EDGELOCK™ SE051 - PROVEN, EASY-TO-USE IOT SECURITY SOLUTION WITH SUPPORT FOR UPDATABILITY AND CUSTOM APPLETS

Webinar Instructions

- Length of the session: around **30 minutes**
- For **questions:** write them in the **NXP Community for Secure Authentication**
- Please complete the **short evaluation survey** after closing the session
- You will receive a **link** to the recorded session and the presentation

Jordi Jofre
Speaker

Application engineer

jordi.jofre@themobileknowledge.com ✉

www.linkedin.com/in/jordijofre/

EdgeLock™ SE051

Proven, easy-to-use IoT security solution with support for updatability and custom applets

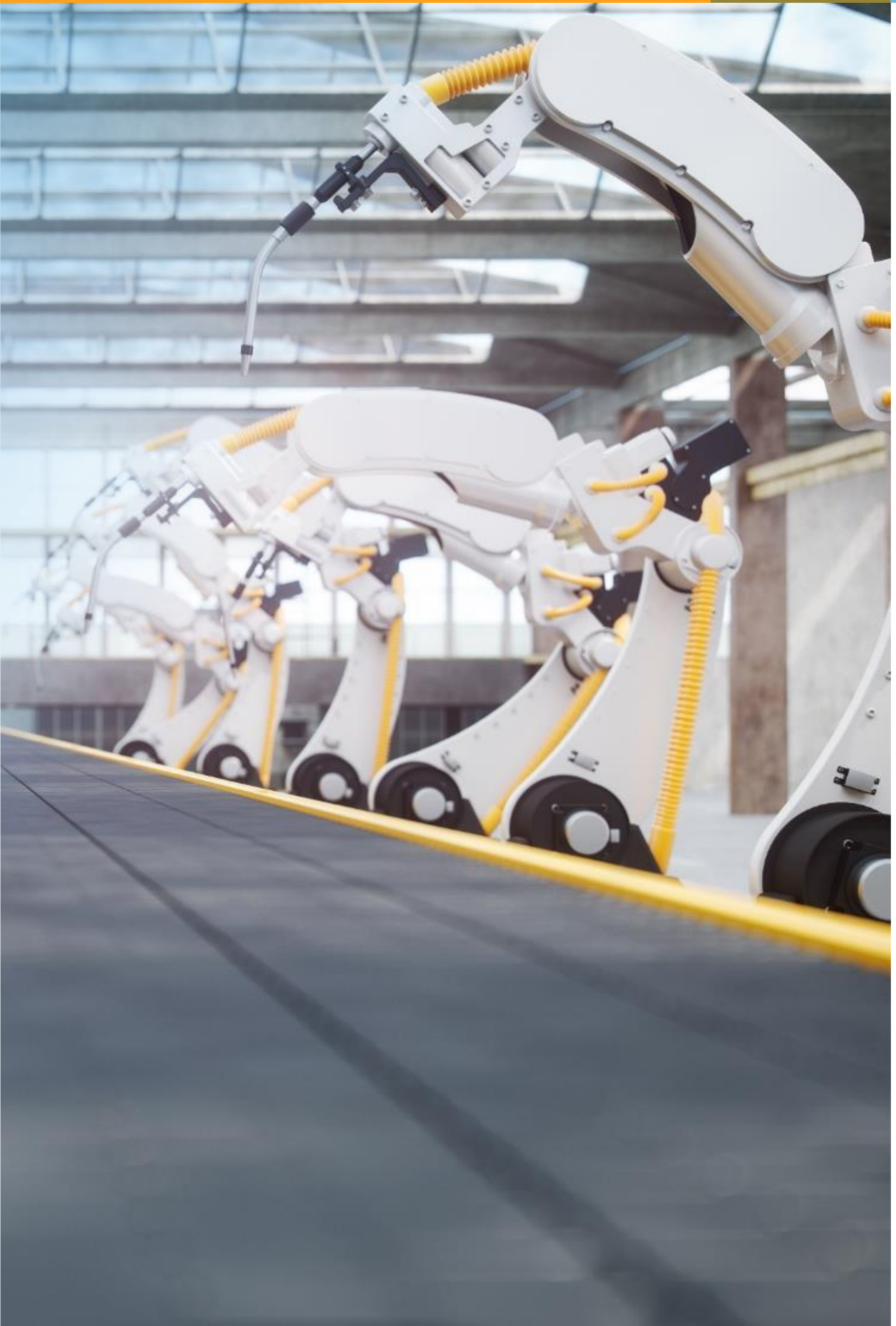
PLUG &TRUST

DECEMBER 2020

SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.



AGENDA

- EdgeLock SE05x secure element family
- EdgeLock SE051 product overview
- EdgeLock SE05x product decision tree
- SEMS Lite for IoT applet updatability
- SEMS Lite for custom applet development
- Support package

PLUG &TRUST

EdgeLock SE05x secure element family

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.

EDGELOCK SE05X SECURE ELEMENT FAMILY
ENHANCED SECURITY WITH MAXIMUM FLEXIBILITY AND FAST DESIGN-IN

- **Root of trust at the IC level**
- **Out-of-the-box solution**

Proven security

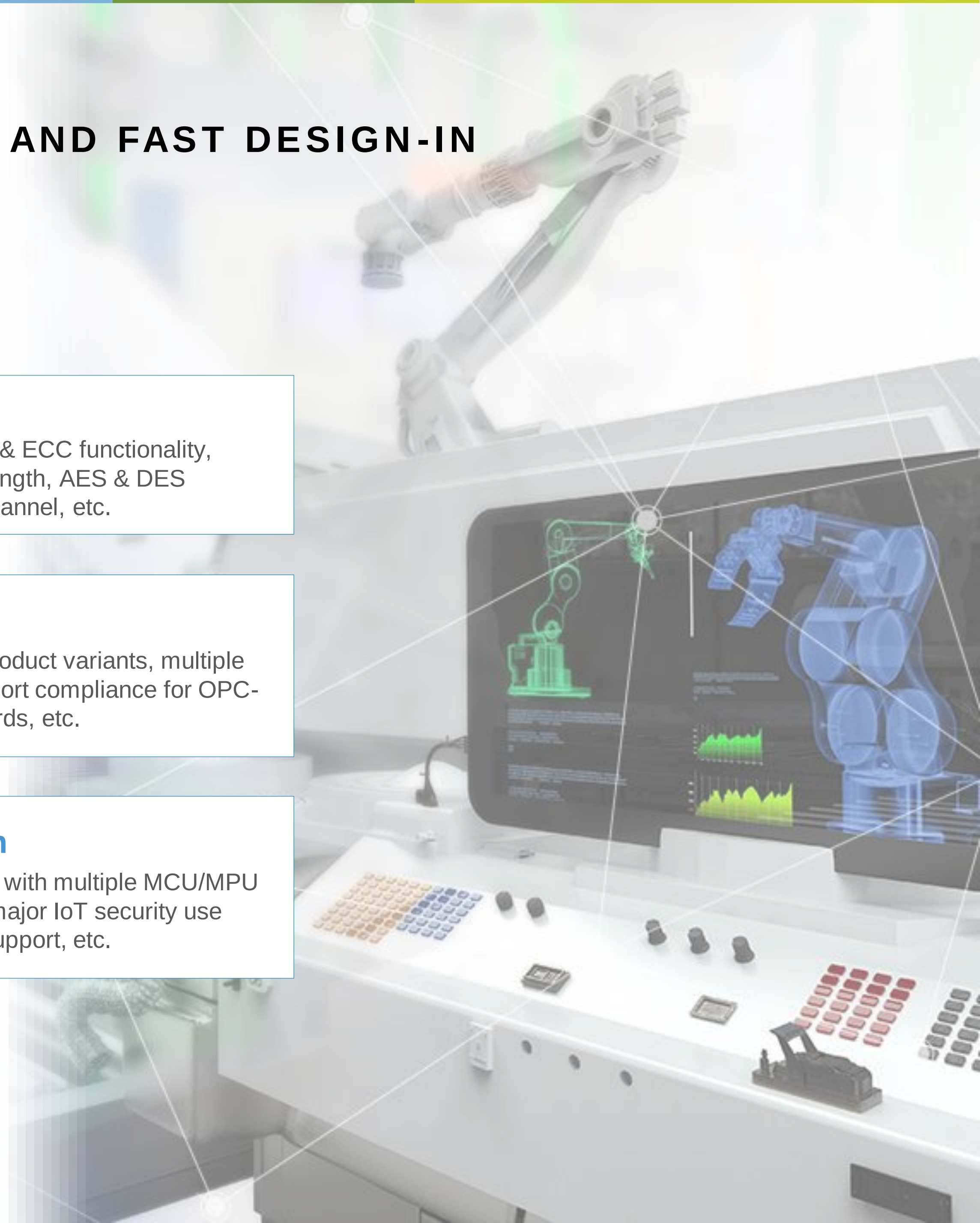
CC EAL6+ based HW & OS, RSA & ECC functionality, future proof curves & higher key length, AES & DES symmetric ciphers, SCP secure channel, etc.

Flexibility

Dynamic user memory, multiple product variants, multiple interfaces, TPM functionality, support compliance for OPC-UA and IEC62443 security standards, etc.

PLUG &TRUST fast design-in

Plug & Trust MW, easy integration with multiple MCU/MPU platforms & OS, sample code for major IoT security use cases, secure cloud onboarding support, etc.



IOT APPLICATIONS AND USE CASES

- Secure Cloud Onboarding
- Device-to-device authentication
- Attestation & Proof of device origin
- Sensor data protection
- Late-stage parameter configuration
- Wi-Fi credential protection
- Secure Access Module
- Device ID for Blockchain
- Trusted platform module

For more information on use cases visit **>> IoT Security**

Industrial PLCs, robots, sensors, IP cameras, Smart meters, energy management, Gateways, routers, EV chargers, Access smart locks, Consumer devices, speakers, Smart appliances, Medical and many more…

EDGELOCK SE PORTFOLIO – EXTENSION OF SE05x PLUG & TRUST PLATFORM

GAME CHANGER IOT SECURITY

mass market

SE050 A/B/C

- Pre-installed IoT Applet
- RSA & ECC in one chip
- Future proof curves
- Attestation
- 50kB user memory
- Multi Cloud support
- Many new SE use cases
- CC EAL6+

UPDATABILITY

non-mass market

SE051 A/C

- Pre-installed IoT Applet
- SEMS Lite: Future proof security due to IoT applet updatability
- New features on top of existing SE050 features (e.g. GMAC, AES GCM, Curve448)
- 46kB user memory + Perso options

APPLET DEVELOPMENT

non-mass market

SE051 P

- No IoT applet pre-installed
- Possibility for own applet development
- Optimized OS for IoT Security
- SEMS Lite for convenient applet loading & updatability
- Up to 140kB user memory

EDGELOCK 2GO
A SET OF SERVICES FOR MANAGING THE CREDENTIALS ON YOUR DEVICES

www.nxp.com/edgelock2go

Ready

- EdgeLock SE050 pre-provisioned with default keys and certificates
  - ECC keys on SE05xA
  - RSA keys on SE05xB
  - ECC & RSA keys on SE05xC
- Device certificates are available for download

Custom

- Supports custom complex keys and certificates configurations in SE05x.
- Device certificates are available for download
- Different T&C and MOQ available for every project size.
- Custom provisioning through NXP distributors and third-party partners (SE050 only).

Managed

- NXP cloud service for managing device identities over-the-air
- Add, update and revoke keys and certificates during the device life-cycle
- Overproduction control
- Zero-touch onboarding of devices into the cloud

Note: Contact NXP for checking availability of services and conditions

EDGELOCK 2GO SE05X READY
EASE-OF-USE CONFIGURATION

EdgeLock SE05x variants come pre-provisioned with keys which can be used for all major use cases not requiring customer specific credentials.

EdgeLock SE050

SE050A

One device-individual ECC NIST P-256 key pair and X.509 certificate signed by NXP Root CA

SE050B

One device-individual RSA 2048-bit key pair and X.509 certificate signed by NXP Root CA

SE050C

- Two device-individual ECC NIST P-256 key pairs and X.509 certificates signed by NXP Root CA
- Two device-individual RSA 2048-bit key pairs and X.509 certificates signed by NXP Root CA
- One device-unique ECC NIST P-256 and one device-unique RSA-2048-bit Attestation key pair and certificates
- Two device-unique RSA 4096-bit key pairs

EdgeLock SE051

SE051A

One device-individual ECC NIST P-256 key pair and X.509 certificate signed by NXP Root CA

SE051C

- Two device-individual ECC NIST P-256 key pairs and X.509 certificates signed by NXP Root CA
- Two device-individual RSA 2048-bit key pairs and X.509 certificates signed by NXP Root CA
- One device-unique ECC NIST P-256 and one device-unique RSA-2048-bit Attestation key pair and certificates
- Two device-unique RSA 4096-bit key pairs

KEY RESOURCES ON EDGELOCK SE050 / SE051

EdgeLock SE050

The fast, easy way to deploy secure IoT connections

Web presence

- Product Page EdgeLock SE050 including documentation, app notes, MW, video tutorials, etc.
- Dev Kit Page EdgeLock SE050 including app notes, etc.
- Product Page EdgeLock SE051 including documentation, app notes, MW, video tutorials, etc.
- Dev Kit Page EdgeLock SE051 including app notes, etc.

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

NEW

PLUG&TRUST

EdgeLock SE051 product overview

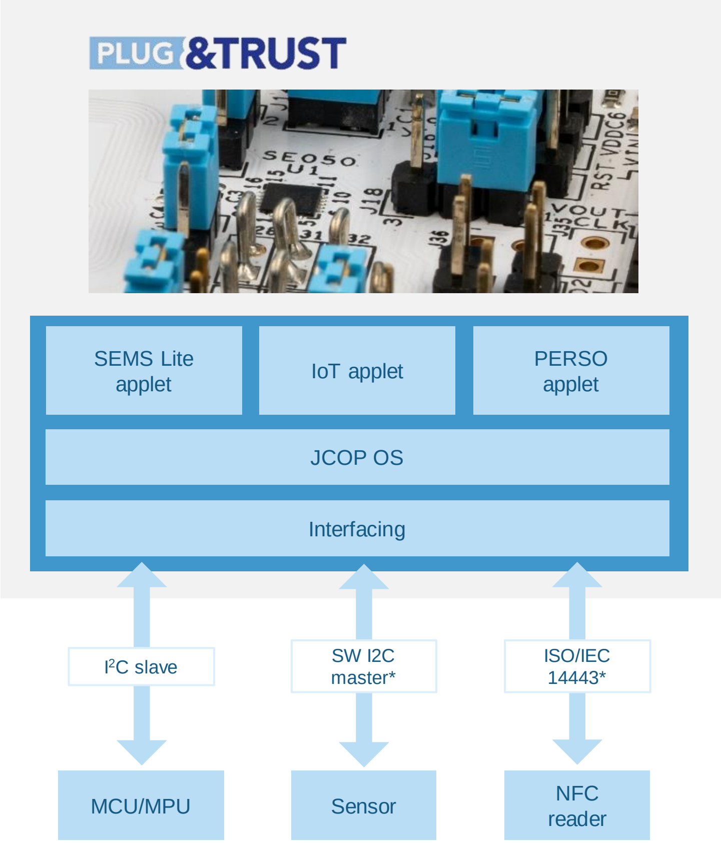
A family extension to **EdgeLock SE050**

SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.

EDGELOCK SE051- FUNCTIONAL VIEW



* *Optional I^2C master and ISO/IEC14443 interfaces to support new IoT security use cases.*

The EdgeLock SE051 is an updatable extension of the EdgeLock SE050, which delivers proven security certified to **CC EAL 6+,** with **AVA_VAN.5** up to the OS level.

IoT applet

Designed for the latest IoT security requirements, allows for securely storing and provisioning credentials and performing cryptographic operations and gives edge-to-cloud security capability right out of the box

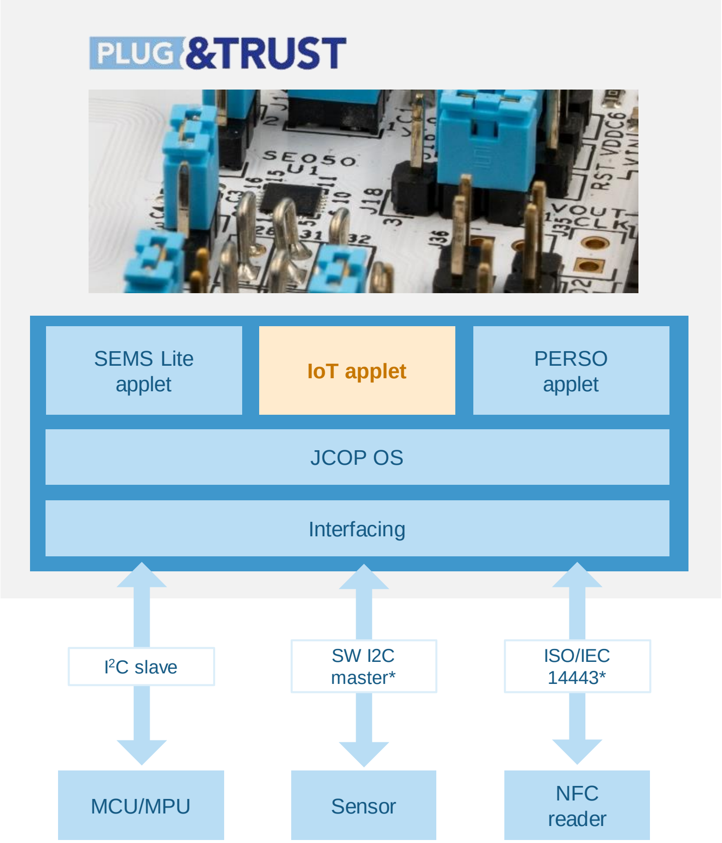
SEMS Lite applet

Provides upgrade functionality of the IoT applet while preserving on device credentials. Can be used for security maintenance or functionality upgrade in the field and to upload additional applets (SE051P).

PERSO applet

Provides the possibility to reconfigure SE051 devices. The configuration options include communication parameter settings of I2C, ISO14443 and ISO7816 interface as well as the deletion of unused operating system (cryptography) modules to gain additional memory.

EDGELOCK SE051- IOT APPLET FEATURES



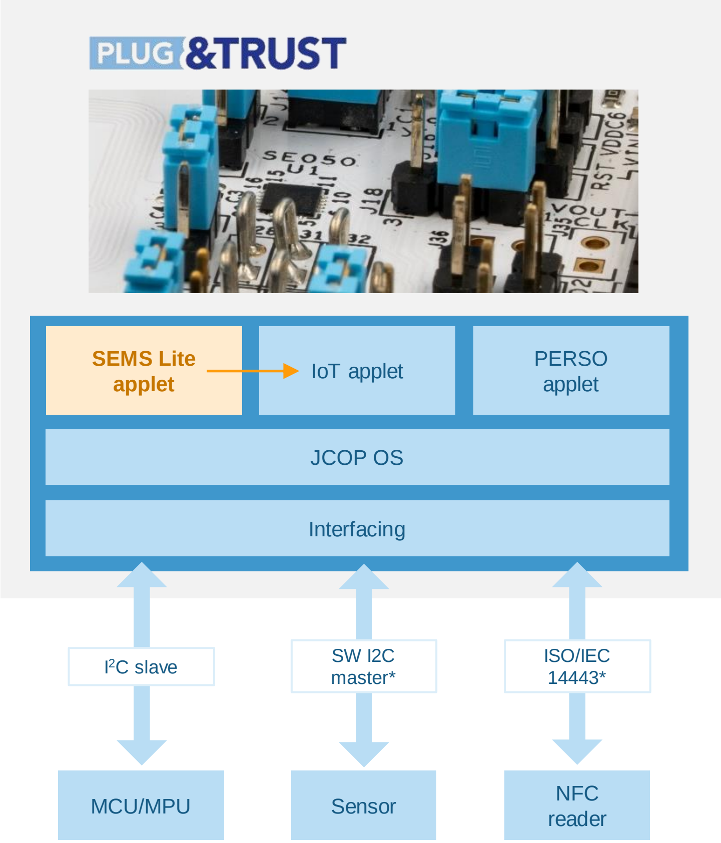
** Optional I²C master and ISO/IEC14443 interfaces to support new IoT security use cases.*

IoT applet

Designed for the latest IoT security requirements, allows for securely storing and provisioning credentials and performing cryptographic operations and gives edge-to-cloud security capability right out of the box.

- **Crypto primitives and functions**
  - RSA, ECC, AES, DES, AES CCM/GCM
  - ECDSA, ECDHE, DH_Mont, ECDAA, EdDSA
  - HMAC, CMAC, GMAC, SHA-1, SHA-224/256/384/512 operations
- **Platform encryption**
  - Applet Secure Channel management (AESKey, EC Key)
- **Lifecycle management**
  - Session management, Timer functionality, Access control, Secure import/export of keys or files.
- **Credential storage**
  - Symmetric key (AES, DES), ECC key, RSA key, HMAC key, Binary file, User ID, Counter, Hash-Extend register
- **Monotonic counters**
  - Monotonic counter creation and management
- **Object & user-based access control**
  - Access-control policies with authentication options based on: User-ID, symmetric key, asymmetric key based authentication
- **Application support**
  - HKDF, MIFARE KDF, PBKDF2 (WiFi EAP), TLS (KDF, PSK), PCRs, Secure sensor readout.

EDGELOCK SE051- SEMS LITE APPLET
FURTHER ENHANCING THE UNIQUE VALUE OF SE050



PLUG &TRUST

SEMS Lite applet → IoT applet

PERSO applet

JCOP OS

Interfacing

I²C slave ↔ MCU/MPU

SW I2C master* ↔ Sensor

ISO/IEC 14443* ↔ NFC reader

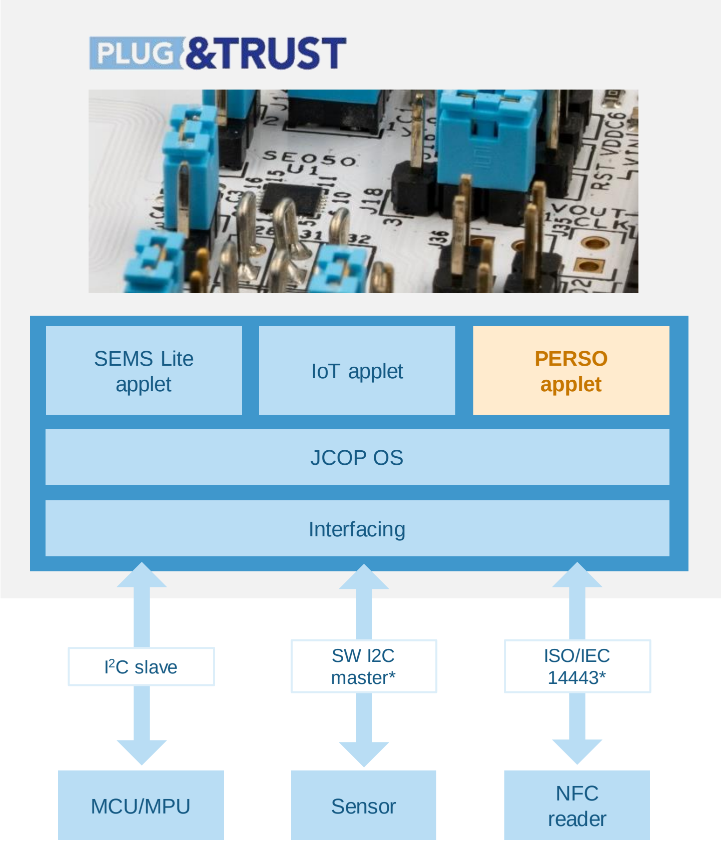
*Optional I²C master and ISO/IEC14443 interfaces to support new IoT security use cases.

SEMS Lite applet

Provides upgrade functionality of the IoT applet while preserving on device credentials. Can be used for security maintenance or functionality upgrade in the field and to upload additional applets (SE051P).

- **Security maintenance**
  - SEMS Lite for convenient applet update/maintenance of 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 cloud platform

EDGELOCK SE051- PERSO APPLET
CONFIGURE PLATFORM FEATURES THROUGH THE SUPPORTED INTERFACES



PLUG&TRUST

SEMS Lite applet

IoT applet

PERSO applet

JCOP OS

Interfacing

I^2C slave

SW I2C master*

ISO/IEC 14443*

MCU/MPU

Sensor

NFC reader

** Optional I^2C master and ISO/IEC14443 interfaces to support new IoT security use cases.*

PERSO applet

Provides the possibility to reconfigure SE051 devices. The configuration options include communication parameter settings of I2C, ISO14443 and ISO7816 interface as well as the deletion of unused operating system (cryptography) modules to gain additional memory.

- **Platform personalization before shipment**
  - PERSO applet exposes an API to **configure** platform-specific configurations or to **delete** specific JCOP modules not required in the target customer application before shipment.
- **Configurable parameters**
  - Contactless communication parameters
  - Contact-based communication parameters
  - I2C interface parameters
- **Deletable modules**
  - Some JCOP modules* can be removed to free memory space, including*:
  - e.g. RSA Key Gen, ECDAA, EdDSA,

Note: Deletion of modules will impact on the EdgeLock SE051 capabilities. For more information and details refer to the AN13015

► The PERSO applet is intended to be **removed** from the system via SEMS-Lite script before deployment to the end-customer to avoid any misconfiguration in the field

EDGELOCK SE051- PRODUCT VARIANTS

SE050 with IoT applet pre-installed + new features and updatability

SE051A2

SEMS Lite, ECC, AES, AES GCM, GMAC, TDES, MIFARE KDF

SE051C2

SEMS Lite, RSA, AES, AES GCM, GMAC, DES, MIFARE KDF, ISO 14443, I2C Master

SE050 w/o IoT applet for customer applet development on JCOP

SE051P2

No IoT applet, SEMS Lite, JCOP4 IoT, ISO7816, ISO14443

	SE051C2	SE051A2	SE051P
SEMS Lite	Yes*	Yes*	Yes*
ECC crypto schemes	ECDSA ECDHE DH_Mont ECDAA EdDSA	ECDSA ECDHE DH_Mont	All crypto features via JCOP OS API available for applet development
ECC curves	NIST (192 to 521 bit) Brainpool (160 to 512 bit) Koblitz (160 to 256 bit) Twisted Edwards (for Ed25519) Montgomery (Curve25519) Barreto-Naehrig (Curve256) Montgomery (Curve448) [Goldilocks]	NIST (192 to 521 bit) Brainpool (160 to 512 bit) Koblitz (160 to 256 bit)	
RSA	RSA (up to 4096)	-	
Symmetric	3DES (2K, 3K) AES (128, 192, 256) AES CCM, AES GCM*	3DES (2K, 3K) AES (128, 192, 256) AES CCM, AES GCM*	
MAC	HMAC, CMAC, GMAC*	HMAC, CMAC, GMAC*	
Hash function	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
Key Derivation Function	TLS (KDF, PSK) MIFARE DESFire KDF PBKDF2 (Wifi EAP) HKDF	TLS (KDF, PSK) MIFARE DESFire KDF PBKDF2 (Wifi EAP) HKDF	
Secure channel	Secure Channel Host-SE (Platform SCP)	Secure Channel Host-SE (Platform SCP)	
User memory (NV)	46 kB (up to 104 kB with PERSO options*)	46 kB (up to 104 kB with PERSO options*)	63 kB (up to 143 kB with PERSO options*)
User memory (RAM)	608 bytes	608 bytes	2106 bytes
Pre-provisioned	Yes	Yes	No
Interfaces	I2C Slave I2C Master ISO 14443	I2C Slave	I2C Slave I2C Master ISO 14443
TRNG	NIST IG7.15, AIS31	NIST IG7.15, AIS31	NIST IG7.15, AIS31
DRBG	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20	NIST SP800-90A, AIS20

** Extension added on top of EdgeLock SE050 features*

PLUG &TRUST

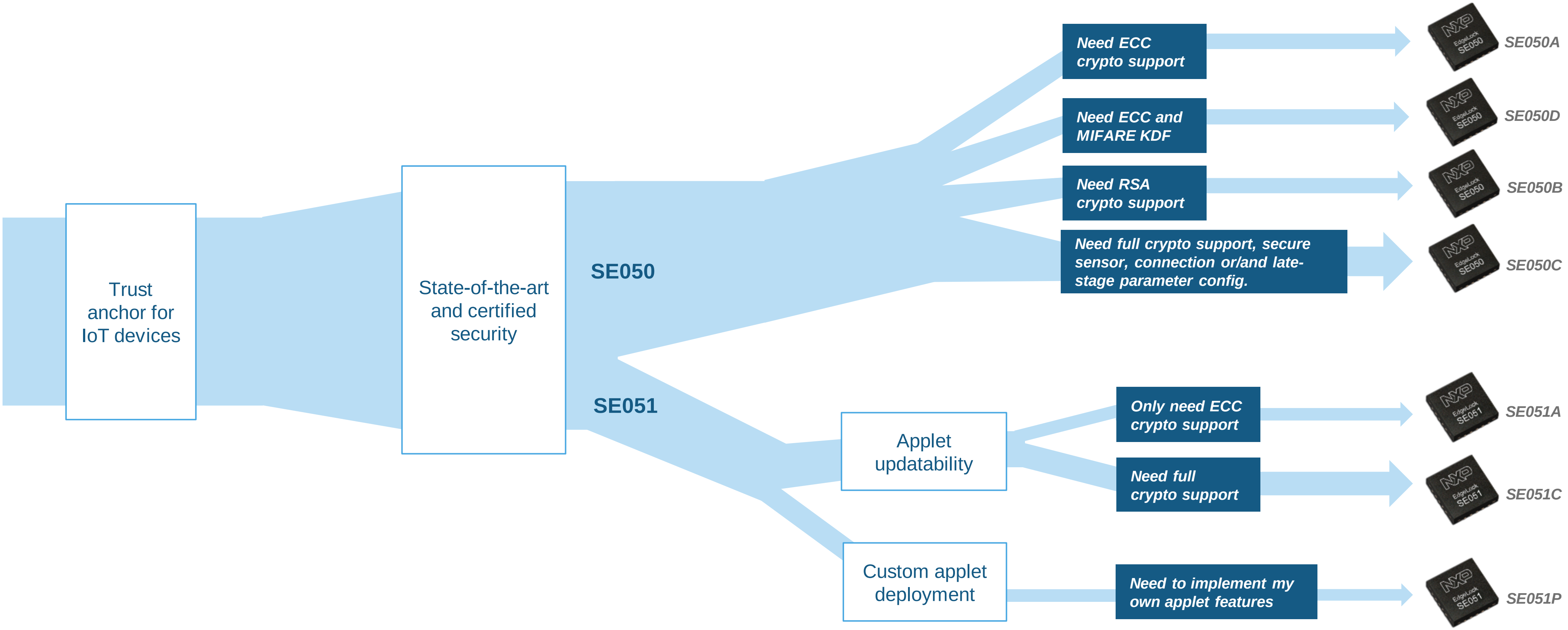
EdgeLock SE05x product decision tree

SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.

EDGELOCK SE05X - PRODUCT TREE SELECTION


Trust anchor for IoT devices
State-of-the-art and certified security
SE050
SE051
Need ECC crypto support
Need ECC and MIFARE KDF
Need RSA crypto support
Need full crypto support, secure sensor, connection or/and late-stage parameter config.
SE050A
SE050D
SE050B
SE050C
Applet updatability
Custom applet deployment
Only need ECC crypto support
Need full crypto support
Need to implement my own applet features
SE051A
SE051C
SE051P

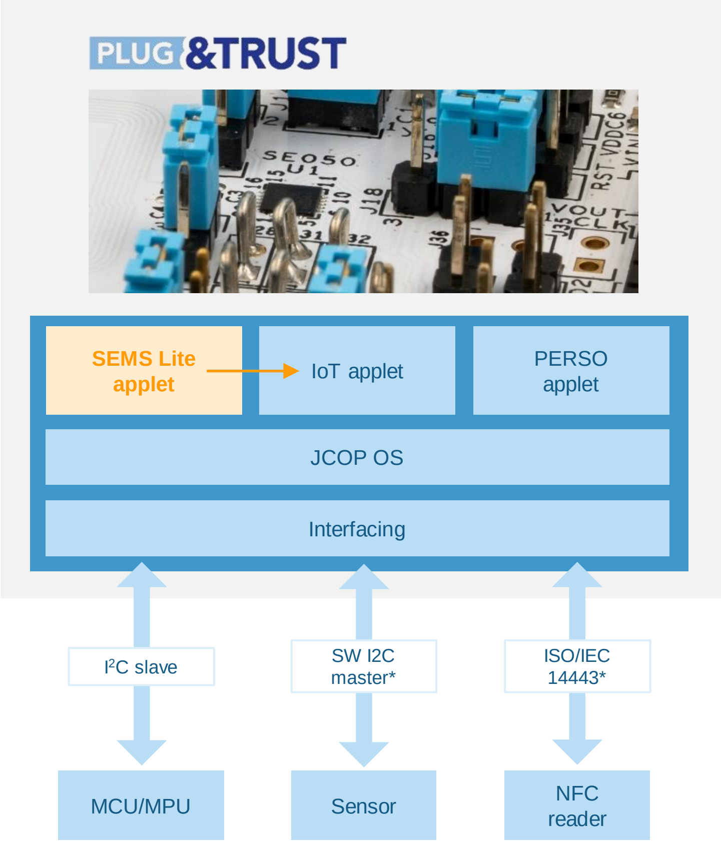
SEMS Lite for IoT applet update

SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.

SEMS LITE IS A DIFFERENTIATING CAPABILITY IN THE IOT SECURE ELEMENT MARKET



PLUG&TRUST

SEMS Lite applet → IoT applet

PERSO applet

JCOP OS

Interfacing

I²C slave

SW I2C master*

ISO/IEC 14443*

MCU/MPU

Sensor

NFC reader

** Optional I²C master and ISO/IEC14443 interfaces to support new IoT security use cases.*

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Card Spec 2.3, Amendment I (SEMS):

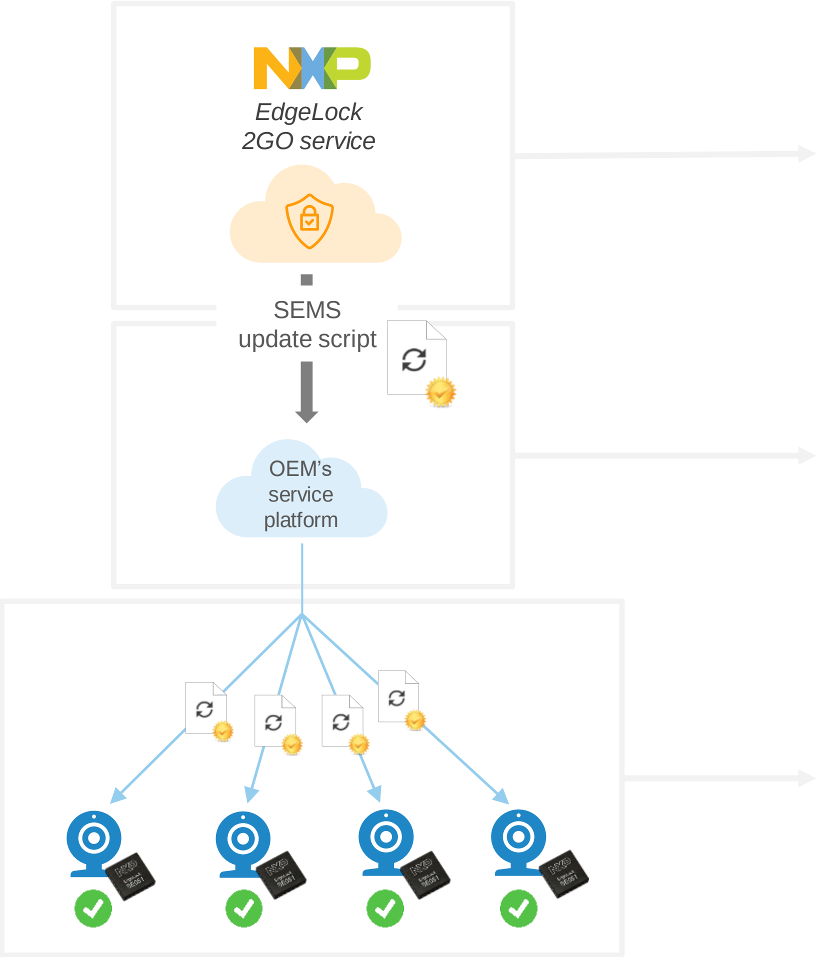
SEMS Lite is a capability based on a **subset** of *GlobalPlatform's Secure Element Management Service (SEMS),* **optimized for IoT use cases**.

GlobalPlatform Card Spec 2.3, Amendment H

EdgeLock SE051 IoT applet uses the on-device data backup mechanism specified in Amendment H. It saves its state and user data during any updates or upgrades in progress.

Global Platform industry standard SEMS has been used to securely update wearable and mobile secure elements for years

IOT APPLET UPDATE PROCESS USING SEMS LITE AND EDGELOCK 2GO



1. NXP pushes the secure IoT applet update package to EdgeLock 2GO

NXP may issue security updates after having fully assessed impact, as well as tested and validated the update on their product.

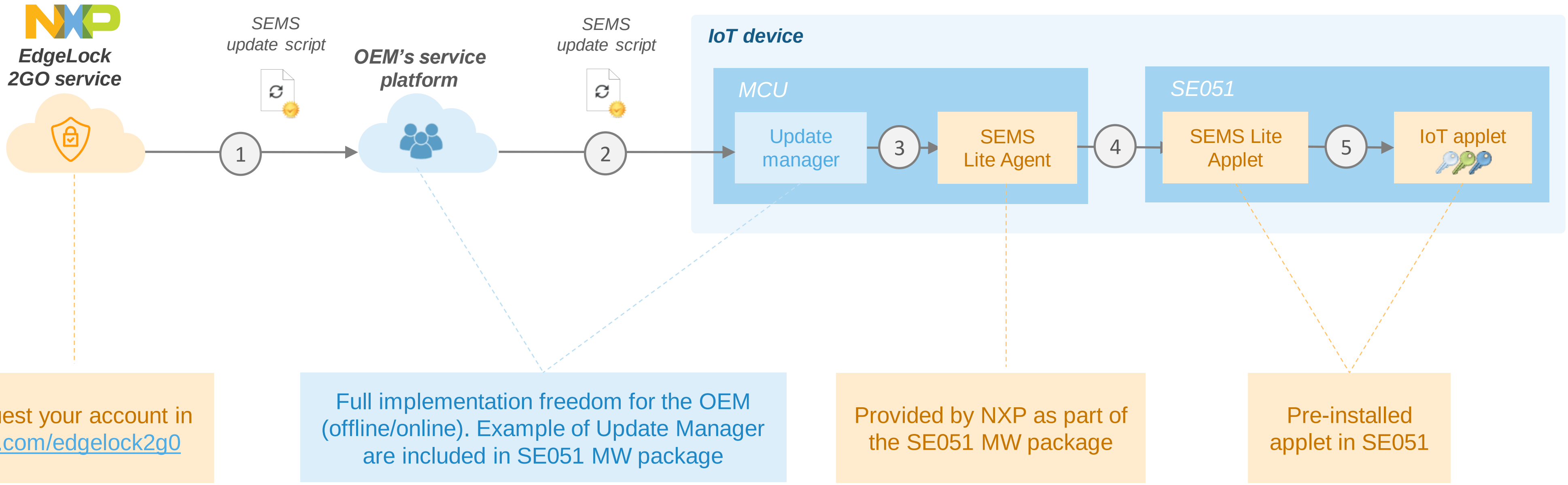
2. OEM downloads the IoT applet update package

The OEM downloads the SEMS update script directly from the EdgeLock 2GO and stores it in a suitable location accessible to IoT devices deployed in the field.

3. IoT device installs the IoT applet update package using SEMS Lite

IoT devices take advantage of the latest IoT applet features and security improvements as soon as they are available.

SEMS LITE NXP FULL SOLUTION OFFERING



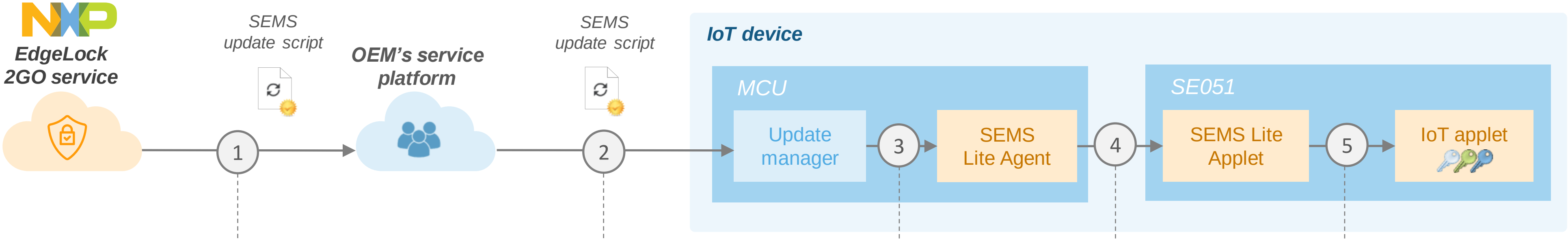
Request your account in nxp.com/edgelock2g0

Full implementation freedom for the OEM (offline/online). Example of Update Manager are included in SE051 MW package

Provided by NXP as part of the SE051 MW package

Pre-installed applet in SE051

IOT APPLET UPDATE PROCESS USING SEMS LITE AND EDGELOCK 2GO (DETAILED)



1. The OEM downloads the update SEMS directly from the EdgeLock 2GO

2. The Update Manager downloads the SEMS update script from the OEM backend

3. The Update Manager forwards the SEMS update script to the SEMS Lite Agent using the SEMS Lite Agent API

4. The SEMS Lite Agent connects to EdgeLock SE051 and triggers the execution of the IoT applet update script

5. The SEMS Lite Applet checks the validity of the script and executes the update commands one by one until the IoT applet is updated

AVAILABLE RESOURCES FOR IOT APPLET UPDATE

Software tools and sample code

sems-lite-ex-update

Project example with a reference implementation of the SEMS Lite Agent.

sems-lite-cli command-line-tool

Pre-compiled executable tool to interact with SEMS Lite Applet API.

sems-lite_json_converter.py

Conversion tool to prepare the update-data as downloaded from NXP

SEMS Lite scripts (via EdgeLock 2GO)

Update IoT Applet 6.0

Recovery Script

Update IoT Applet 6.1

Test update-script, just updates version, no functionality change

Delete Perso-Applet

Script to remove Perso applet from the SE051. Check AN13015 for more details

Documentation

AN12907 Secure update of EdgeLock SE051 IoT applet

Describes the SEMS Lite feature and explains how it can used to update the EdgeLock SE051 IoT applet.

Plug & Trust MW documentation (SEMS Lite Agent)

SEMS Lite Agent API description and usage flows.

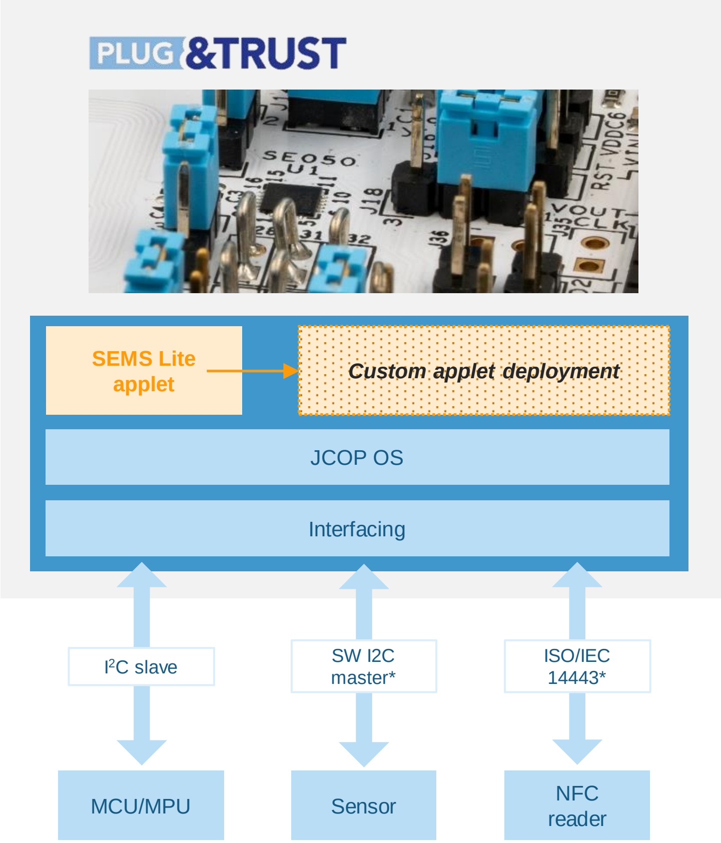
SEMS Lite for custom applet development & deployment on EdgeLock SE051P

SECURE CONNECTIONS FOR A SMARTER WORLD

EXTERNAL

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.

EDGELOCK SE051P – FLEXIBILITY TO CREATE YOUR CUSTOM APPLETS



** Optional I²C master and ISO/IEC14443 interfaces to support new IoT security use cases.*

Custom applet development and deployment

- No IoT applet. Freedom to develop your own custom applets to meet the specific needs of your use cases and business
- Offload critical security functions to your own custom applets and keep taking advantage of the high security offered by EdgeLock SE051 hardware and software
- Use the powerful NXP JCOP Tools to develop, test and debug your custom applets
- Control the complete deployment lifecycle of your custom applets: load, update, delete applets thanks to SEMS Lite support

AVAILABLE RESOURCES FOR APPLET DEVELOPMENT

Applet development and debug

NXP JCOP Tools plugin for Eclipse

Eclipse plugin for applet development. Available in NXP DocStore* upon request (**sw500120**).

EdgeLock SE051P Simulator for Eclipse

Simulator for EdgeLock SE051P integrated with JCOP Tools plugin for Eclipse. Available in NXP DocStore* upon request (**sw630101**).

OM-SE051ARD development board with EdgeLock SE051P

Arduino compatible development board for SE051P. Available upon request.

Applet deployment using SEMS Lite

LS-CGT

Tool to automate the generation of secure SEMS Lite scripts to deploy custom applets. Available in NXP DocStore upon request (sw630101).

EdgeLock SE05x Plug & Trust Middleware

Contains all the tools required to execute custom SEMS Lite scripts to deploy custom applets in EdgeLock SE051P. Available in NXP website.

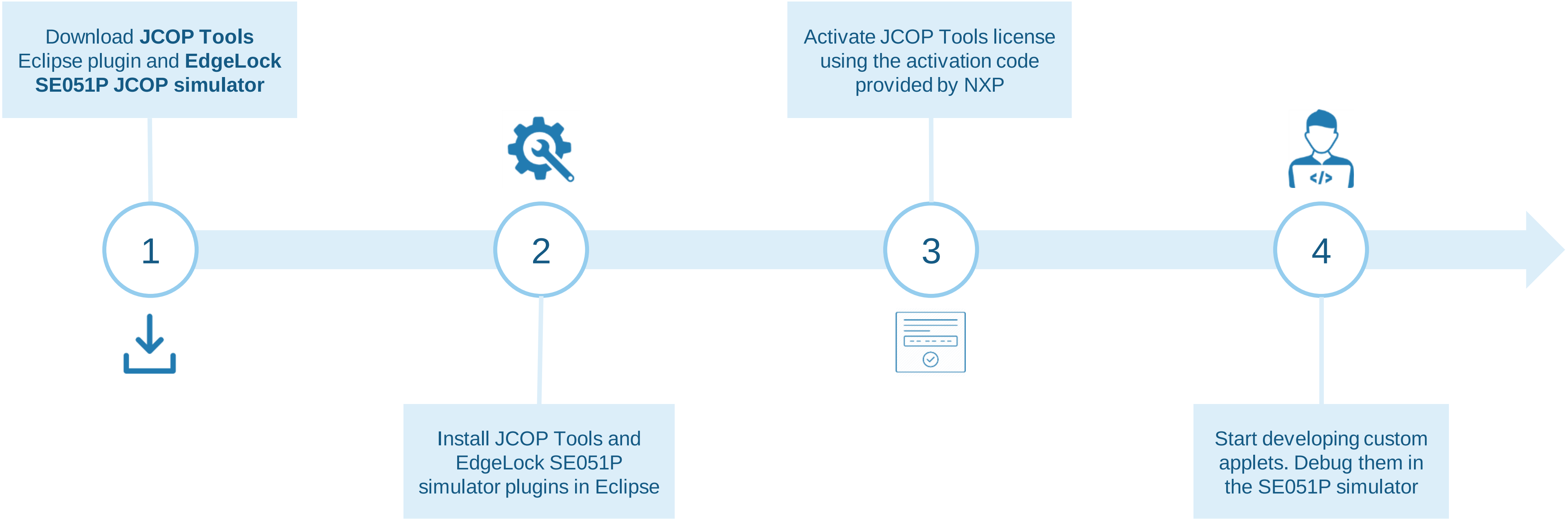
Application notes

AN12909 - How to develop JCOP applets on SE051 using JCOP Tools.

Quick start guide and step-by-step instructions to develop, debug and deploy custom applets in EdgeLock SE051P. Available in NXP DocStore* upon request (**an641010**).

** Docstore is NXP's web portal for the distribution of secure and export-controlled documentation.*

NXP JCOP TOOLS DEVELOPMENT ENVIRONMENT SETUP PROCESS



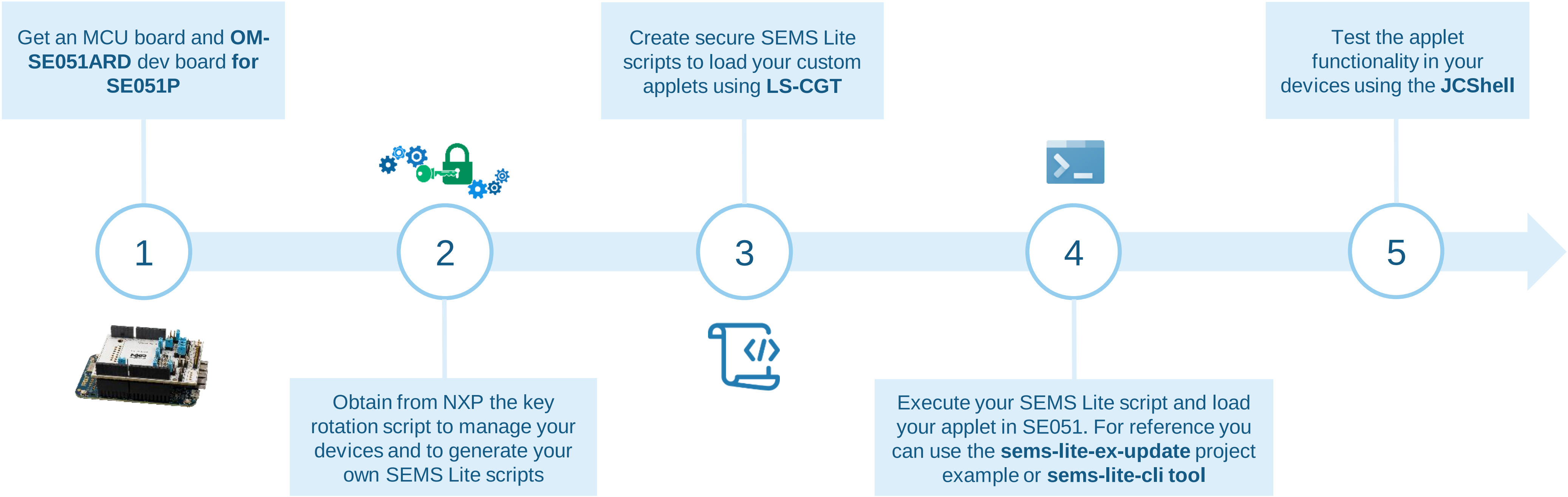
1. Download **JCOP Tools** Eclipse plugin and **EdgeLock SE051P JCOP simulator**

2. Install JCOP Tools and EdgeLock SE051P simulator plugins in Eclipse

3. Activate JCOP Tools license using the activation code provided by NXP

4. Start developing custom applets. Debug them in the SE051P simulator

APPLET DEPLOYMENT PROCESS WITH SE051 SUPPORT PACKAGE



1. Get an MCU board and **OM-SE051ARD** dev board **for SE051P**

2. Obtain from NXP the key rotation script to manage your devices and to generate your own SEMS Lite scripts

3. Create secure SEMS Lite scripts to load your custom applets using **LS-CGT**

4. Execute your SEMS Lite script and load your applet in SE051. For reference you can use the **sems-lite-ex-update** project example or **sems-lite-cli tool**

5. Test the applet functionality in your devices using the **JCShell**

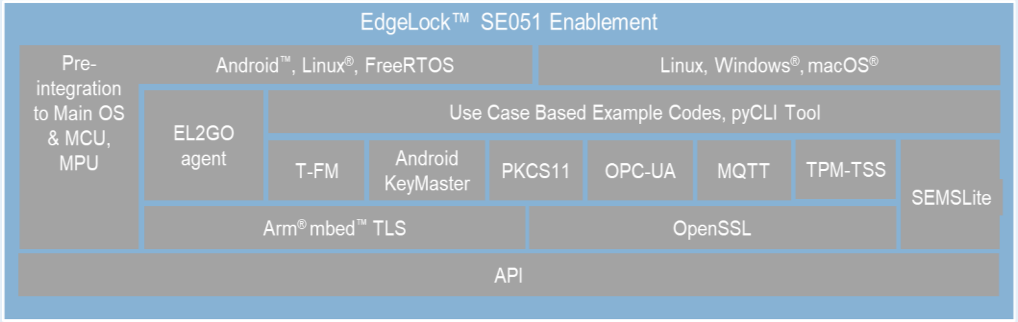
Support package

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.

EDGELOCK SE05X PLUG & TRUST PRODUCT SUPPORT PACKAGE

EdgeLock SE051 Plug & Trust middleware



EdgeLock™ SE051 Enablement

Pre-integration to Main OS & MCU, MPU

Android™, Linux®, FreeRTOS

Linux, Windows®, macOS®

EL2GO agent

Use Case Based Example Codes, pyCLI Tool

T-FM

Android KeyMaster

PKCS11

OPC-UA

MQTT

TPM-TSS

SEMSLite

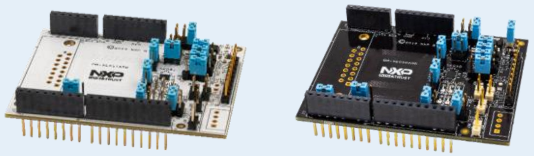
Arm® mbed™ TLS

OpenSSL

API

SE05x Arduino compatible development kits

- FRDM-K64F
- i.MX8
- i.MX RT1060
- LPC55S



Supported evaluation MCU/MPU boards

Demo codes

Documentation

NXP Semiconductors

AN12394

Get started with SE050 support package

1 About SE050 support package

The SE050 support package is a comprehensive set of resources that simplifies design-in and reduces time to market. It offers libraries for different MCUs, integration with the most common OSs including Linux, Windows, RTOS and Android. It also includes example codes for major use cases, extensive application notes and compatible development kits for i.MX, LPC and Kinetis microcontrollers.

The SE050 support package is prepared to demonstrate the latest IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or protection of sensor data, among many others. You can leverage SE050 support package to simplify the implementation of strong security mechanisms to meet the ever-increasing demand for easy-to-design and scalable IoT security.

EDGELOCK SE05X PLUG & TRUST PRODUCT SUPPORT PACKAGE (DETAILED)

Product specification and HW

- DS-SE050 SE050 Datasheet
- DS-SE051 SE051 Datasheet
- AN12413 SE050 IoT Applet APDU Spec
- AN12543 SE051 IoT Applet APDU Spec
- AN12436 SE050 Configurations
- AN12973 SE051 Configurations
- AN12514 SE050 User Guidelines
- AN12730 SE051 User Guidelines
- UM11225 NXP SE05x T=1 Over I2C Specification
- SOT1969-1 HX2QFN20 Datasheet
- AN1902 Package assembly guidelines

Software

- SE-PLUG-TRUS-MW SE05x Middleware + included .html API docu
- SE-PLUG-TRUST-SD-CARD-IMX8 SE05x Middleware SD card image
- SE-SDK-K64F SDK for FRDM-K64
- SE-SDK-LPC55S69 SDK for LPC55S69
- SE-SDK-IMXRT1060 SDK for i.MX RT 1060
- SW500120 NXP JCOP Tools plugin for Eclipse (*DocStore)
- SW630101 LS-CGT (*DocStore)

Cloud connection guides

- AN12400 SE05x Secure connection to OEM Cloud
- AN12404 SE05x Secure connection to AWS IoT Core
- AN12402 SE05x Secure Connection to Azure IoT Hub
- AN12401 SE05x Secure connection to Google Cloud IoT Core
- AN12403 SE05x Secure Connection to Watson IoT

Quick start guides and getting started manuals

- AN13013 Get started with SE05x support package
- AN12488 SE05x Plug & Trust middleware porting guidelines
- AN12398 SE05x Quick start guide Windows (Visual Studio)
- AN12396 SE05x Quick start guide with Kinetis (K64F)
- AN12450 SE05x Quick start guide with i.MX RT 1060
- AN12542 SE05x Quick start guide with LPC55S69
- AN12397 SE05x Quick start Guide i.MX6UL (Linux)
- AN12570 SE05x Quick start guide with Raspberry Pi
- AN13027 SE05x Quick start Guide i.MX8M (Linux)
- AN12907 SE051 Secure update of IoT Applet
- AN13014 Moving from SE050 to SE051

Use cases

- AN12399 SE05x for device-to-device authentication
- AN12449 SE05x Sensor data protection
- AN12664 SE05x for late-stage configuration
- AN12569 SE05x Secure access control in Industrial
- AN12662 SE05x Binding a host device to EdgeLock SE050
- AN12660 SE05x Ease ISA/IEC 62443 compliance with EdgeLock
- AN12661 SE05x for Wi-Fi Credential Protection
- AN12663 SE05x TPM functionality
- AN12907 SE051 Secure update of the IoT applet
- AN13015 SE051 How to use PERSO applet
- AN12909 SE051 How to develop applets using JCOP Tools (*DocStore)

Development kit documentation

- AN12395 OM-SE050ARD board hardware overview
- AN13016 OM-SE051ARD board hardware overview

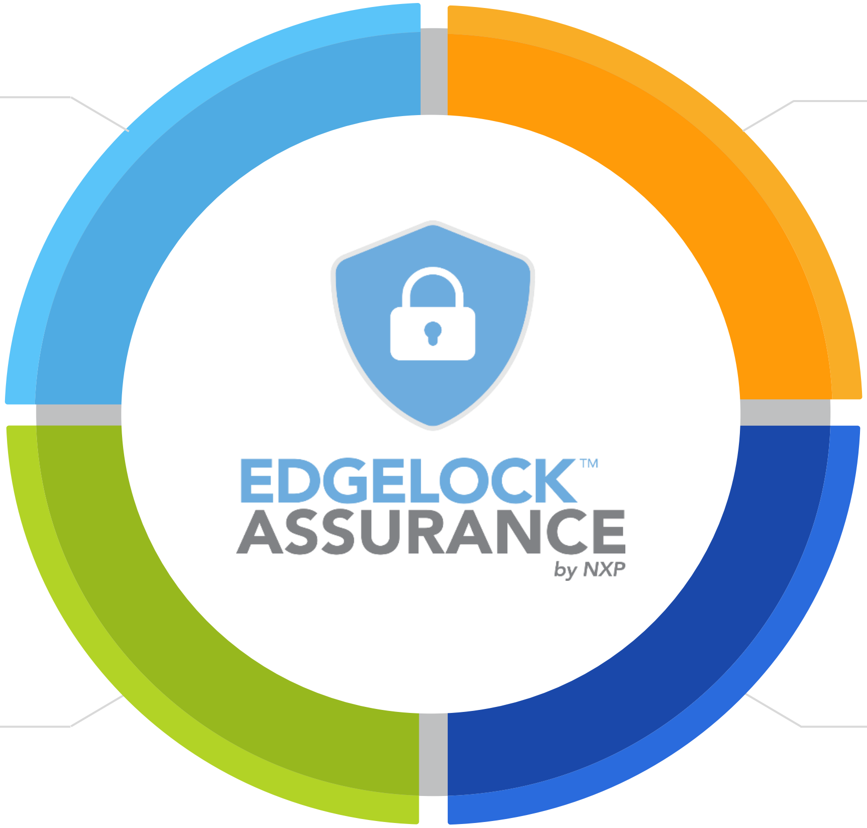
Closure

SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.

EDGELOCK ASSURANCE PROGRAM
RECOGNIZED FOR SECURITY ACROSS MANY MARKETS



PRODUCTS
Discrete and integrated solutions to meet your needs

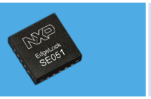
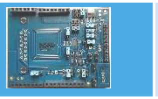
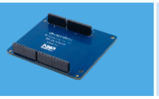
SUPPORT
NXP and partner ecosystem support for end-to-end security

PROCESS
Security-by-design is integral to how we operate

COMPLIANCE
Products designed to meet relevant industry standards

ORDERABLE TYPES AND BOARDS

For more info check out www.nxp.com/SE051

SE051 variant	Orderable part number	Description	Temperature range	12NC
SE051C2	SE051C2HQ1/Z01XDZ	SEMS Lite, ECC, RSA, , AES, MIFARE KDF, I2C Slave, I2C Master, ISO14443	-40 to +105 °C	935414457472
SE051A2 	SE051A2HQ1/Z01XEZ	SEMS Lite, ECC, AES, , MIFARE KDF, I2C Slave	-40 to +105 °C	935414458472
SE051P2	SE051P2HQ1/Z011AZ	No IoT applet, SEMS Lite, JCOP 4 IoT, I2C Slave, I2C Master, ISO14443	-40 to +105 °C	935409596472
SE051A/C Dev Kit	OM-SE051ARD	SE051A/C Arduino compatible development kit	-40 to +105 °C	935399187598
SE051P Dev Kit 	X-OM-SE051ARD-P *	SE051P Arduino compatible development kit	-40 to +105 °C	935416598598
Raspberry Pi adapter 	OM-SE050RPI	Arduino to Raspberry Pi Layout Adapter board	N/A	935398642598

* SE051P Dev kit board should be requested through your NXP representative

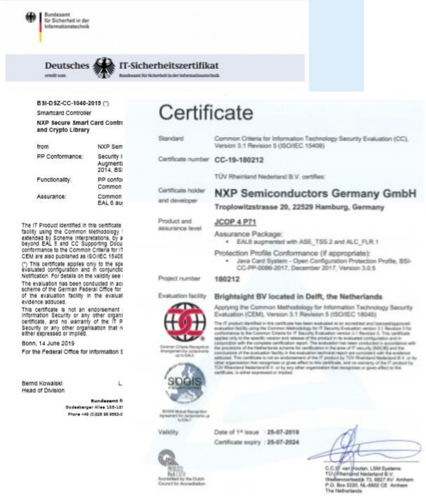
KEY POINTS TO HAVE IN MIND FOR CHOOSING EDGELOCK SE051

PLUG&TRUST

EdgeLock SE051

Extension to the EdgeLock SE050 with the capability for updatability and delivering proven security certified to CC EAL 6+, with AVA_VAN.5 up to the OS level

- Proven Security - CC EAL 6+
- Unique Feature Set – High Flexibility
- Updatability – Security Maintenance
- Solution for Fast Design-In



Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1040-2019 (*)

Smartcard Controller

NXP Secure Smart Card Contr
and Crypto Library

from NXP Sem
PP Conformance: Security I
Augment
2014, BSI
Functionality: PP confor
Common
Assurance: Common
EAL 6 au

The IT Product identified in this certificate
facility using the Common Methodology
extended by Scheme Interpretations, by a
beyond EAL 5 and CC Supporting Docu
conformance to the Common Criteria for IT
CEM are also published as ISO/IEC 15408

(*) This certificate applies only to the spe
evaluated configuration and in conjunctio
Notification. For details on the validity see

The evaluation has been conducted in acc
scheme of the German Federal Office for
of the evaluation facility in the evaluat
evidence adduced.

This certificate is not an endorsement
Information Security or any other organi
certificate, and no warranty of the IT P
Security or any other organisation that r
either expressed or implied.

Bonn, 14 June 2019

For the Federal Office for Information S

Bernd Kowalski
Head of Division

Bundesamt f
Godesberger Allee 185-18
Phone +49 (0)228 99 9582-0

Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number: CC-19-180212

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer: NXP Semiconductors Germany GmbH
Troplowitzstrasse 20, 22529 Hamburg, Germany

Product and assurance level: JCOP 4 P71

Assurance Package:
- EAL6 augmented with ASE_TSS.2 and ALC_FLR.1

Protection Profile Conformance (if appropriate):
- Java Card System - Open Configuration Protection Profile, BSI-CC-PP-0099-2017, December 2017, Version 3.0.5

Project number: 180212

Evaluation facility: Brightsight BV located in Delft, the Netherlands

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

[illegible]

Validity: Date of 1st issue : 25-07-2019
Certificate expiry : 25-07-2024

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

More information and questions about this training session at:

NXP Community for Secure Authentication

Mobile Knowledge

MobileKnowledge is a team of HW, SW and system engineers, experts in **smart, connected and secure** technologies for the IoT world. We are your ideal **engineering consultant** for any specific support in connection with your **IoT** and **NFC** developments. We design and develop secure HW systems, embedded FW, mobile phone and secure cloud applications.

Our services include:

- **Secure hardware design**
- **Embedded software development**
- **NFC antenna design** and **evaluation**
- **NFC Wearable**
- **EMV L1 pre-certification support**
- **Mobile** and **cloud application development**
- **Secure e2e system design**
- **ISO 26262 Functional Safety** Engineering Services*

MIFARE Accredited Training Partner

NXP GOLD PARTNER

MOBILE WORLD CAPITAL BARCELONA

We help companies leverage the **secure IoT revolution**

contact@themobileknowledge.com

www.themobileknowledge.com

* MobileKnowledge engineers were trained in ISO 26262 Functional Safety by TÜV SÜD.

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V. ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2020 NXP B.V.