EdgeLock® Secure Enclave

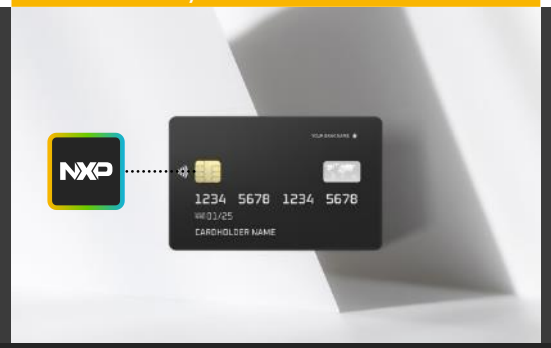
Made for resilience

Technology six pack

March 2024

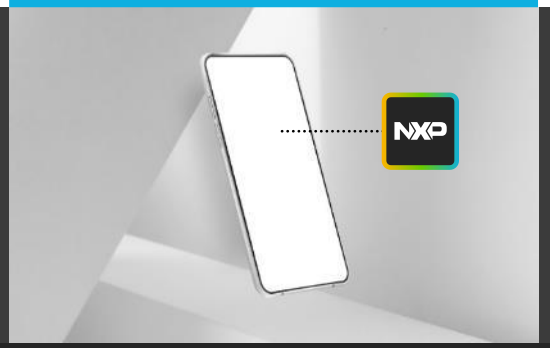
NXP brings trust to Edge Processing leveraging security expertise built over decades

Payment
Payment & Access



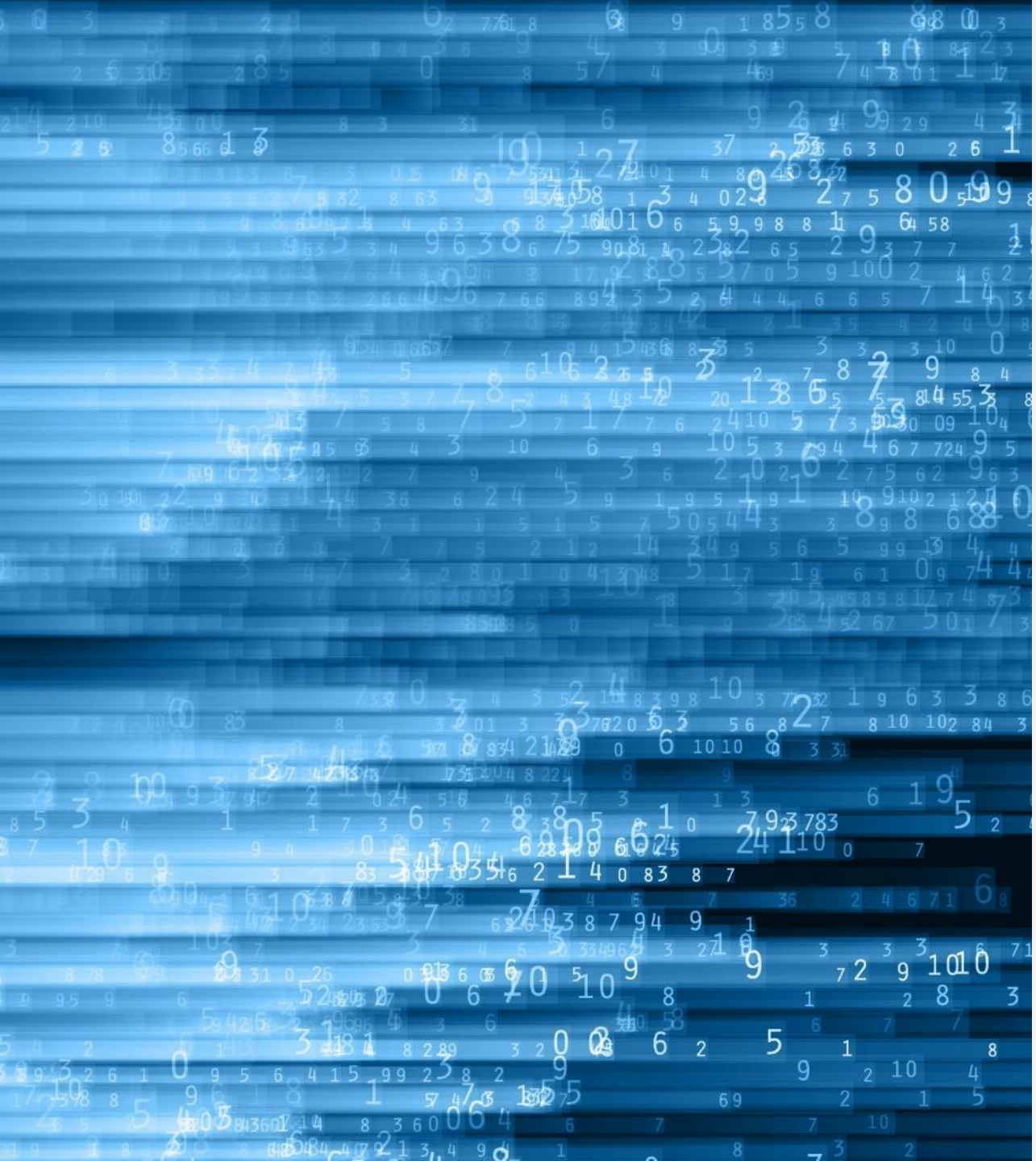
Government
Identity

Mobile
Mobile Wallet



EDGELOCK®
SECURE ENCLAVE

Industrial & IoT
Device security & trusted connections



Connectivity means exposure and cyber risk

Connectivity opens routes into consumer data and systems, as well as key infrastructures such as healthcare & industrial.

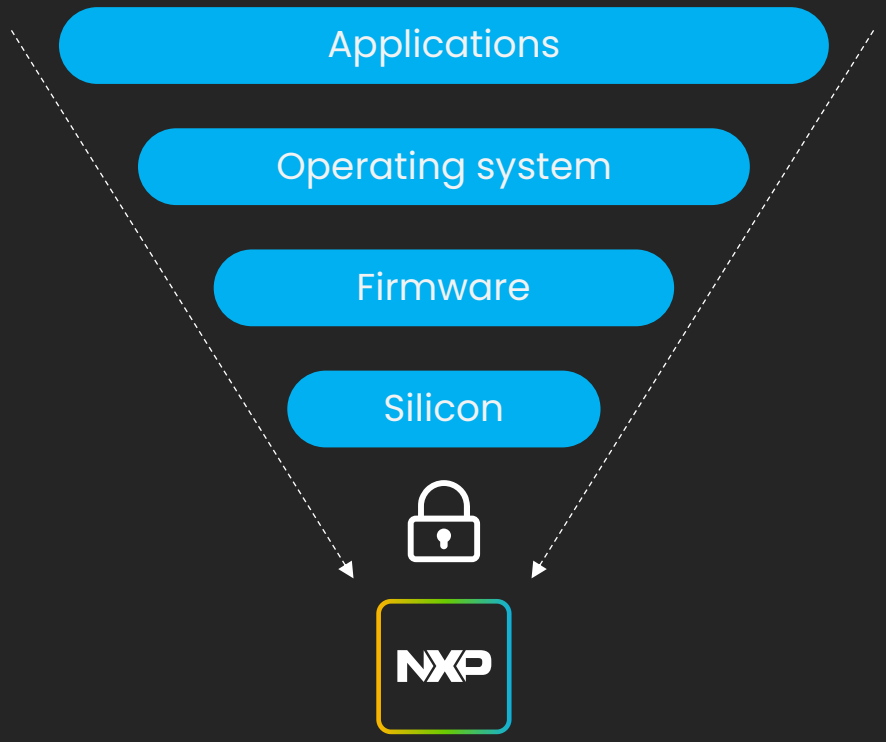
Data encryption & verification, as well as authentication in networks are a must.

But any vulnerability left on devices is also a threat putting at risk availability of services, consumer privacy, people safety, and assets.

Device security is key to mitigate risks

- Many vulnerabilities on device can be exploited by hackers, very often remotely, and including:
  - SW bugs in communication stack, OS or application SW, leading for example to undefined device behaviors
  - Lack of verification on executed FW/SW
- This usually ends up with installation of malicious code, leakage of authentication keys, data extraction, device and service unavailability, etc.

Towards a silicon-based trust anchor to protect security functions



Complex SW is a risk factor

Software of connected devices is complex and prone to many vulnerabilities.

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.

NXP supports OEMs in accessing regulated markets and building resiliency

nxp.com/security

Security functions on-chip with EdgeLock technology, EdgeLock 2GO services, secure provisioning tools/SDK

Extensive 'toolbox' to implement and activate product security capabilities as required by regulators

EdgeLock Secure Enclave (integrated on MCU/MPUs), EdgeLock Secure Elements & Authenticators

Enhanced HW protections of security functions: minimize risks of retrofit, maximize resilience in field, facilitate demonstrability of security robustness and assurance

EdgeLock Assurance program

Procurement of secure components, with NXP Security Maturity Process & chip security certifications (SESIP[1] – EN17927), providing 'Security by Design' at component level, independent 3rd party assessment and Product Security Incident Response handling (PSIRT)

NXP introduces EdgeLock Secure Enclave — a root of trust integrated on NXP edge processing platforms

- 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
- Prevents attacks exploiting shared processing/ storage resources typical to some Trusted Execution Environments

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

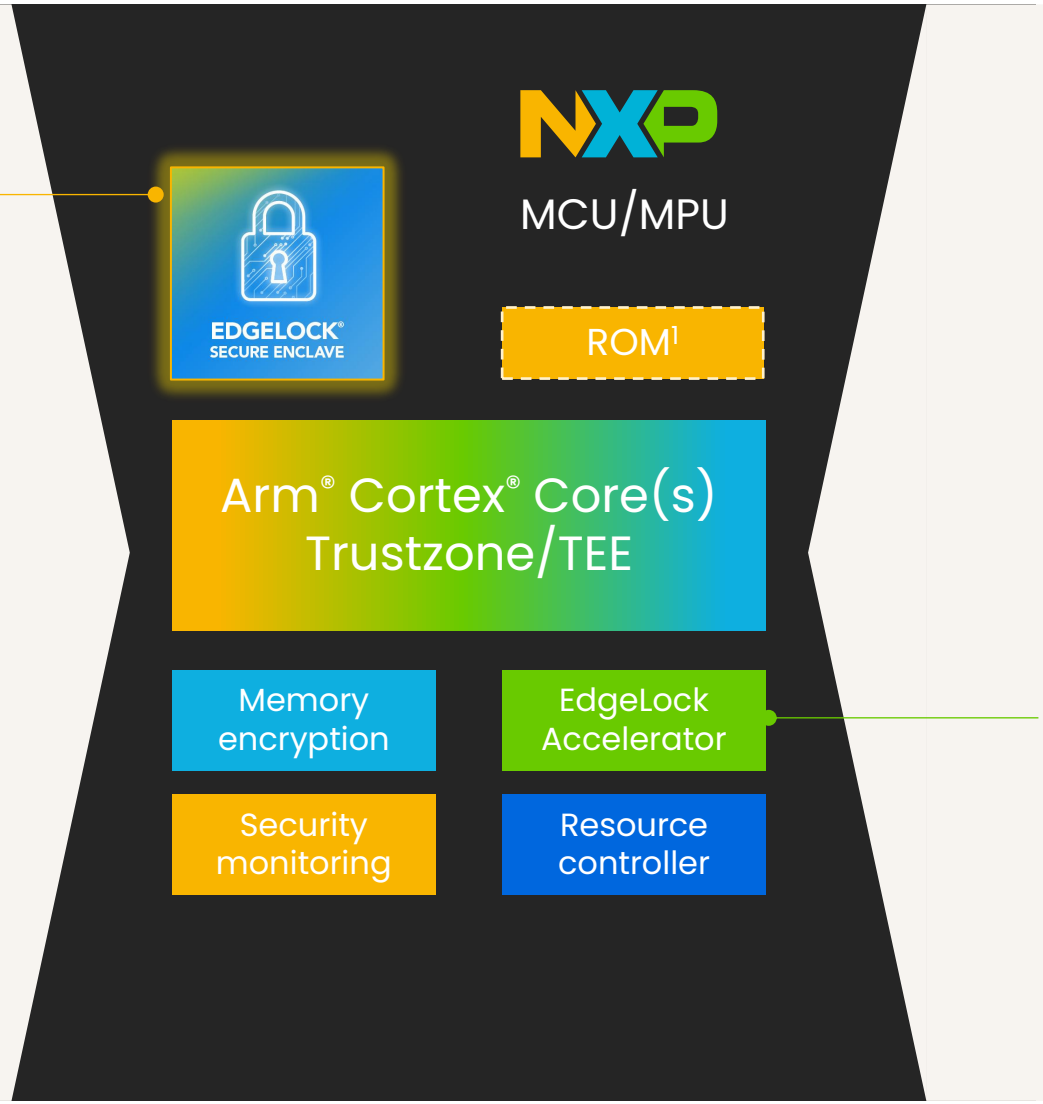
	Core	Advanced
Crypto Services, TRNG	■	■
Secure Key Store	■	■
Device Unique Identity & Keys	■	■
Device Attestation	■	■
Secure Connections	■	■
Key MNGT OTA (EdgeLock 2GO)	**(optional)**[1]	■
Enclave FW/Crypto Updatability	**(optional)**[1]	■
Runtime Device Protection		■
Integrated typically on:	Arm® Cortex®-M 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

EdgeLock Secure Enclave is the headquarter of processing platform security

EdgeLock Secure Enclave

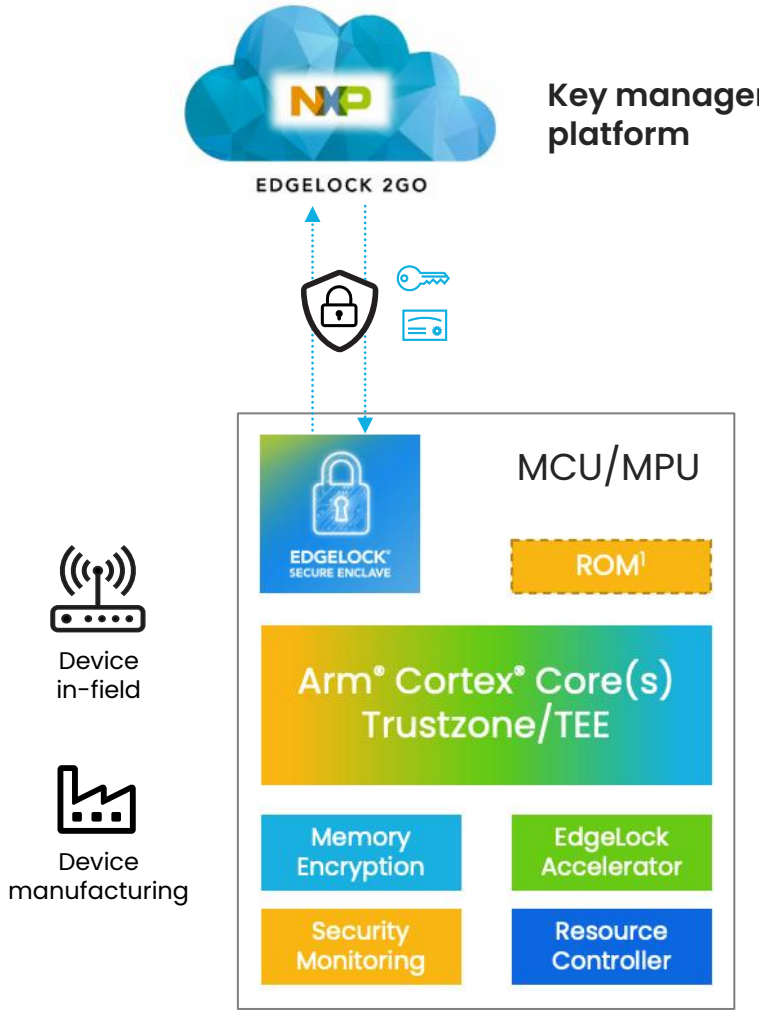
- Root of Trust in the system (isolation)
- Hosts secrets (keys) and platform integrity credentials
- Drives & monitors SoC integrity
- Agnostic of OS running on Application core
- Agnostic of application core type
- Usable through open-source stacks



EdgeLock Secure Enclave embeds cryptographic co-processor but can be aided by specific EdgeLock Accelerator on some MCU/MPUs for advanced crypto performances on target applications

1. Optional ROM (MCUs)

EdgeLock Secure Enclave connects securely to EdgeLock 2GO platform



Please contact NXP sales for availability of EdgeLock 2GO on specific MCU/MPU

EdgeLock Secure Enclave eases the deployment of security on IoT products

- Support of **key security functions** reducing development efforts for OEMs, and including secure boot, measured boot & device attestation, authentication, secure debug, secure update, secure connect, device lifecycle management, data encryption/ authentication, SW (IP) protection
- **Cost savings** on physical protections built at equipment casing level
- An accelerated path to **IoT product certification** (e.g., IEC 62443, US Trust Mark, Cyber Resilient Act) and easier certification maintenance
- **Secure manufacturing** in untrusted locations (control over supply chain) with secure SW and credential install (even for FLASH-less processors)
- An **offload of cryptographic operations** freeing resources on application cores, especially in the context of low latency applications & time-sensitive networks
- **Secure update of root of trust credentials**, at manufacturing but also during device lifetime, without investment in key management infrastructure for OEMs
- **Runtime device protection** functions for management of security in field (Advanced profile)

EdgeLock Secure Enclave, foundation for compliance to cyber regulations & standards

- Secure device initialization and configuration
- Asset authentication
- Secure device access control
- Data protection
- Product monitoring and cyber security state awareness
- Vulnerability fix and secure update
- Reduction of incidents' impact and product availability

U.S. CYBER TRUST MARK

ETSI EN 303 645 V2.1.1 (2020-06)

CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

EDGELOCK SECURE ENCLAVE

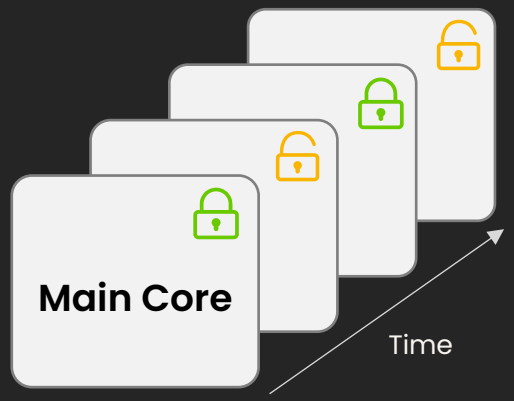
A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.

ISA/IEC 62443
Series of Standards

ISA IEC ISO

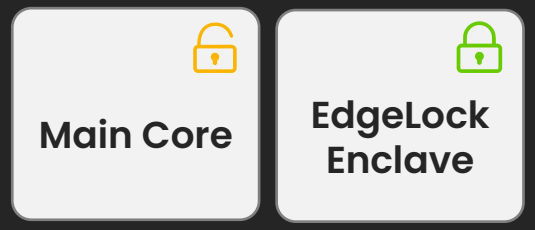
EdgeLock Secure Enclave goes beyond TrustZone® to protect security functions

TrustZone



Time isolation

Enclave

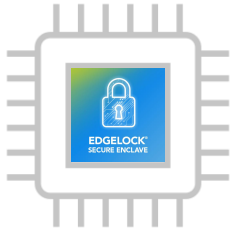


Physical isolation

- TrustZone is based on alternate execution in time of SW partitions on the same core (with limitation of access to peripherals and memory per partition)
- **EdgeLock Secure Enclave** provides
  - Higher degree of isolation based on physical separation, more secure for critical and sensitive security functions
  - Ease of use (no interruption of application SW)
  - Availability for runtime integrity protection functions
- NXP provides both technologies (sometimes concurrently on same IC but for different usage)

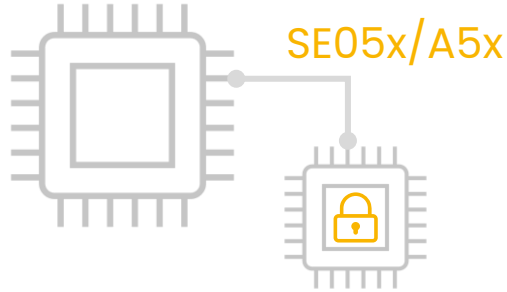
NXP EdgeLock Secure Element offering complements EdgeLock Secure Enclave

- Both EdgeLock Secure Enclaves and EdgeLock Secure Elements are secure vaults for device credentials and provide cryptographic services
- EdgeLock Secure Element adds protections against advanced HW (physical) attacks, high certification levels and can be personalized with custom credentials at NXP manufacturing
- EdgeLock Secure Enclave, integrated into NXP processing platform, adds device integrity attestation & protection (including runtime with advanced profile)



Enclave

- ✓ Protection against SW and basic HW attacks
- ✓ Certified according to SESIP/PSA
- ✓ Edge processing integrity protection
- ✓ Integrated into NXP (W)MCU/MPUs



Secure Element

- ✓ Protection against SW and advanced HW attacks
- ✓ Certified Common Criteria EAL6+, FIPS
- ✓ Customization & personalization at NXP
- ✓ Can be plugged to any type of ASIC or processor (including non-NXP MCU/MPU)

EdgeLock Secure Enclave
Made for resilience

Future-proof security hardware

Essential security tool to access newly regulated market and remain certified

Continuity of chain of trust, from chip manufacturing to commissioning of end-user equipment

Secure device management to stay in control with devices in the field in a dynamic cyber landscape

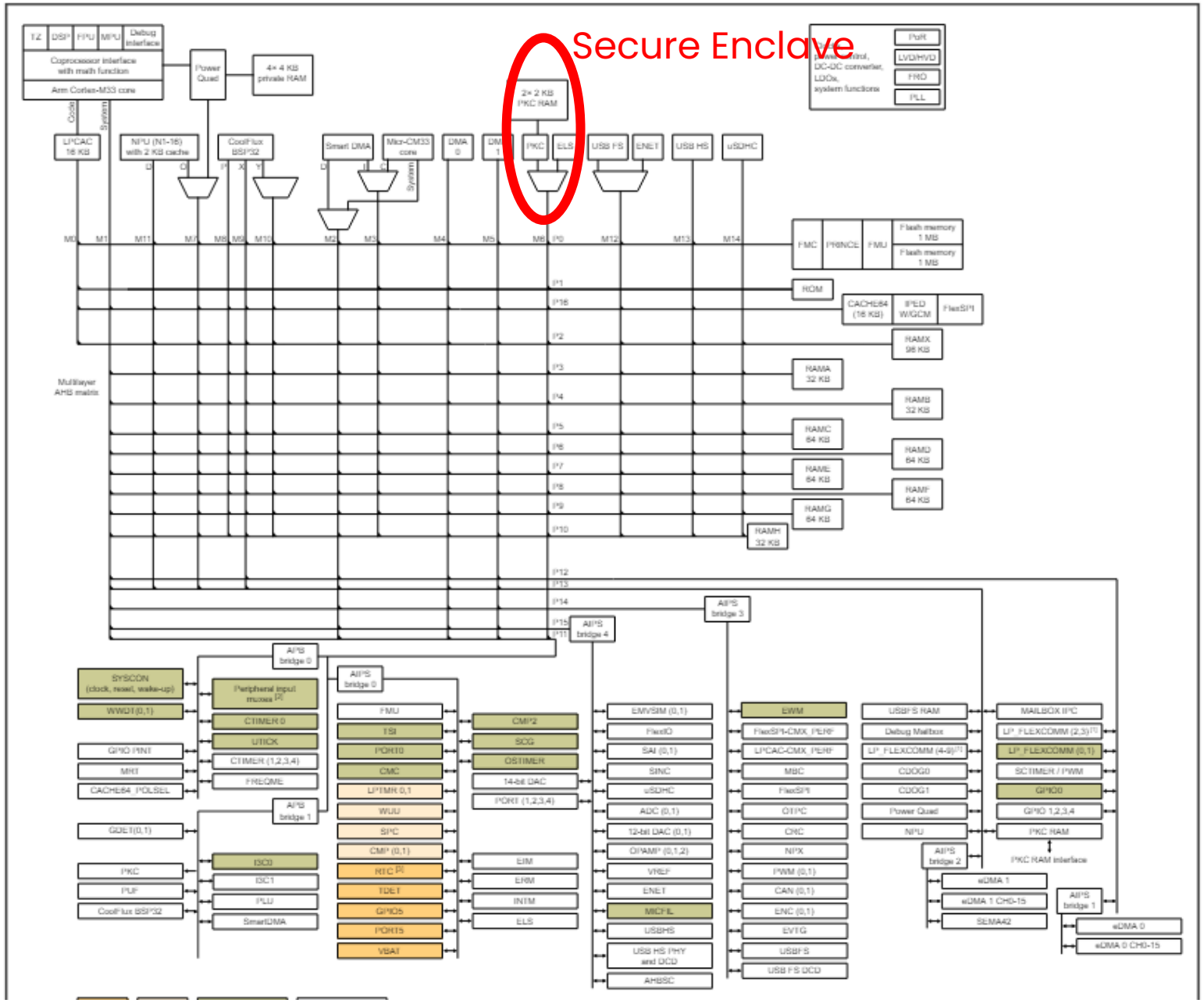
nxp.com/security

nxp.com

Annex

MCX N bus connections

How the AHB matrix treats the secure enclave and the PKC (Public Key Cryptography) different from the rest of the chip building the security island (EdgeLock Secure Enclave). Reference [MCX Nx4x Reference Manual]



EdgeLock Assurance program
Made for resilience

EdgeLock Assurance Program portal.
- General information of how NXP manages Edgelock assurance
- Description and links to how NXP makes Edgelock secured and certified

EdgeLock conpliance portal.
- Links to the certification databases

nxp.com/security