 is a black-box & Time-limited penetration testing without cooperation from the developer. However, NXP goes beyond by requesting the evaluation labs to check the source code as well.

SESIP Assurance Level 3 is a white-box vulnerability analysis. Time-limited

independent 3rd party labs verify the security claims of NXP products, and the robustness of the implementation is measured against specific attack potentials.

The product's security functionality claims are included in the publicly available **Security Target (ST)** document, and when applicable, the enforced Protection Profiles used in the security evaluation

NXP Certification Process: third party evaluation labs review NXP product security, from threat model to source code

NXP supplies

- Threat Modelling
- Threat Mitigation (Security Mechanisms)
- NXP Security Claims
- Security Guidance
- ISO 21434, RED, US CTM, 62443 Compliance claim mapped in
- Source Code
- IEC 62443-4-1/ISO 21434 process & evidence

Security Lab evaluates and verifies

- Security Testing
- Compliance Claim proof (Crypto, RNG)
- Code Review
- Development Process proof

NXP applies PSA Protection Profile

PSA Certified is an independent security framework and evaluation scheme

- **PSA Level 1** provides evidence that security by design principles have been used in the development of an IoT device, system software or chip. (It is based on a questionnaire).
- **PSA Level 2** specifically addresses scalable software attacks and details security functions necessary in the silicon to prevent those types of attacks (logical security). It requires independent 3rd party labs assessment based on SESIP security evaluations, and protection profile.
- **PSA Level 3** adds hardware attacks which have historically required more time, more experience and more expensive equipment to execute (physical security), and is based on SESIP security evaluations and protection profile.

NXP also applies advanced protection profiles at SESIP certification

NXP bootstraps proof of conformance of OEM products with additional SESIP protection profile

- MCU/MPU Protection Profile standardized in Global Platform
- **Augmented with requirements** from industry standards such as
  - IEC 62443 (Industrial Equipment),
  - NIST 8425 (U.S. Cyber Trust Mark),
  - EN 18031 (Radio Equipment Directive),
  - ETSI 303 645 (Security for Consumer IoT)

Leverage NXP MCU/MPU certifications to build **proof of conformance to Industry security standards at end-product level**

1

Access on TrustCB[1] portal the NXP certificate and security target for selected NXP MCU/MPU

2

Navigate in menu, access IoT pane -> Certificates -> SESIP.

The **SESIP Certificate Report (CR)** obtained by NXP attests the security claims included in the Security Target document.

3

The **Security Target (ST)** describes the security features & functions included in the NXP certified product as well as their implementation

OEMs can leverage on the mappings between standards requirements and NXP security features included in Security Target

4

Based on NXP documents, build your **self-declaration or provide evidences** to evaluation lab for conformance to Industry standards or regulations such as Radio Equipment Directive (RED, EN 18031), IEC 62443-4-2 or NIST 8425 (U.S. Cyber Trust Mark),

TrustCB

SESIP Certificates

CR PDF ST PDF

IEC

U.S. CYBER TRUST MARK

https://trustcb.com/iot/sesip/sesip-certificates/

Simplifying OEM security conformance efforts with NXP certification documents

Extract of SESIP certificate

TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2300162-01
	TrustCB B.V. declares that
Product	i.MX93 EdgeLock Secure Enclave Version A1
	of
Sponsor (and Developer)	NXP Semiconductors Germany GmbH *in* Hamburg, Germany
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.2, July 2023 **Based on** ISO/IEC 15408-1:2009, -2 :2008, -3:2008, Common Criteria for Information Technology Security Evaluation (CC) v3.1, rev 5, and ISO/IEC 18045:2008, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM) v3.1, rev 5 COMMON CRITERIA
ST Reference	i.MX93 EdgeLock Secure Enclave SESIP Security Target, version 1.2
	Summarised:
Assurance Package	SESIP3 *with* Physical Attacker Resistance *and* Software Attacker Resistance: Isolation of Platform
SESIP Profile	SESIP Profile for Secure MCUs and MPUs v1.0, SESIP Profile for PSA Certified Level 3 v1.0
	As evaluated by:
Evaluation Facility	Riscure B.V. located in Delft, The Netherlands
	Under scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.3
Validity	Date of issue: 2024-06-10 Date of expiry: 2026-05-28
Certification Mark	SESIP™3
Signatory	Wouter Slegers, CEO

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave...*continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
	cryptographic functionalities that can be use to identify and authenticate a user and build the final non-repudiation solution.
CR 2.13 – Use of physical diagnostic and test interfaces	Secure Debugging provides protected access to the physical diagnostic and test interfaces of the entire SoC (including the i.MX93 EdgeLock Secure Enclave subcomponent).
CR 3.1 – Communication integrity CR 3.1(1) – Communication authenticity	Cryptographic Operation provides cryptographic operations that can be used to protect integrity and authenticity of transmitted information. Cryptographic Key Generation and Cryptographic Random Number Generation provides cryptographic functionalities that can be used to generate the cryptographic materiel necessary for the protection of transmitted information.. Cryptographic KeyStore provides secure storage that can be used to store cryptographic material (e.g. shared secret) on which such protections is be based. Physical Attacker Resistance provides protections of cryptographic services involved in secure communication integrity and authenticity enforcement against physical attacks. Software Attacker Resistance: Isolation of Platform provides protections of cryptographic services involved in secure communication integrity and authenticity enforcement against remote and local logical attacks.
CR 3.2 – Protection from malicious code	Secure Initialization of Platform provides protection against installation and execution of unauthorized software by checking the integrity and authenticity of the i.MX93 EdgeLock Secure Enclave own firmware, as well as the ones of other SoC processors, at each reset, as part of the secure boot. Software Attacker Resistance: Isolation of Platform provides isolation of the i.MX93 EdgeLock Secure Enclave subsystem against remote and local logical attacks that could be led from malicious code loaded into the rest of SoC. Note also that i.MX93 EdgeLock Secure Enclave is physically isolated from the rest of the SoC by design, using dedicated hardware.
CR 3.3 – Security functionality verification CR 3.3(1) – Security functionality verification during normal operation	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the components to verify the intended operation of the claimed security functions by requiring the execution of functional and penetration testing to those security functions. Secure Initialization of Platform provides integrity and authenticity verification of the i.MX93 EdgeLock Secure Enclave own firmware, as well as the ones of other SoC processors, ensuring a proper helth chack and security configuration at each reset, as part of the secure boot. Attestation of Platform State provides, on demand, the attestation of the state of the i.MX93 EdgeLock Secure Enclave subcomponent (including hashes of the firmware and patch, as well as life cycle state) that can be used to verify the state of the component during operation. Physical Attacker Resistance provides monitoring and detecting of physical attacks during operation.
CR 3.4 – Software and information integrity CR 3.4(1) – Authenticity of software and information CR 3.4(2) – Automated notification of integrity violations	Secure Initialization of Platform provides, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data of i.MX93 EdgeLock Secure Enclave and/or other SoC processors before any execution. Secure Update of Platform additionally checks the version verification of the i.MX93 EdgeLock Secure Enclave firmware/software to be launched. Attestation of Platform State provides, on demand, the attestation of the state of the i.MX93 EdgeLock Secure Enclave subcomponent (including hashes of the firmware and patch, as well as life cycle state).

Extract of Security Target (ST), with example of mapping between IC security features and IEC 62443-4-2 requirements

For governmental applications and protection of sensitive information, NXP certifies products against FIPS and Common Criteria standards

Federal Information Processing Standard - FIPS 140-3

- **FIPS 140-3 L1:** basic security requirements, no physical security, no authentication of end users
- **FIPS 140-3 L2:** limited physical security and authentication of end-users
- **FIPS 140-3 L3:** enhanced physical security, limited environmental protection, identity-based authentication of end-users
- **FIPS 140-3 L4:** full envelope of physical protection, full environmental protection, formal modeling

NXP also certifies algorithm implementation thru Cryptographic Algorithm Validation Program (CAVP) and certifies entropy source against the NIST SP 800-90B standard through the Entropy Source Validation (ESV) program.

Common Criteria

- **CC EAL 1:** products undergo functional testing only
- **CC EAL 2:** closer examination of the design and architecture of the product to identify potential vulnerabilities.
- **CC EAL 3:** systematic testing and a thorough review of security features
- **CC EAL 4:** comprehensive security assessment encompassing design, testing, and code review
- **CC EAL 5:** formal and repeatable process for security development
- **CC EAL 6:** formal verification of design and Security Mechanisms
- **CC EAL 7:** formal methods to verify the design and implementation of security functions

i.MX 93

First MPU with integrated Secure EdgeLock Enclave SESIP/PSA L3 certified,

including evidence of conformance to IEC 62443 and US Trust Mark requirements

RW612

First tri-radio (Wi-Fi® 6, Bluetooth® Low Energy 5.3, 802.15.4) SESIP/PSA L3 certified,

including evidence of conformance to US Trust Mark and ETSI 303 645

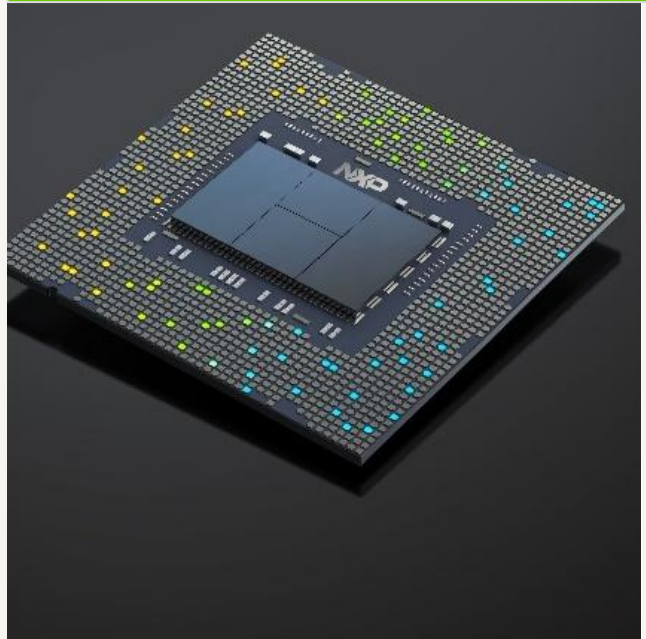
NXP innovates in security certification

SE050/51

First Secure Element IEC 62443-4-2 certified

SE052F

First Secure Element FIPS 140-3 L3 (physical security L4) and Common Criteria EAL6+ (HW/OS) certified



K32W148

MCX W71

First multi-protocol WMCU with conformance to Radio Equipment Directive, SESIP/PSA L2 certified

Certified EdgeLock® Assurance

Security is fundamental to the solutions we create. When you see Certified EdgeLock Assurance, you'll know it's designed to meet industry standards and certified according to Common Criteria EAL3 or higher, SESIP L2 or higher, or equivalent. Proven processes and validation assessments help ensure we deliver trusted solutions for your security challenges. Together, we can advance the world securely with confidence.

Certified EDGELOCK® ASSURANCE by NXP

NXP EdgeLock Security
Protecting the Edge at scale

Cyber attacks increases, exposing device manufacturers and infrastructures owners to disruptions, ransomware and many other related costs

A risk & threat analysis is necessary to design and incorporate adequate protections

NXP offers a range of solutions to address different types of attacks, providing resilience, scalability and modularity to match requested protection profile. Furthermore, NXP EdgeLock security facilitates practical deployment of security in field

NXP provides strong support to compliance with EdgeLock assurance program and evidences of conformance to cyber security standards and regulations

nxp.com