EdgeLock® Secure Element (SE) & Secure Authenticator (SA)

IoT Security Portfolio 6-Pack

PLUG&TRUST

The fast, easy way to deploy secure IoT connections

BL C&S IoT Security Team

MARCH 2022

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

NOTE TO DISTRIBUTORS

- This deck focuses on the mass market variants of the EdgeLock SE & SA portfolio.
- If you have a customer with need for application specific variants as the updatable EdgeLock SE051, the UWB variant EdgeLock SE051W,
  or you need more information on the Middleware of EdgeLock 2GO Service, please contact your NXP Account Manager who will connect you to the NXP CAS or BL team.

OVERVIEW

GENERAL PART

- Portfolio overview
- Platform features
- PSP concept
- Certification
- EdgeLock 2GO service

PRODUCT SPECIFIC PART

- EdgeLock SE050E generic mass market SE for multiple IoT use cases (mass market)
- EdgeLock SE050F FIPS certified SE (FIPS variant)
- EdgeLock A5000 SA for authentication use cases (mass market)

Short heads up:

- EdgeLock SE051 updatable SE (application specific markets)
- EdgeLock SE051W SE for UWB (application specific markets)

EDGELOCK SECURE ELEMENTS AND SECURE AUTHENTICATORS
A ROOT OF TRUST ENABLING NEW USE CASES

Certified state of the art security concepts strongly protect against most recent attack scenarios. Additional features enable a wide range of use cases to answer multiple application needs in IoT and especially industrial.

ENHANCED SECURITY

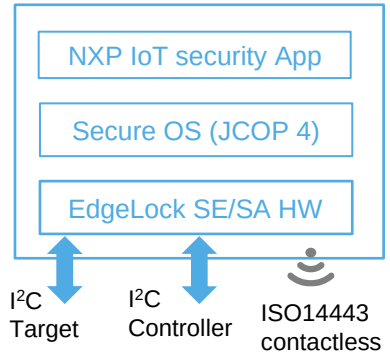
- CC (Common Criteria) EAL 6+ AVA_VAN.5 certified HW & OS and FIPS 140-2 L3
- RSA & ECC functionalities
- Future proof curves & higher key length
- Encrypted communication with host processor
- Symmetric ciphers for en/decryption

HIGH FLEXIBILITY

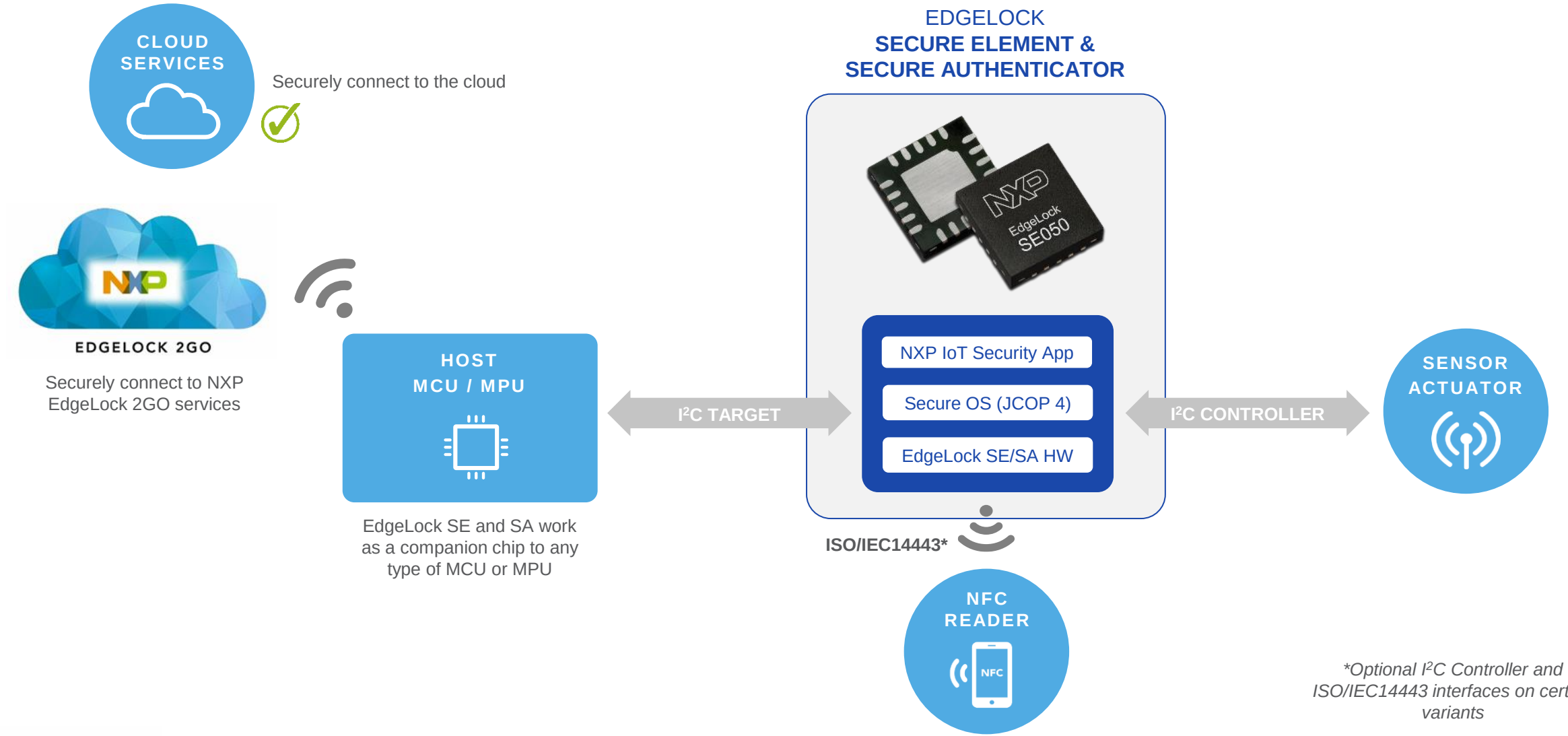
- Product family with multiple solutions for various use cases in Industrial, Smart City, Smart Metering, and Smart Home.
- Flexible applet with dynamic user memory. 8-50kB.
- Multiple interfaces – I^2C Target, I^2C Controller, ISO14443, depending on configuration.
- Plug & Trust: Easy integration with multiple MCU/MPU platforms, OS and clouds
- Support for TLS, IEC62443, DLMS\COSEM, ISO15118, OPC-UA, Matter, Qi 1.3 Authentication, UWB

PLUG &TRUST

Out-of-the-box Solution

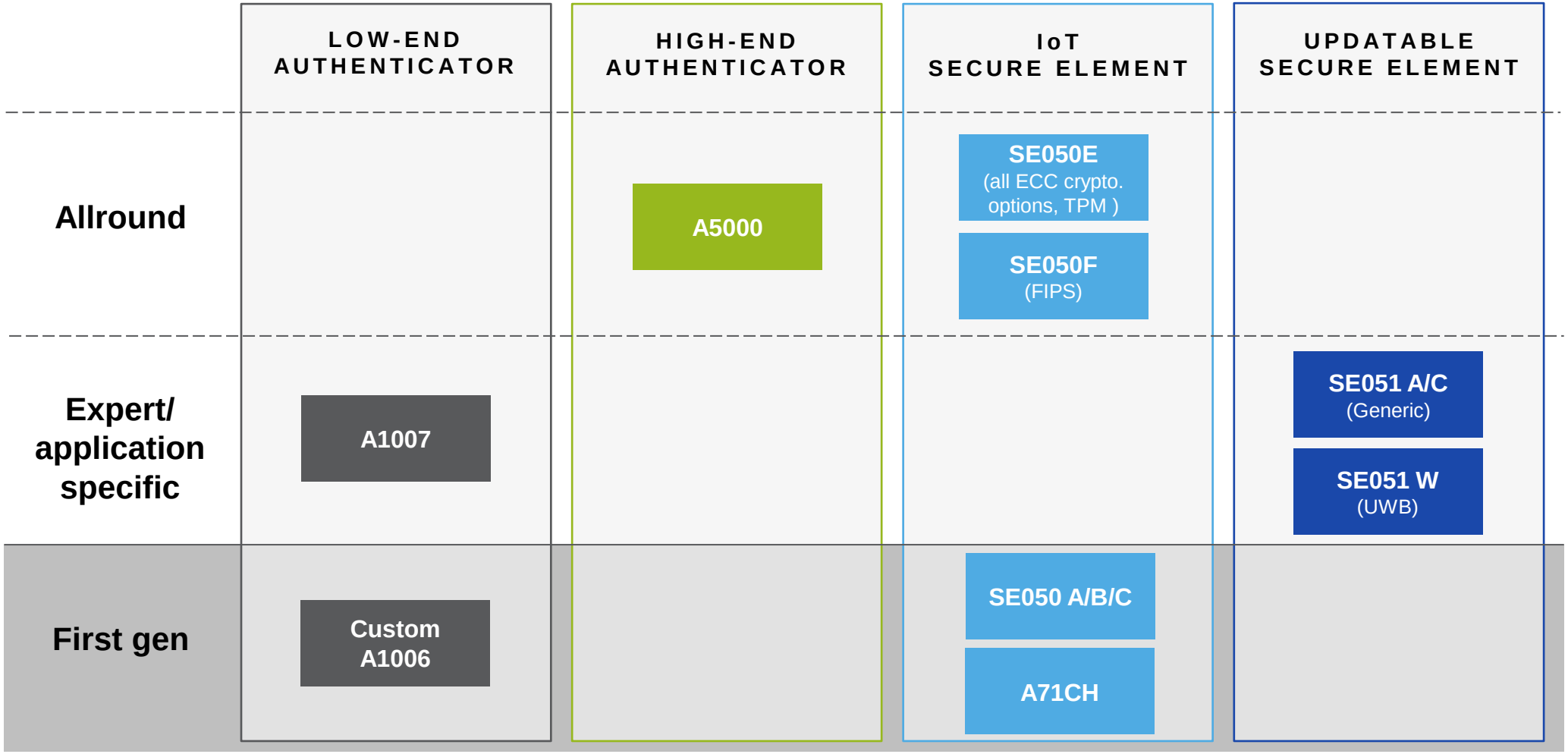


A TRUSTED HARDWARE THAT CAN BE ADDED TO ANY IOT ARCHITECTURE FOR SECURITY



Optional I²C Controller and ISO/IEC14443 interfaces on certain variants

PORTFOLIO CHANGES: OVERVIEW Q2 2022 PICTURE



EDGELOCK SECURE ELEMENT AND SECURE AUTHENTICATOR PORTFOLIO INTRODUCING THE NEW NXP SECURE AUTHENTICATOR

FIT-TO-PURPOSE CERTIFIED AUTHENTICATOR

mass market

A5000

FIT-TO-PURPOSE SECURE AUTHENTICATOR

- Simple authentication use case with event counters
- Device calibration & configuration data
- Dynamic key management

ALLROUND MULTI USE CASE SE

mass market

SE050E/F

UPDATABILITY

non-mass market

SE051

ALL ROUND SECURE ELEMENT – FLEXIBLE SOLUTIONS FOR MULTIPLE USE CASES

- Rich crypto set & agility (incl. RSA, MIFARE, Future proof Crypto Curves)
- Large dynamic File system (50 kB) and API for multi-use cases support
- Secure sensing & actuation interface
- TPM functionalities
- Updateable offline (SE051x)

EDGELOCK SE05X AND EDGELOCK A5000 SE/SA FAMILY

How to enable secure IoT application?

What?

- A **turnkey** solution for several IoT applications and use cases
- **Easy** integration from trust provisioning to secure coding
- **Certified, future proof and updatable.**
- **Extended** PSP for customers' integration

Why?

- Implementing IoT solutions is not an easy task: secure implementation of cryptographic algorithms, key and credential management, trust in the supply chain, compliance with security standards
- Secure implementations and IoT solutions require customers focus and engagement from A to Z of a project which is a burden for most customer

How?

- NXP takes care of all the security/enablement aspects from trust provisioning to secure coding.
- EdgeLock SE05x implements the cryptographic algorithms and protocol required for most IoT application, from TLS to KDFs
- EdgeLock 2GO services, NXP provisions credentials and customize SE/SA without the need for a customer to set up a costly PKI infrastructure
- EdgeLock SE/SA is certified Common Criteria EAL 6+, FIPS 140-2 Level 3 and SE051 is updatable
- All EdgeLock products come with a PSP including Host SW and DevKit so that customers can focus only on the application definition

			A1007	A5000	SE050E	SE050F (FIPS Module)	SE051C2	SE051A2	SE051W
Authentication Application \ IoT Applet	ECC Crypto Schemes	ECDSA	X (P-224 bit only)	X	X	X	X	X	X
		ECDH/ECDHE	X (ECDH only)	X	X		X	X	X
		DH_Mont			X		X		
		ECDAA			X		X		
		EdDSA			X		X		
	Supported Elliptic Curves	Binary 163bit	X						
		NIST (192 to 521 bit)		X (256/384 only)	X	X (>=224 bit)	X	X	X
		Brainpool (160 to 512 bit)			X	X (>=224 bit)	X	X	X
		Koblitz (160 to 256 bit)			X	X (>=224 bit)	X	X	X
		Barreto-Naehrig (256 bit)			X		X		
		Curve25519 [Twisted Edwards/Montgomery]			X		X		
		Montgomery-Curve448			X		X		
	RSA	RSA				>=2k, no RSA plain, no RSA 4kGen	Up to 4k		Up to 2k
	Symmetric Crypto Algorithm	PRESENT (NXP Proprietary)	X						
		3DES (2K, 3K)		X	X	X (only 3K)	X	X	X
		AES (128, 192, 256)		X	X	X	X	X	X
	AES Modes	CBC, ECB, CTR		X	X	X	X	X	X
		CCM, GCM		X	X		X	X	X
	MAC	HMAC, CMAC		X	X	X	X	X	X
		GMAC		X	X				X
	Hash Function	SHA-1, SHA-224 to 512		X -256/384	X	X (No SHA-1)	X	X	X
	Key Derivation (KDF)	TLS (KDF, PSK)		X	X		X	X	X
		MIFARE DESFire			X		X	X	X
		PBKDF2 (Wifi EAP)			X		X	X	X
		HKDF		X	X	X	X	X	X
	TPM Functionality				X		X		
	Secure Channel	Secure Channel Host-SE (Platform SCP)		X	X	X (Mandatory)	X	X	X
	Pre-Provisioned		X	X	X	X	X	X	X
App. Specific Support	Updatability	SEMS Lite					X	X	X
	UWB								UWB secure ranging
HW Features	TRNG			NIST SP800-90B, AIS31	NIST SP800-90B, AIS31	NIST SP800-90B, AIS31	NIST SP800-90B, AIS31	NIST SP800-90B, AIS31	NIST SP800-90B, AIS31
	DRBG			NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20
	User Memory – Full Feature - NV		4 kbit	8 kB	50 kB	50 kB	46 kB	46 kB	25 kB
	User Memory – Maximum - NV		4 kbit	8 kB	50 kB	50 kB	104 kB	104 kB	25 kB
	Interfaces	OWI	X						
		ISO14443				X	X		X
		I^2C Target	X	X (up to 1 Mbit/s)	X (up to 1 Mbit/s)	X (up to 3.4 Mbit/s)	X (up to 3.4 Mbit/s)	X (up to 3.4 Mbit/s)	X (up to 3.4 Mbit/s)
		I^2C Controller			X	X	X		X
	Temperature range		-40 to +85 ºC	-40 to +105 °C	-40 to +105 °C	-40 to +105 °C	-40 to +105 °C	-40 to +105 °C	-40 to +105 °C
	Package		HXSON6	HX2QFN20	HX2QFN20	HX2QFN20	HX2QFN20	HX2QFN20	HX2QFN20

IOT APPLICATIONS

INDUSTRIAL
PLCS
ROBOTS
SENSORS
NETWORKING DEVICES

IP CAMERAS

SMART METERS
ENERGY MANAGEMENT
DLMS/COSEM

GAMING

GATEWAYS
ROUTERS

EV CHARGERS

ACCESS
SMART LOCKS
UWB
FREE-HANDS ACCESS

COMPUTING

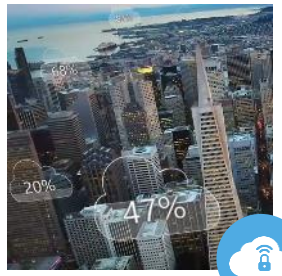
SMART HOME
MATTER
CONSUMER DEVICES
SPEAKERS

SMART APPLIANCES
MATTER

MEDICAL

MOBILE ACCESSORIES

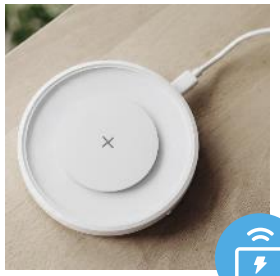
USE CASES ENABLING IOT APPLICATIONS
EDGELOCK SECURE ELEMENT / SECURE AUTHENTICATOR



SECURE CLOUD ONBOARDING

DEVICE-TO-DEVICE AUTHENTICATION

ATTESTATION & PROOF OF DEVICE ORIGIN



QI 1.3 WIRELESS CHARGING AUTHENTICATION

SENSOR DATA PROTECTION

LATE-STAGE PARAMETER CONFIGURATION

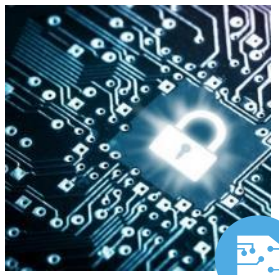
WI-FI CREDENTIAL PROTECTION

MATTER DEVICE COMMISSIONING

SECURE ACCESS MODULE

UWB

DEVICE ID FOR BLOCKCHAIN



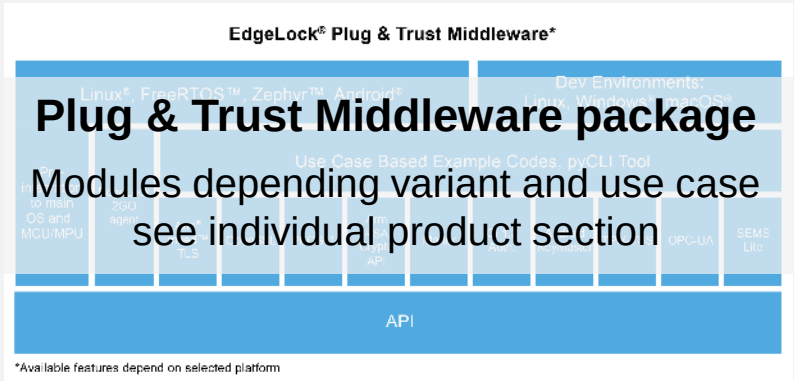
TRUSTED PLATFORM MODULE

IOT SECURITY USE CASES

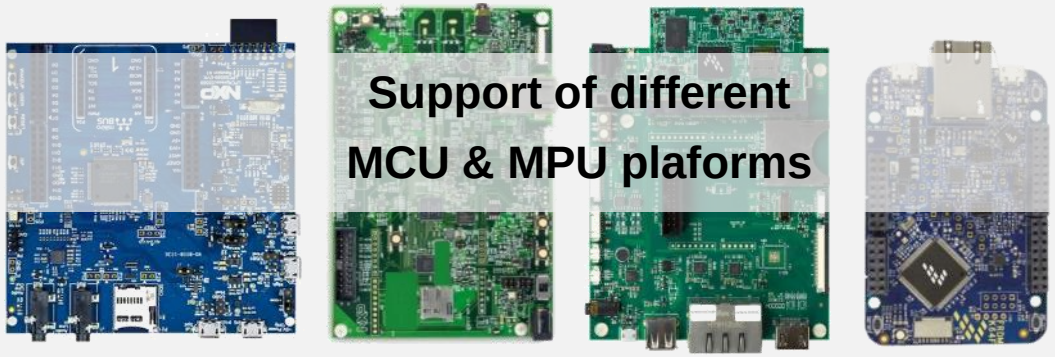
EdgeLock SE/SA are converging secure sensing, secure connections to multiple cloud services, and integrity protection of a trusted IoT platform.

EACH PRODUCT VARIANT COMES WITH A DEDICATED PRODUCT SUPPORT PACKAGE - CONCEPTUAL VIEW, DETAILS PER PRODUCT SECTION

Plug & Trust middleware



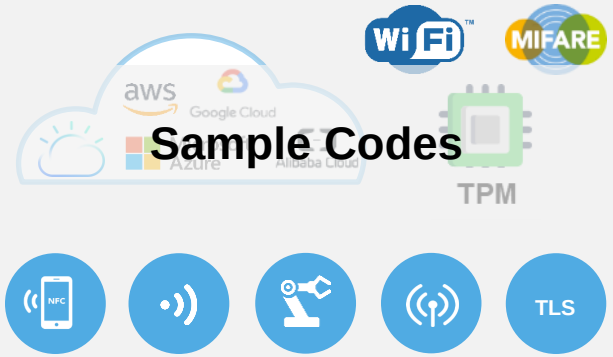
Supported evaluation MCU/MPU boards



- K64F
- LPC55S69
- i.MX RT1060
- i.MX RT1170
- i.MX 8M
- Raspberry Pi
- HiKey 960

EdgeLock SE050 Arduino compatible development kit

Demo codes



Documentation

Omni comprehensive host-agnostic support package allow customers to easily implement security features in multiple MCU/MPU without needing secure coding nor credentials injection.
Example SW codes for several use cases: cloud onboarding, TLS, Host- SE binding, TPM functionalities

PLUG & TRUST MIDDLEWARE ON NXP.COM

- The NXP Plug & Trust Middleware can be downloaded from the “Tools & Software” area on the respective product page.
- The NXP Plug & Trust Middleware is part of the product support package of our A5000 and SE05x family.
- NXP may update the NXP Plug & Trust Middleware with new features and maintenance of the existing code.
- NXP may at its own discretion consider requests for changes or new features. Any request should be communicated to NXP for consideration as early as possible.
- License:
  - The NXP Plug & Trust Middleware package available on nxp.com comes with a proprietary EULA click through license
  - Mini and Nano packages with subsets of the components are also available with an Apache2 license on GitHub

EDGELOCK SE05x AND A5000 BOARDS

OM-A5000ARD

- **Color**: purple
- **Board 12NC**: 9354 243 19598
- **Sample**:
  A5000R2HQ1/Z016U
  OEF: A736r4

OM-SE050ARD-E

- **Color**: blue
- **Board 12NC**: 9354 332 66598
- **Sample**:
  SE050E2HQ1/Z01Z3
  OEF: A921r1

OM-SE050ARD-F

- **Color**: black
- **Board 12NC**: 9354 357 63598
- **Sample**:
  SE050F2HQ1/Z018H
  OEF: A92Ar1

OM-SE051ARD

- **Color**: white
- **Board 12NC**: 9353 991 87598
- **Sample**:
  SE051C2HQ1/Z01TV
  OEF: A8FAr5

OM-SE051ARD-W

- **Color**: yellow
- **Board 12NC**: 9354 210 01598
- **Sample**:
  SE051W2HQ1/Z013Y
  OEF: A739r5 (IC will report A739r4)

KEY RESOURCES ON EDGELOCK SE & SA

Web Presence

Portfolio Family Webpage

>> IoT Security and Authentication

Product Webpage

including documentation, app notes, MW, video tutorials, etc.

>> PSP EdgeLock SE050

>> PSP EdgeLock A5000

Development Kit Webpage

including app notes, etc.

>> TSP EdgeLock SE050

>> TSP EdgeLock A5000

Public Webinars

EdgeLock SE050 product introduction & new use cases *(30 min)*

>> Watch the recording

Getting started with EdgeLock SE050 support package *(30 min)*

>> Watch the recording

Getting started with EdgeLock SE050 for Industrial *(30 min)*

>> Watch the recording

Use Cases

Information on use cases

including one-pagers, app notes, demo videos, supporting documentation, etc.

>> IoT Security Use Cases

EDGELOCK SE & SA PRODUCT FAMILY ORDER DETAILS

Variant	Status	Orderable Part Number	Description	T-Range	12NC
A5000	orderable	A5000R2HQ1/Z016UZ	Simple use case certified IoT SA with ECC NIST, AES	-40 to +105 °C	9354 262 25472
A5000 dev kit	orderable	OM-A5000ARD	A5000 Arduino compatible development kit	-40 to +105 °C	9354 243 19598
SE050E	orderable	SE050E2HQ1/Z01Z3Z	Mainstream ECC variant (ECC all curves, AES, 3DES, MIFARE KDF, I^2C Controller)	-40 to +105 °C	9354 343 82472
SE050E dev kit	orderable	OM-SE050ARD-E	SE050E Arduino compatible development kit	-40 to +105 °C	9354 332 66598
SE050F	orderable	SE050F2HQ1/Z018HZ	FIPS variant (ECC, RSA, AES, 3DES, MIFARE KDF, CL-IF, I^2C Controller)	-40 to +105 °C	9354 284 44472
SE050F dev kit	orderable	OM-SE050ARD-F	SE050F Arduino compatible development kit,	-40 to +105 °C	9354 357 63598
SE051C2	orderable	SE051C2HQ1/Z01XDZ	SEMS Lite, ECC, RSA, AES, MIFARE KDF, I^2C Target, I^2C Controller, ISO14443	-40 to +105°C	9354 144 57472
SE051A2	orderable	SE051A2HQ1/Z01XEZ	SEMS Lite, ECC, AES, MIFARE KDF, I^2C Target	-40 to +105°C	9354 144 58472
SE051A/C Dev Kit	orderable	OM-SE051ARD	SE051A/C Arduino compatible development kit (config of SE051C2)	-40 to +105°C	9353 991 87598
SE051W	orderable	SE051W2HQ1/Z019TZ	SE051 for UWB, in conjunction with SR150	-40 to +105°C	9354 284 64472
SE051W dev kit	orderable	OM-SE051ARD-W	SE051W Arduino compatible development kit for UWB	-40 to +105°C	9354 210 01598
RasPi board	orderable	OM-SE050RPI	Arduino to Raspberry-Pi adapter board (for all SE & SA ARD boards)		9353 986 42598

Certification and Standards

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP EDGELOCK SE & SA CERTIFIED, FUTURE PROOF AND MAINTAINED SECURITY

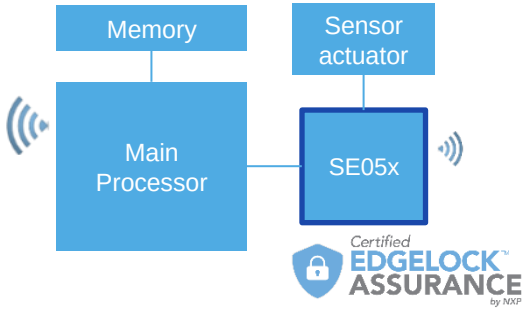
SMART HOME

SMART CITY

INDUSTRIAL

CERTIFIED SECURITY

- EdgeLock SE05x and A5000 is a discrete HW **tamper resistant security** component
- **Dedicated safe environment** to host security functions (by isolation)
- Companion chip to any type of MCU, MPU and AP bringing design **scalability and interoperability**
- **Certified EAL 6+ and FIPS 140-2** according to Common Criteria standard with 3rd party lab evaluation

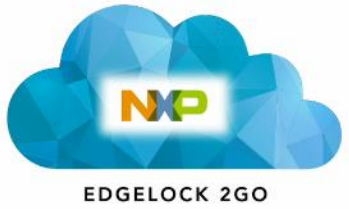


FUTURE PROOF

- **Compliance** to different application requirements and regions thru support of a broad range of cryptographic options and key lengths
- **Multi use case security** component including secure connections to multiple cloud & services, device attestation, secure remote device administration, secure device configuration, secure sensing and actuation, secure UWB ranging, device-user binding

MAINTAINED SECURITY

- **SEMS Lite** technology for applet update OTA, multicast (SE051)
- Device **root keys/certificates** pre-injection in NXP trusted and secure infrastructure
- **NXP Edgelock 2GO** Cloud Service associated with SE05x for seamless key management OTA: e.g., cloud migration during life, installation and revocation of services, management of FW verification keys & access keys, management of device configuration, overproduction control, renewal and rotation of keys/certs



CERTIFICATES AND SUPPORTED STANDARDS

SMART HOME

SMART CITY

INDUSTRIAL

CERTIFICATES

- **Common Criteria CC EAL 6+ AVA_VAN.5**
  - All platforms certified up to OS level according to Common Criteria standard with 3rd party lab evaluation
- **FIPS 140-2 Level 3**
  - SE050/1 FIPS certified L3 with physical security of L4 and RNG compliant to SP800-90A/B
  - NXP provides ready to use FIPS approved modules (SE050F, SE051F).
  - All security rules enforced automatically. No need to be aware and follow all of the security rules as e.g. in the level 2 module's Security Policy.
- **SE051 SESIP**
  - SESIP is the Security Evaluation Standard designed for IoT Platforms, by GlobalPlatform.
  - SE051 have been certified with full physical attack resistance for the NXP IoT applications and secure lifecycle management
- **IEC62443-4-1 and -4-2** for Industrial IoT
  - All SE enabling IEC62443,
  - app note www.nxp.com/docs/en/application-note/AN12660.pdf
  - SE050/1 certified to IEC62443-4-1
  - SE051 certified to IEC62443-4-2
  Customers can leverage the SE05x IEC62443 certification for their composite certification.

SUPPORTED STANDARDS

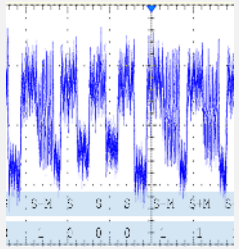
- **OPC UA**
  - Mainstream variants enabling OPC UA, sample code available
- **Smart Metering**
  - DLMS/COSEM: A5000, SE50E include crypto functions enabling DLSMS
  - Dedicated variants for German, France & UK Metering
- **EV Charging, ISO15118**
  - SE05x enabling ISO15118
- **Qi 1.3 Authentication**
  - A5000/SE05x enabling WPC Qi 1.3 Authentication for wireless chargers
- **UWB**
  - Dedicated variant for UWB: SE0501W
- **Matter, Smart Home**
  - Dedicated variant enabling full Matter Security

PLUG&TRUST

EDGELOCK SE & SA PROVIDE HIGHLY CERTIFIED AND PROVEN SECURITY

- EdgeLock SE/SA embed tamper resistance technology against attackers with high attack potential.
- All logical and physical attacks known to date by academia, security community, government bodies are in scope including:

SIDE-CHANNEL ATTACKS



- Power analysis (SPA, DPA, CPA)
- Electromagnetic analysis (SEMA, DEMA, CEMA)
- Timing Analysis
- Template Analysis
- Machine Learning attacks (new: deep learning)

PHYSICAL ATTACKS

- Focused Ion Beam (FIB) incl. IC modification
- Micro-probing
- Signal forcing
- Photon emission microscopy
- Reverse-engineering

FAULT INJECTION ATTACKS

- Power glitching
- Electromagnetic fault injection
- FBBI
- Laser fault injection
- Single and multiple shot scenarios

LOGICAL ATTACKS

- Fuzzing
- API misuse
- Test feature misuse
- RNG entropy analysis
- Micro-arch. attacks like Spectre/Meltdown

EdgeLock 2GO Service

SECURE CONNECTIONS
FOR A SMARTER WORLD

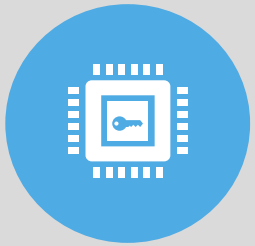
EDGELOCK 2GO SERVICE FOR DEVICE IDENTITY MANAGEMENT

EdgeLock 2GO

A set of services for managing the credentials on your devices

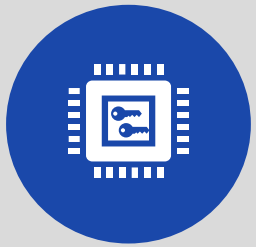
EDGELOCK® ASSURANCE by NXP

EDGELOCK 2GO **READY**



EdgeLock SE & SA pre-provisioned with default keys and certificates

EDGELOCK 2GO **CUSTOM**



Custom provisioning of EdgeLock SE & EdgeLock SA

EDGELOCK 2GO **MANAGED**

NXP cloud service for managing device identities over-the-air

For more information, visit www.nxp.com/EdgeLock2GO

EDGELOCK 2GO READY: CONFIGURATION

	Pre-injected Root of Trust*	Applet Updatability
A5000	• Two ECC NIST P-256 key pairs & X.509 certificates	
SE050E	• Four ECC NIST P-256 key pairs and X.509 certificates • One ECC NIST P-256 and attestation** key pair and certificates	
SE050F	• Four ECC NIST P-256 key pairs and X.509 certificates • Two RSA 2048-bit key pairs and X.509 certificates • One ECC NIST P-256 and one RSA 2048 attestation** key pair and certificates • Two RSA 4096 key pairs	
SE051A	• Two ECC NIST P-256 key pairs & X.509 certificates	SEMS Lite for Applet updates Perso Applet for platform config
SE051C	• Four ECC NIST P-256 key pairs and X.509 certificates • Two RSA 2048-bit key pairs and X.509 certificates • One ECC NIST P-256 and one RSA 2048 attestation** key pair and certificates • Two RSA 4096 key pairs	SEMS Lite for Applet updates Perso Applet for platform config

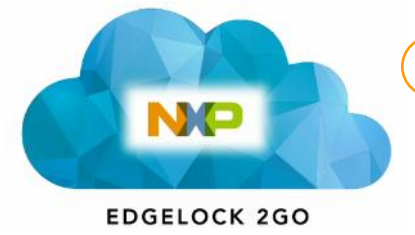
*certificates are signed by NXP Root CA, keys are device individual.
For more details, please refer to the specific Configuration Data Sheet.

** Attestation keys have the “read with attestation” policy. For more details refer to the APDU spec

@DISTRIBUTORS: PLACEHOLDER SLIDE TO ADD YOUR PROVISIONING SERVICE

EDGELOCK 2GO MANAGED

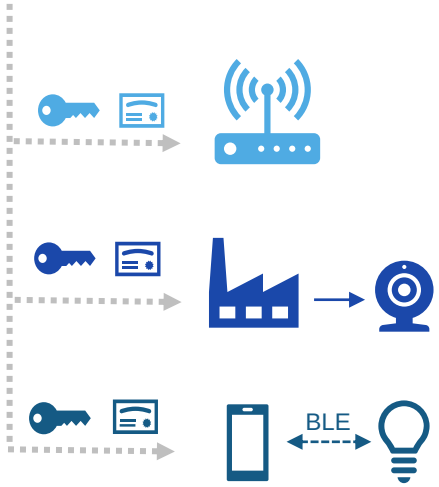
Onboard and manage the lifecycle of your devices



2 Register your devices to your services

Your cloud service

1 Issues keys and certificates for your devices



Your devices

3 Your devices can connect to your cloud services

SECURE

- End-to-end security from chip to cloud
- Leveraging NXP security infrastructure
- Leveraging EdgeLock SE05x/A5000

ZERO-TOUCH

- Easy to configure
- Automatically onboard your devices in your cloud account
- No key or certificate handled by OEM

FLEXIBLE

- Supports multiple types of credentials
- Apply different configurations depending on your customers or projects
- Renew or add new credentials on devices in the field

PLUG&TRUST

Request an eval account at: https://contact.nxp.com/edgelock2go-signup

EdgeLock SE050E

Mainstream Secure Element

EdgeLock SE050F

FIPS-Certified Secure Element

SECURE CONNECTIONS
FOR A SMARTER WORLD

KEY RESOURCES ON EDGELOCK SE050

Web Presence

Product Webage
including documentation, app notes, MW, video tutorials, etc.

>> PSP EdgeLock SE050

Development Kit Webpage
including app notes, etc.

>> TSP EdgeLock SE050

Public Webinars

EdgeLock SE050 product introduction & new use cases *(30 min)*

>> Watch the recording

Getting started with EdgeLock SE050 support package *(30 min)*

>> Watch the recording

Getting started with EdgeLock SE050 for Industrial *(30 min)*

>> Watch the recording

Use Cases

Information on use cases
including one-pagers, app notes, demo videos, supporting documentation, etc.

>> IoT Security Use Case

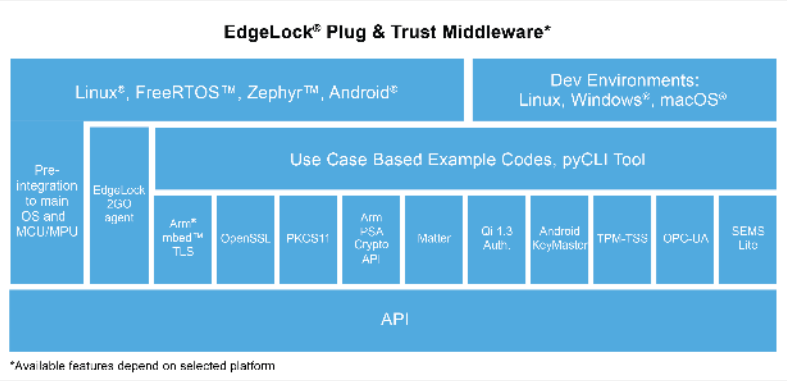
EDGELOCK SE050E AND A5000 LINECARD COMPARED WITH LEGACY SE050C & -A

			A5000	SE050E	SE050F	SE050C2	SE050A2
Authentication Application \ IoT Applet	**ECC Crypto Schemes**	ECDSA	X	X	X	X	X
		ECDH/ECDHE	X	X		X	X
		DH_Mont		X		X	
		ECDAA		X		X	
		EdDSA		X		X	
	Supported Elliptic Curves	NIST (192 to 521 bit)	X (256/384 only)	X	X (>=224 bit)	X	X
		Brainpool (160 to 512 bit)		X	X (>=224 bit)	X	X
		Koblitz (160 to 256 bit)		X	X (>=224 bit)	X	X
		Barreto-Naehrig (256 bit)		X		X	
		Curve25519 [Twisted Edwards/Montgomery]		X		X	
		Montgomery-Curve448		X			
	RSA	RSA			>=2k, no RSA plain, no RSA 4kGen	Up to 4k	
	Symmetric Crypto Algorithm	PRESENT (NXP Proprietary)					
		3DES (2K, 3K)	X	X	X (only 3K)	X	X
		AES (128, 192, 256)	X	X	X	X	X
	AES Modes	CBC, ECB, CTR	X	X	X	X	X
		CCM, GCM	X	X			
	MAC	HMAC, CMAC	X	X	X	X	X
		GMAC	X	X			
	Hash Function	SHA-1, SHA-224 to 512	X -256/384	X	X (No SHA-1)	X	X
	Key Derivation (KDF)	TLS (KDF, PSK)	X	X		X	X
		MIFARE DESFire		X		X	X
		PBKDF2 (Wifi EAP)		X		X	X
		HKDF	X	X	X	X	X
	TPM Functionality			X		X	
	Secure Channel	Secure Channel Host-SE (Platform SCP)	X	X	X (Mandatory)	X	X
	Pre-Provisioned		X	X	X	X	X
HW features	**TRNG**		NIST SP800-90B, AIS31	NIST SP800-90B, AIS31	NIST SP800-90B, AIS31	NIST SP800-90B, AIS31	NIST SP800-90B, AIS31
	DRBG		NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20
	User Memory – Full Feature - NV		8 kB	50 kB	50 kB	50 kB	50 kB
	User Memory – Maximum - NV		8 kB	50 kB	50 kB	50 kB	50 kB
	Interfaces	OWI					
		ISO14443			X	X	
		I^2C Target	X (up to 1 Mbit/s)	X (up to 1 Mbit/s)	X (up to 3.4 Mbit/s)	X (up to 3.4 Mbit/s)	X (up to 3.4 Mbit/s)
		I^2C Controller		X	X	X	
	Temperature range		-40 to +105 °C	-40 to +105 °C	-40 to +105 °C	-40 to +105 °C	-40 to +105 °C
	Package		HX2QFN20	HX2QFN20	HX2QFN20	HX2QFN20	HX2QFN20

EDGELOCK SE050 TO SCALE SECURITY FEATURES OUT OF THE BOX WITH FLEXIBILITY

[WWW.NXP.COM/SE050](WWW.NXP.COM/SE050)

EdgeLock SE050 Plug & Trust middleware



Supported evaluation MCU/MPU boards

K64F

LPC55S69

i.MX RT1060

i.MX RT1170

i.MX 8M

Raspberry Pi

HiKey 960

EdgeLock SE050 Arduino compatible development kit

OM-SE050ARD-E

OM-SE050ARD-F

Demo codes

Documentation

Omni comprehensive host-agnostic support package allow customers to easily implement security features in multiple MCU/MPU without needing secure coding nor credentials injection.
Example SW codes for several use cases: cloud onboarding, TLS, Host- SE binding, TPM functionalities

PLUG&TRUST

EDGELOCK SE050 PROVIDES HIGHLY CERTIFIED AND PROVEN SECURITY – CC & FIPS

CC EAL 6+ including AVA_VAN.5 up to OS level

EdgeLock SE050's security concept IntegralSecurity architecture 3.0 includes **various countermeasures against the most recent attacks scenarios**.

SE050 HW (N7121) and SW (JCOP 4) platform achieved Common Criteria Security Certification with security assurance level **CC EAL 6+** in 2019 from German BSI. EAL 6+ evaluation is performed by an independent security lab and includes:

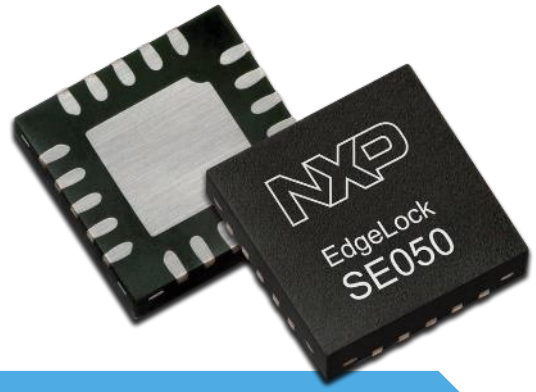
- Intense penetration testing on level AVA_VAN.5 against attacks with high attack potential (AVA_VAN describes the vulnerability assessment, AVA_VAN.5 is the highest level in CC).
- White box vulnerability analysis of HW and SW source code.
- Semi-formal and formal analysis of security, rigorous functional testing.
- Development, life cycle, site audits, secure manufacturing, testing, same as for governmental use.

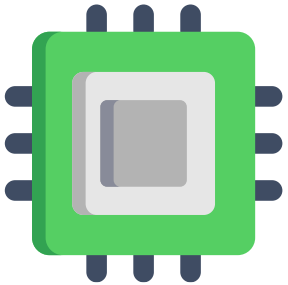
FIPS 140-2 level 3*

https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3840

* FIPS Certified SE050 will require a specific configuration

EDGELOCK SE05x: BEYOND TPM, SECURITY TAILOR-MADE FOR THE IOT





Trusted Platform Module (TPM)

A Trusted Platform Module, or TPM, is a secure crypto-processor for computing devices that provides hardware-based protection of sensitive credentials

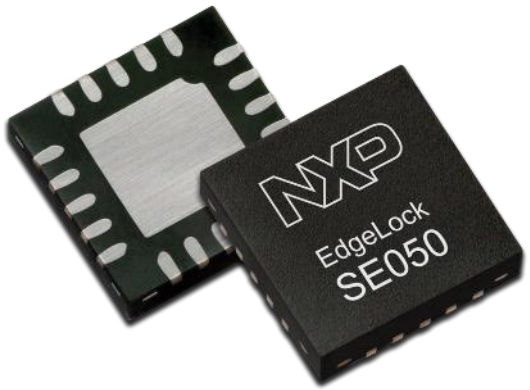
UNCOMPROMISING TPM-LIKE SECURITY…

Certified CC EAL 6+ VAN 5 on HW & SW level and FIPS 140-2 Lv 3 (SE050)

Pre-installed IoT applet offering TPM-like capabilities

- Secure cryptographic processing
- Secure key storage
- Unique ID generation and storage
- Attestation capabilities
- PCRs to remotely verify device health and ensure trust

EDGELOCK SE05x: BEYOND TPM, SECURITY TAILOR-MADE FOR THE IOT



EdgeLock SE05x

EdgeLock SE050, EdgeLock SE051

… TAILOR-MADE FOR THE IOT, GOING BEYOND TPM

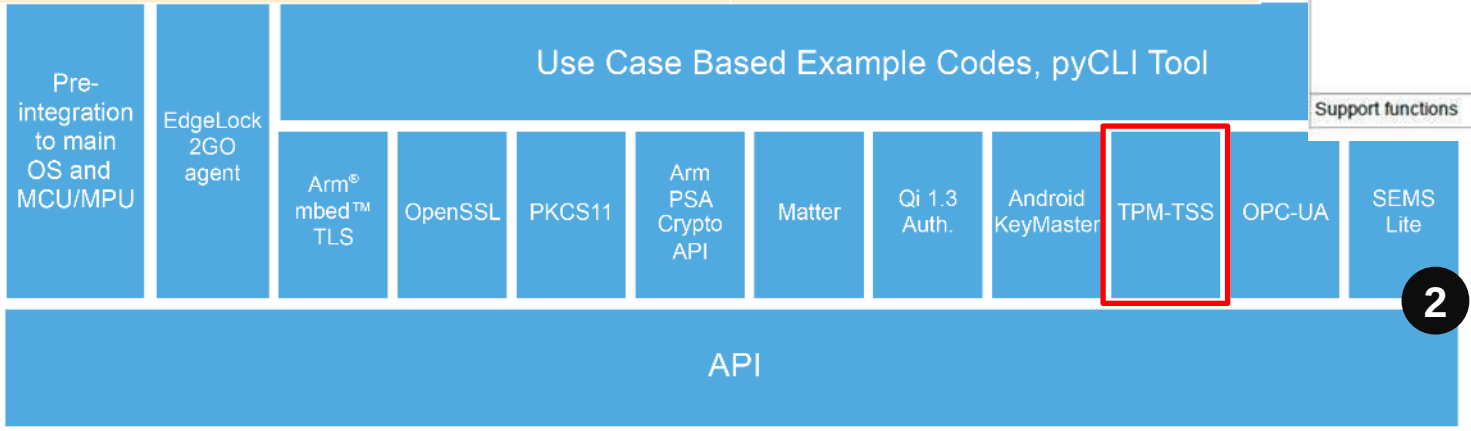
- Flexible management of credentials and access-right policies
- Secure binding to the host controller using GlobalPlatform SCP03
- Pre-integration with connectivity stacks and multi-cloud support
- Multi-tenancy support
- Fast adaptation to current and upcoming standards (FIPS 140-2, ISA/IEC 62443, DLMS-COSEM)
- Lightweight **Plug & Trust middleware** for fast design in and integration

PLUG&TRUST

EDGELOCK SE05x – SUPPORT OF TPM FUNCTIONALITY

1 TPM functionality In EdgeLock SE050

TPM function	Part of SE050
Basic Security Concepts: Secrecy, Shared secret, Integrity, Authentication, Authorization, Anti-replay, Nonrepudiation	Yes
Secure Hash: For hash-extend operations, HMACs, tickets, asymmetric-key digital signatures, and key-derivation functions	Yes
Anonymous attestation DAA	Yes
Hash extend	Yes
HMAC	Yes
KDF to derive both symmetric and asymmetric keys.	Yes
Symmetric Keys	Yes
Asymmetric keys (RSA, ECC etc.)	Yes
Digital signatures	Yes
Public key certification	Yes
PCRs for attested boot	Yes, CRTM Log event totally secured
Reserved handles	Yes
Plaintext password authorization session	Yes
Nonce concept against replay attack	Yes, every authentication item has a random number
Permanent entities in TPM 2.0: 3 persistent hierarchies (Platform, Storage and Endorsement use cases)	As many hierarchies as needed, limited by 50kB memory
Authorizations and Sessions	Yes
Dictionary attack lockout reset	Similar functionalitiy : "Fail authentication retry counter"
The ephemeral hierarchy or the NULL hierarchy	Similar functionality: "Transient keys"
SPI interface	No, encrypted I2C instead



*Available features depend on selected platform

AN12663

EdgeLock™ SE05x to implement TPM-like functionality

Rev. 1.0 — 7 December 2020 Application note

Table 1. TPM Functions supported by Plug & Trust middleware

Function	TPM APIs	Supported Algorithms
Asymmetric Signing and Verification	Esys_VerifySignature () Esys_Sign ()	RSA-SSA (TPM2_ALG_RSASSA) RSA-PSS (TPM2_ALG_RSAPSS) RSA-ECDSA (TPM2_ALG_ECDSA)
Asymmetric RSA Encryption and Decryption	Esys_RSA_Encrypt () Esys_RSA_Decrypt ()	RSA-OAEP (TPM2_ALG_OAEP) RSA (TPM2_ALG_RSAES)
AES Encryption & Decryption	Esys_EncryptDecrypt () Esys_EncryptDecrypt2 ()	AES-CTR (TPM2_ALG_CTR) AES-CBC (TPM2_ALG_CBC) AES-ECB (TPM2_ALG_ECB)
Hashing	Esys_Hash ()	SHA1 (TPM2_ALG_SHA1) SHA256 (TPM2_ALG_SHA256) SHA384 (TPM2_ALG_SHA384) SHA512 (TPM2_ALG_SHA512)
HMAC	Esys_HMAC ()	SHA1 (TPM2_ALG_SHA1) SHA256 (TPM2_ALG_SHA256) SHA384 (TPM2_ALG_SHA384) SHA512 (TPM2_ALG_SHA512)

Table 1. TPM Functions supported by Plug & Trust middleware...*continued*

Function	TPM APIs	Supported Algorithms
Random number generation	Esys_GetRandom ()	-
PCR	Esys_PCR_Extend () Esys_PCR_Event () Esys_PCR_Read () Esys_PCR_Allocate () Esys_PCR_Reset ()	-
Support functions	Esys_ReadPublic ()	-

3 Appnote including list of APIs in TSS Abstraction layer

2 TSS abstraction layer in EdgeLock SE05x Plug & Trust Middleware

EDGELOCK 2GO READY CONFIGURATION

	Pre-injected Root of Trust*	Applet Updatability
SE050E	• Four ECC NIST P-256 key pairs and X.509 certificates • One ECC NIST P-256 and attestation** key pair and certificates	
SE050F	• Four ECC NIST P-256 key pairs and X.509 certificates • Two RSA 2048-bit key pairs and X.509 certificates • One ECC NIST P-256 and one RSA 2048 attestation** key pair and certificates • Two RSA 4096 key pairs	

*certificates are signed by NXP Root CA, keys are device individual.
For more details, please refer to the specific Configuration Data Sheet.

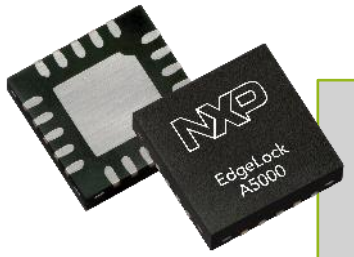
** Attestation keys have the “read with attestation” policy. For more details refer to the APDU spec

EdgeLock A5000

Secure Authenticator
Mass Market Ready

SECURE CONNECTIONS
FOR A SMARTER WORLD

EDGELOCK A5000 – NEW CERTIFIED SECURE AUTHENTICATOR



CERTIFIED SECURE AUTHENTICATOR

mass market

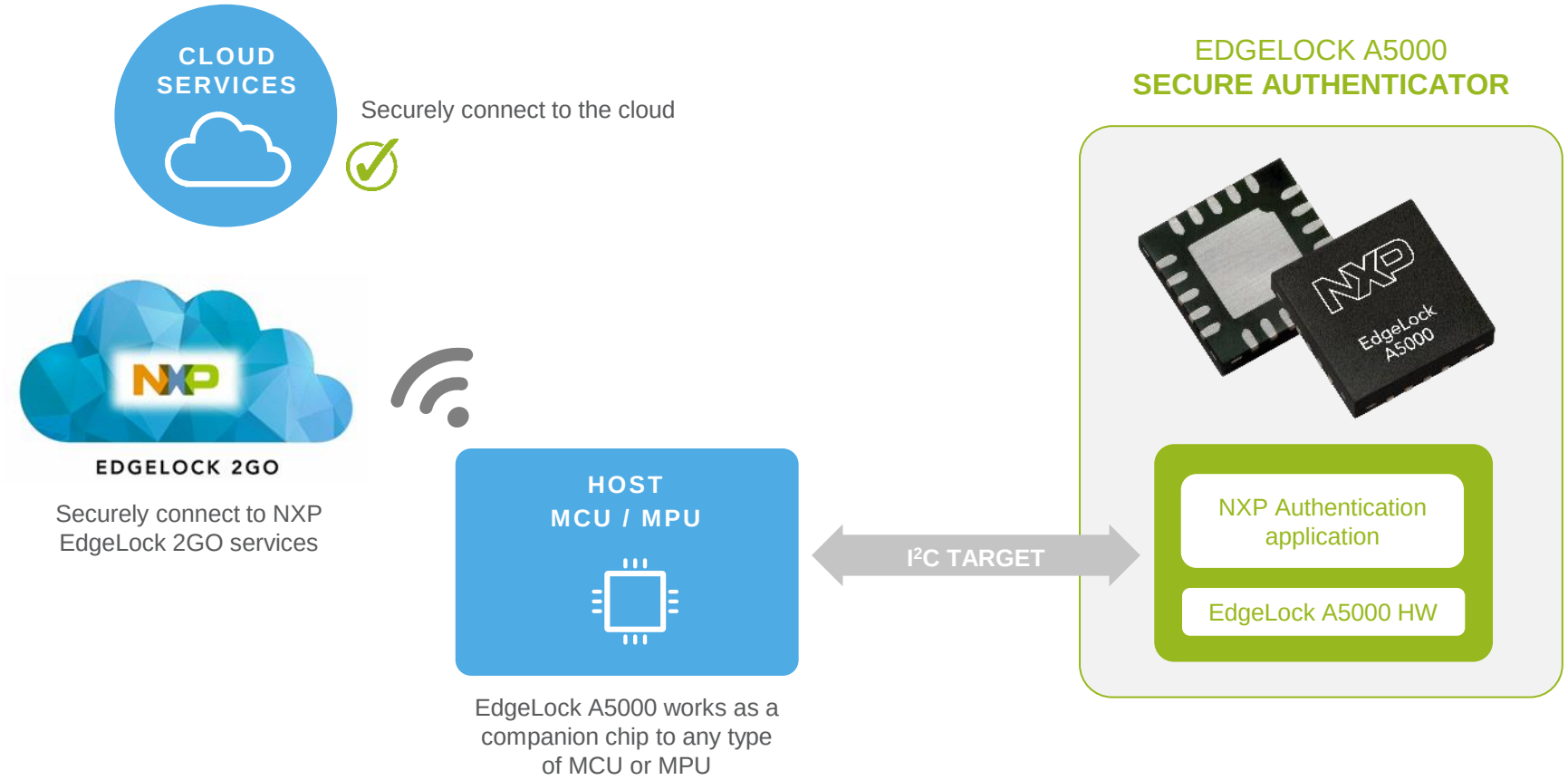
A5000

- New Certified Authenticator
- Dedicated Authentication Application
- CC EAL 6+ AVA_VAN.5
- ECC NIST P256/384 curves supported
- Mono Use Cases
  - Anticounterfeit
  - Cloud Onboarding
  - DLMS-COSEM
  - Qi 1.3 Authentication
- I^2C Target
- 8kB user memory
- Extended temperature range (-40 to +105 °C)
- Small and very thin HXQFN20 package particularly suited for space limited applications (3 mm x 3 mm x 0.33 mm)

Part Number	A5000
Package	HX2QFN20
Launch Date	March 2022

PLUG&TRUST

A TRUSTED HARDWARE THAT CAN BE ADDED TO ANY IOT ARCHITECTURE FOR SECURITY



KEY BENEFITS OF ADDING EDGELOCK A5000 SECURE AUTHENTICATOR

PROTECT

State of the art security for your credentials and secure vault

EdgeLock A5000 enables the use of the credentials for authentication use cases, store device credentials calibration and configuration data, device revocation lists

MANAGE

Credential management for both offline and online system

Renewed secret key generation on chip with attestation of keys

Key & Digital certificate management through NXP EdgeLock 2GO service

READY TO GO

Securely pre-injected for anticounterfeit, originality check and onboarding

Leverage certified NXP Trust Provisioning PKI for pre-provisioned credentials on A5000.

No need to establish PKI system for customers

DIFFERENTIATE

With higher, certified security

Differentiate your product with certified security, and secure access to your devices as OEM

EDGELOCK A5000 SUPPORTS KEY AUTHENTICATION USE CASES MAKING IT SUITABLE FOR ONE OF THE FOLLOWING APPLICATIONS

SECURE CLOUD ONBOARDING

DEVICE-TO-DEVICE AUTHENTICATION

ATTESTATION & PROOF OF DEVICE ORIGIN

QI 1.3 WIRELESS CHARGING AUTHENTICATION

Enabling IoT Authentication Applications

SMART METERS
ENERGY MANAGEMENT
EV CHARGERS

SMART APPLIANCES
MATTER
HOME SMOKE DETECTORS
OTHER ELECTRONIC ACCESSORIES

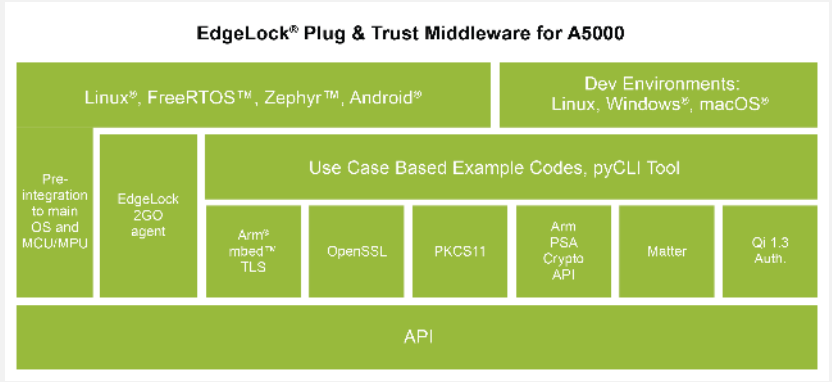
MOBILE ACCESSORIES
CHARGERS
WEARABLE
COMPUTING

PLUG&TRUST

EDGELOCK A5000 PLUG & TRUST PRODUCT SUPPORT PACKAGE

[WWW.NXP.COM/A5000](WWW.NXP.COM/A5000)

EdgeLock SA Plug & Trust Middleware



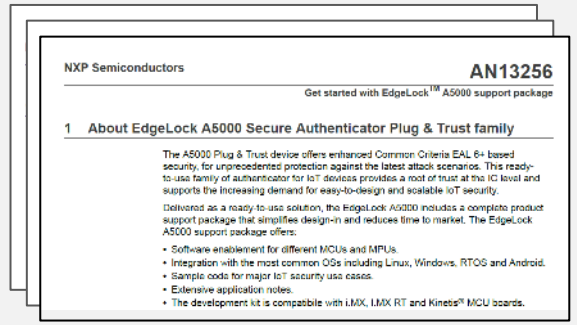
Supported evaluation MCU/MPU boards

A5000 Arduino compatible development kit

- K64F
- LPC55S69
- i.MX RT1060
- i.MX RT1170
- i.MX 8M
- Raspberry Pi

Demo codes

Documentation



EDGELOCK 2GO READY CONFIGURATION

	Pre-injected Root of Trust*	Applet Updatability
A5000	• Two ECC NIST P-256 key pairs & X.509 certificates	

*certificates are signed by NXP Root CA, keys are device individual.
For more details, please refer to the specific Configuration Data Sheet.

EDGELOCK A5000 – DETAILS

			A5000
Authentication Application	ECC Crypto Schemes	ECDSA	X
		ECDH/ECDHE	X
		DH_Mont	
		ECDAA	
		EdDSA	
	Supported Elliptic Curves	Binary 163bit	
		NIST (192 to 521 bit)	X (256/384 only)
		Brainpool (160 to 512 bit)	
		Koblitz (160 to 256 bit)	
		Barreto-Naehrig (256 bit)	
		Curve25519 [Twisted Edwards/Montgomery]	
		Montgomery-Curve448	
	RSA	RSA	
	Symmetric Crypto Algorithm	PRESENT (NXP Proprietary)	
		3DES (2K, 3K)	X
		AES (128, 192, 256)	X
	AES Modes	CBC, ECB, CTR	X
		CCM, GCM	X
	MAC	HMAC, CMAC	X
		GMAC	X
	Hash Function	SHA-1, SHA-224 to 512	X -256/384
	Key Derivation (KDF)	TLS (KDF, PSK)	X
		MIFARE DESFire	
		PBKDF2 (Wifi EAP)	
		HKDF	X
	TPM functionality		
	Secure Channel	Secure Channel Host-SE (Platform SCP)	X
	Pre-Provisioned		X
HW features	TRNG		NIST SP800-90B, AIS31
	DRBG		NIST SP800-90A, AIS20
	User Memory – Full Feature - NV		8 kB
	User Memory – Maximum - NV		8 kB
	Interfaces	OWI	
		ISO14443	
		I^2C Target	X (up to 1 Mbit/s)
		I^2C Controller	
	Temperature Range		-40 to +105 °C
	Package		HX2QFN20

EdgeLock SE051

non-mass market

Updatable Secure Element application specific markets

SECURE CONNECTIONS FOR A SMARTER WORLD

EDGELOCK SECURE ELEMENT AND SECURE AUTHENTICATOR PORTFOLIO

FIT-TO-PURPOSE CERTIFIED AUTHENTICATOR

mass market

A5000

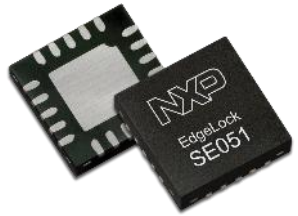
FIT-TO-PURPOSE SECURE AUTHENTICATOR

- Simple authentication use case with event counters
- Device calibration & configuration data
- Dynamic key management

ALLROUND MULTI USE CASE SE

mass market

SE050E/F



UPDATABILITY

non-mass market

SE051

ALL ROUND SECURE ELEMENT – FLEXIBLE SOLUTIONS FOR MULTIPLE USE CASES

- Rich crypto set & agility (incl. RSA, MIFARE, Future proof Crypto Curves)
- Large dynamic File system (50 kB) and API for multi-use cases support
- Secure sensing & actuation interface
- TPM functionalities
- Updateable offline (SE051x)

EDGELOCK SE051 FURTHER ENHANCING THE UNIQUE VALUE OF SE050

SECURITY MAINTENANCE

- SEMS Lite for convenient applet update/maintenance of EdgeLock SE051

EFFICIENCY AND FLEXIBILITY

- Multi cast (one-to-many) updates instead of point-to-point updates
- No need for own TSM (Trusted Service Manager) infrastructure
- Covering online and offline update scenarios

BEST PRACTICE

- Applet updatability is a well-established feature in other secure NXP products
- It is based on the Global Platform industry standard SEMS and is used to securely update mobile secure elements since years

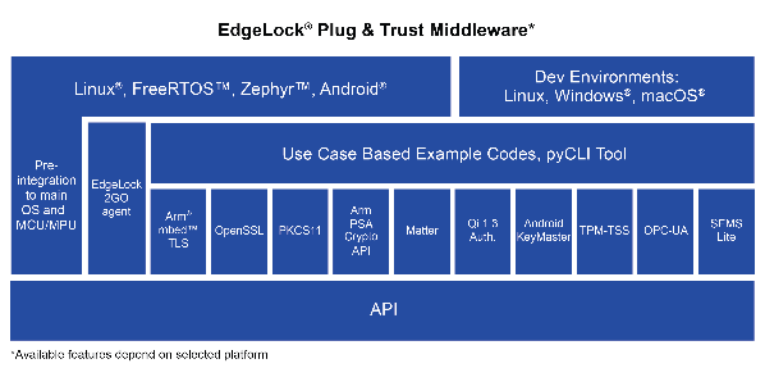
FULL SOLUTION OFFERING

- Update Manager, SEMS Lite Agent, SEMS Lite Applet
- Update distribution through EdgeLock 2GO

EDGELOCK SE051 PLUG & TRUST PRODUCT SUPPORT PACKAGE

[WWW.NXP.COM/SE051](WWW.NXP.COM/SE051)

EdgeLock Plug & Trust middleware



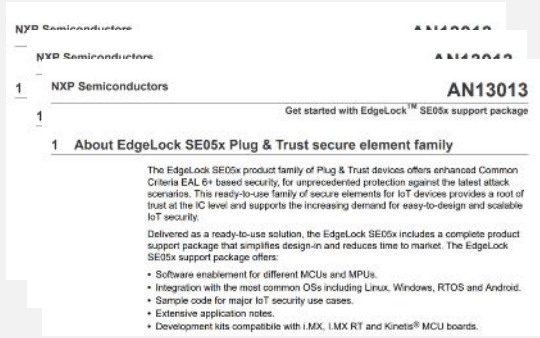
Supported evaluation MCU/MPU boards

EdgeLock SE051 Arduino compatible development kit

- K64F
- LPC55S69
- i.MX RT1060
- i.MX RT1170
- i.MX 8M
- Raspberry Pi
- HiKey 960

Demo codes

Documentation



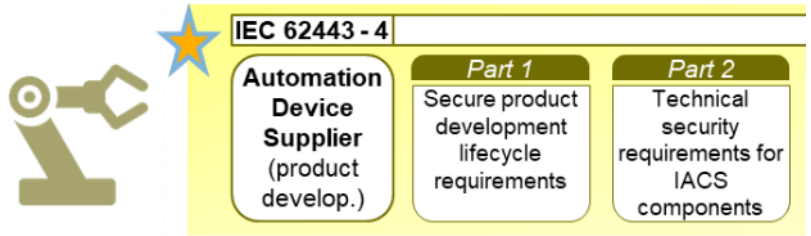
EDGELOCK 2GO READY CONFIGURATION

	Pre-injected Root of Trust*	Applet Updatability
SE051A	• Two ECC NIST P-256 key pairs & X.509 certificates	SEMS Lite for Applet updates Perso Applet for platform config
SE051C	• Four ECC NIST P-256 key pairs and X.509 certificates • Two RSA 2048-bit key pairs and X.509 certificates • One ECC NIST P-256 and one RSA 2048 attestation** key pair and certificates • Two RSA 4096 key pairs	SEMS Lite for Applet updates Perso Applet for platform config

*certificates are signed by NXP Root CA, keys are device individual.
For more details, please refer to the specific Configuration Data Sheet.

** Attestation keys have the “read with attestation” policy. For more details refer to the APDU spec

IEC 62443-4-1 /-2 CERTIFICATION



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. IITS2 003346 0003 Rev. 00

Holder of Certificate: **NXP Semiconductors Germany GmbH**
Business Line Connectivity & Security
Troplowitzstrasse 20
22529 Hamburg
GERMANY

Site(s): NXP Semiconductors Germany GmbH
Business Line Connectivity & Security
Troplowitzstrasse 20, 22529 Hamburg, GERMANY

Certification Mark:

Product Type: Industrial IT Security

Model(s): **SE051**

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003A:2018 (IEC 62443-4-1: Full Product Profile)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 21CR03S002
Valid until: 2024-01-31

Date, 2021-03-26 (Enrico Seidel)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

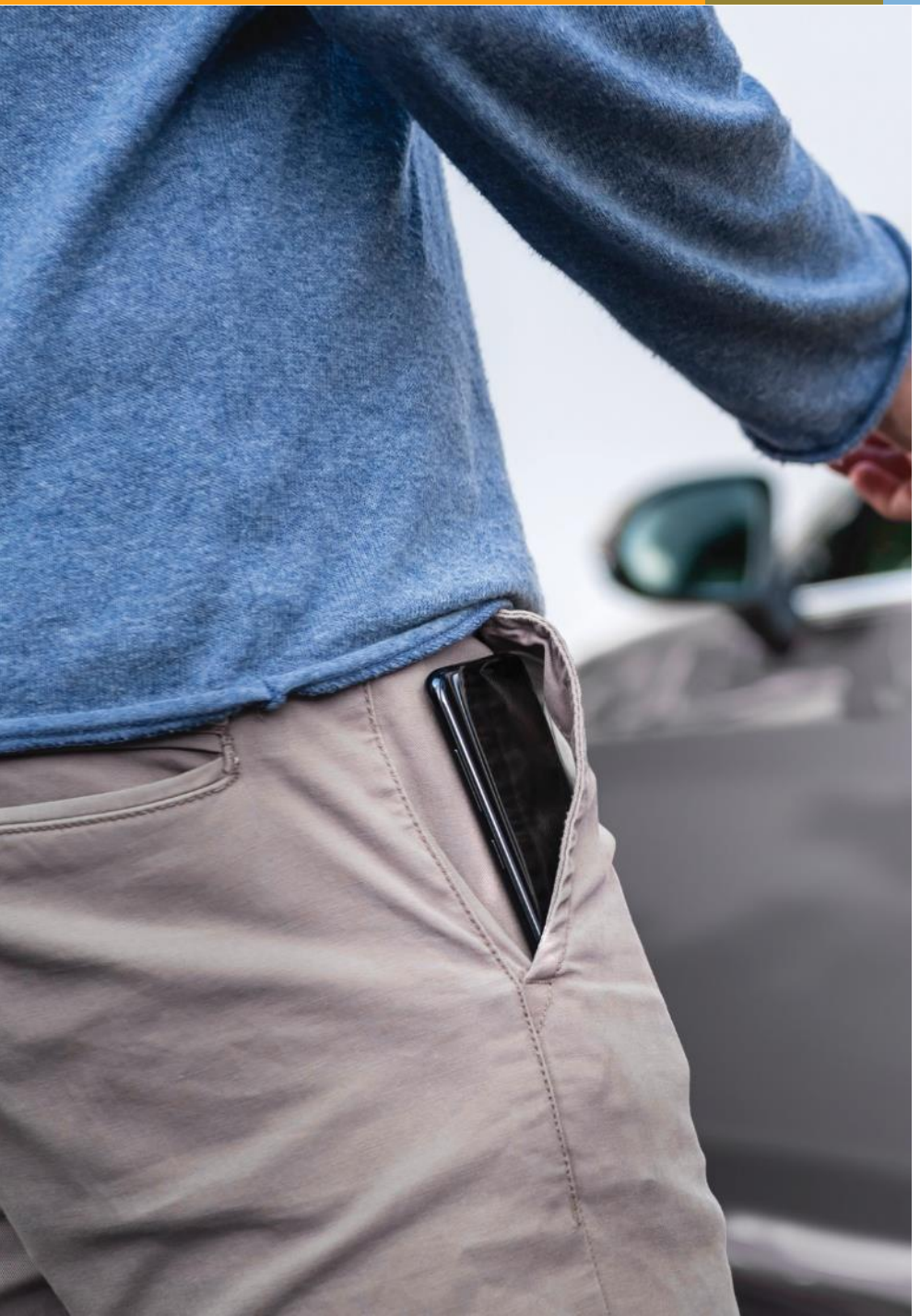
TÜV®

EdgeLock SE051W

non-mass market

Secure Element for UWB
application specific / selected markets

SECURE CONNECTIONS
FOR A SMARTER WORLD



ULTRA WIDEBAND ENABLING TRULY HANDSFREE USE CASES

- Accurate hands-free access control, both logical and physical
- Indoor localization for Smart Industries
- Highly secure

SE051W PROVIDES SECURITY TO ULTRA-WIDEBAND USE CASES

How to ensure only valid users get access via UWB?

What?

EdgeLock SE051 IoT Security use cases enhanced by secure UWB ranging for access and localization applications

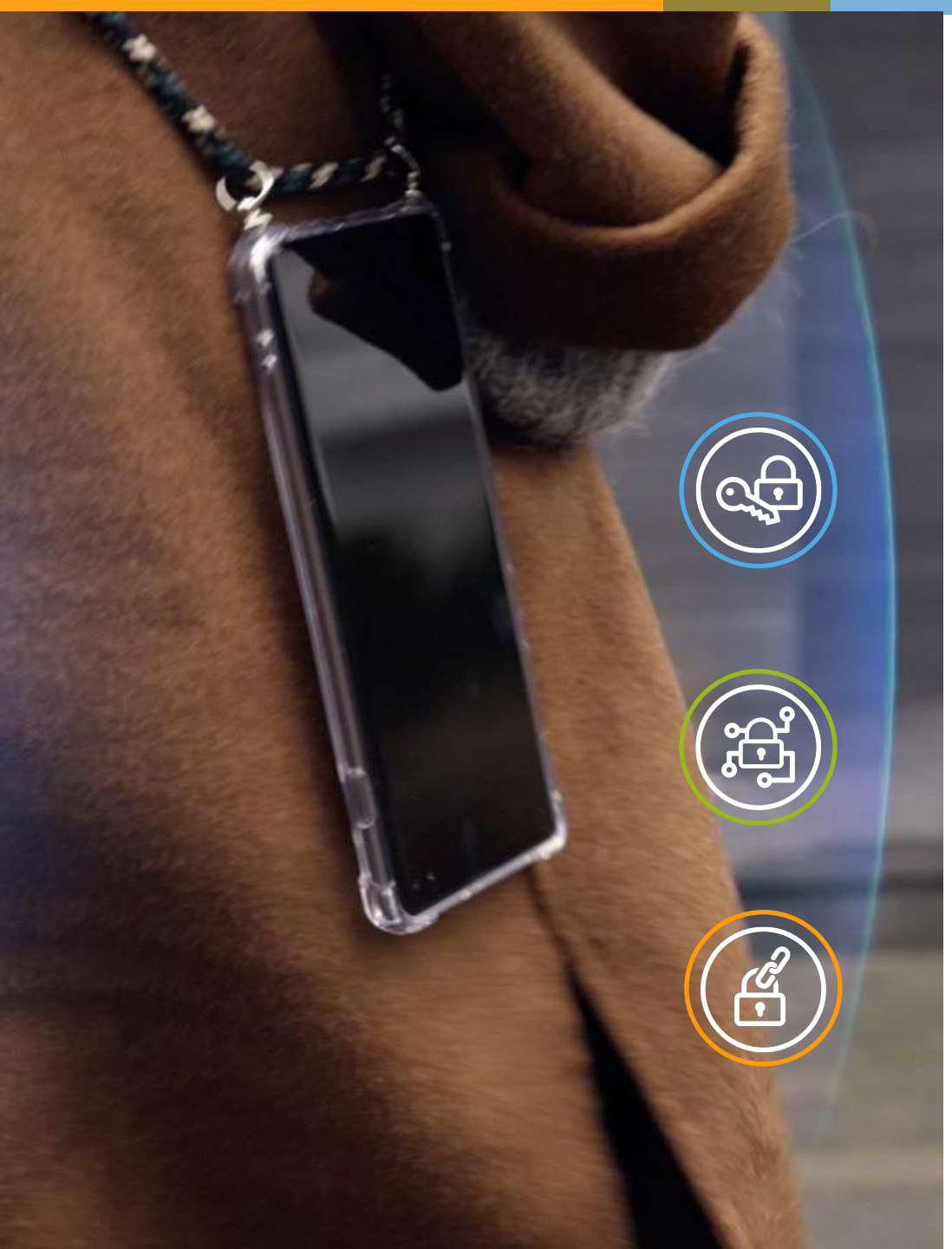
- Pre-integration with SR150 UWB chip
- Enabling secure dynamic ranging
- One solution for multiple use cases that can scale across platforms
- FIRA Compliance

Why?

- Certain UWB use cases like access control require security to ensure only valid users get access (physical & logical access)
- Secure ranging root key as well as access control keys must be protected

How?

- Secure binding between SR150 and SE051W right from the beginning
- SE051W stores the root key, uses it to establish the secure channel with SR150 and supports dynamic STS (Scrambled Time Stamp)
- pre-loaded applets for multiple IoT & secure ranging use cases
- Plug & Trust MW for ease of use



RADIO RANGING & ATTACK SCENARIOS

- Relay attacks are a serious threat to hands-free transactions
- UWB is resistant to relay attacks, SE051W protects on top against replay attacks

PROTECTION AGAINST RELAY ATTACKS	Time-of-flight measurement
PROTECTION AGAINST REPLAY ATTACKS	Scrambled Timestamp Sequence changing with every packet
MOBILE / IOT DEVICE AUTHENTICATION	Session key agreement with each device for each access, Extra PHY layer security in IEEE 802.15.4z

ALIBABA

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP EDGELOCK AUTHENTICATORS FOR ALIBABA: OVERVIEW

A5000 	A71CL 
FOR DOMESTIC AND OVERSEAS MARKETS	**FOR DOMESTIC CHINA MARKET**
SUPPORTS: ALIBABA, MICROSOFT AZURE, AWS, GOOGLE CLOUD PLATFORM, IBM WATSON)	**SUPPORTS:** ALIBABA CLOUD SERVICES
Common Criteria certified EAL 6+	ICA Level 1 certified
NXP IoT API	ID^2 API
I^2C interface – 1 Mbit/s	I^2C interface – 400 Kbit/s
Package: HX2QFN20 (3x3mm)	Package: HVSON-8 (4x4mm)
ECC NIST 256/384 bits and AES 128/256 bits cryptography	RSA & 3DES cryptography
NXP EdgeLock 2GO Key Management service support	-
Available Q1 2022	Available
Ordering via NXP and its distribution partners	Ordering via Alibaba

Contact information: Steven.zhu@nxp.com

SECURE CONNECTIONS
FOR A SMARTER WORLD