AN12973

SE051 configurations

Rev. 2.0 — 8 July 2024

Application note

Document information

Information	Content
Keywords	SE051
Abstract	Definition of available EdgeLock SE051 variants.

1 Overview

The SE051 family comprise of several variants that differentiate on applet and configuration level.

Table 1 shows which applets are available on which SE051 variants.

Table 1. Application Specific Applet

SE051 Variant	IoT Applet	Applet Updatability (SEMS Lite)	Customer Applet Programmability (SEMS Lite)	Secure UWB (FiRa Lite, SUS)	Perso applet	Type 4 Tag Applet
SE051A	x	x			x	
SE051C	x	x			x	
SE051P			x		x	
SE051W	x	x		x		
SE051H	x	x				x
Documentation	AN12543 [1]	AN12907 [3]	AN12909 [4]	AN13525 [6]	AN13015 [5]	AN13788 [8]

Table 2. Generic information

Category	Value
Security Certification	CC EAL6+ (HW+JCOP)
JavaCard version	3.0.5
GlobalPlatform Specification version	GP 2.3.1
Reserved SSD AID for all applications	D276000085304A434F9003

2 SE051 A/C – pre-configuration for ease of use with IoT Applet

2.1 General description

EdgeLock SE051 A/C comes with pre-integrated IoT applet. These variants with pre-integrated IoT applet are offered off-the-shelf pre-provisioned for ease of use. This means that for most of the use cases and cloud services customers are not required to program additional credentials. Device public cloud keys or IDs can be read out from the chip (e.g. at manufacturing time) and installed on different Cloud services depending on the respective Cloud authentication modalities. Additional information on the usage of the credentials can be found in several application notes on the NXP website. Also see SE051 APDU Specification, section 3.2.

The SE051 platform allows the update of the applet. NXP has launched a new applet with version number 7.2 in 2022 and all new products will have the newest applet. To check which applet is delivered in SE051 please refer to Table 4. All new parts with date code starting from 2022 are containing applet 7.2.

2.1.1 IoT applet configurations

Table 3. SE051 A/C IoT applet configurations

Categories		SE051A2	SE051C2
ECC Crypto Schemes	ECDSA	x	x
	ECDH	x	x
	ECDHE	x	x
	DH_Mont		x
	EdDSA		x
	PAKE		
Supported Elliptic Curves	ECC NIST (192 bit to 521 bit)	x	x
	Brainpool (160 bit to 512 bit)	x	x
	Koblitz (160 bit to 256 bit)	x	x
	Twisted Edwards (for Ed25519)		x
	Montgomery (Curve25519)		x
	Montgomery (Curve448) [Goldilocks]		x
RSA	RSA (up to 4096 bit)		x
Symmetric Crypto Algorithm	3DES (2K, 3K)	x	x
	AES (128 bit, 192 bit, 256 bit)	x	x
AES modes	CBC, CTR, ECB	x	x
	CCM, GCM	x	x
Hash Function	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	x	x
MAC	HMAC, CMAC, GMAC	x	x
Key Derivation (KDF)	TLS (KDF, PSK)	x	x
	MIFARE DESFire KDF	x	x
	PBKDF2	x	x
	HKDF	x	x
Secure Channel	Secure Channel Host-SE (Platform SCP)	x	x
TRNG		NIST SP800-90B, AIS31	NIST SP800-90B, AIS31
DRBG		NIST SP800-90A, AIS20	NIST SP800-90A, AIS20
Memory reliability	up to 100 million write cycles / 25 years	x	x
User Memory	Full Featured to Max Value	46 kB to 104 kB	46 kB to 104 kB
User Memory – Full Feature - NV		46 kB	46 kB
User Memory – Maximum - NV		104 kB	104 kB

Table 3. SE051 A/C IoT applet configurations*...continued*

Categories		SE051A2	SE051C2
User Memory - RAM (Clear on deselect)		608 bytes	608 bytes
Pre-Provisioned		x	x
Interfaces	Contactless: ISO/IEC 14443 passive, type A		x
	I^2C Target, up to 3.4 Mbit with clock stretching enabled	x	x
	I^2C Controller, Fast Mode (400 kbit/s)		x
Power saving modes	Power-Down (with state retention), ~430 µA (ISO7816) - 460 µA (I^2C)	Disabled [1]	Disabled [1]
	Deep Power-Down (no state retention), <5 µA	x	x
Temperature	Standard, -25 °C - 85 °C		
	Extended, -40 °C - 105 °C	x	x
Packaging	Plastic QFN, 3 mm x 3 mm (HX2 QFN20)	x	x
Clock Stretching		Disabled [2]	Disabled [2]

[1] Power-down mode availability to be enabled using the Perso applet, see [5].

[2] Clock stretching can be enabled using the Perso applet, see [5].

2.2 Variant identifier

The identifying information can be read out using the example "get info" from SE051 Plug&Trust MW package. This variant identifier is also known as OEF ID. This will allow to distinguish the delivered configuration.

Table 4. Variant identifiers

Variant	Variant Identifier (OEF ID)	Applet Version	Date Code[1]
SE051A2	A920	7.2	>= 2150
SE051C2	A8FA	7.2	>= 2201
SE051A2	A565	6.0	<= 2149
SE051C2	A564	6.0	<= 2152

[1] Date code can be found either on the reel label or on the IC marking, see chapter Marking in the SE051 DS [2]

2.3 Common keys

The keys in Table 5 are present in all configurations.

For the value of the Platform SCP keys (set as default in key set 11), please refer to Table 6.

A second set of Platform SCP keys are inserted with KVN 12. Key set 12 is a recovery key set. It can be used to establish a platform SCP connection in case key set 11 is lost. After authentication with key set 12, key set 11 can be updated again to the new values. Keep in mind that it is required that key set 12 shall be changed to a customer defined and owned value before the SE051 product is deployed in production. For generic products, NXP own the recovery key set. For customized products, the recovery key value can be retrieved from EdgeLock2Go and customers can update them if recovery feature is not required. As an example for key update, please refer to "se05x_RotatePlatformSCP03Keys" in the Plug & Trust MW.

Table 5. Common objects

Key name	Details and type	Certificate	Erasable by customer	Identifier
Common files	UUID	N/A	No	0x7FFF0206
Platform SCP	Default Value needed to perform update of the key	N/A	No	N/A
Recovery SCP	Default Value needed to perform recovery	N/A	No	N/A
ECKey session	Establish an ECC256 based EC key session	N/A	No	0x7FFF0201
ECKey import	Used for ImportExternalObject	N/A	No	0x7FFF0202

Table 6. Default Platform SCP keys

Configuration	ENC	MAC	DEK	OEF ID
SE051A2	88ea9fa686f3cf2ffcaf4b1cba93e442	4f163f59f07431f43ee2ee1834a52334	d476cf47aa27b54ab3dbebe7656d6770	A920
SE051C2	bfc2dbe1828e035d3e7fa36b902a05c6	bef85bd7ba0497d628781ce47b188c96	d873f316be297f2fc9c0e45f54710699	A8FA
SE051A2	840a5d51795511c9cef0c96fd2cbf041	646bc2b8c3a4d9c1fa8d7116be04fdfe	03e6699aca9426d9c38922f8914ce5f7	A565
SE051C2	88dbcd65820d2aa06ffab92aa8e79364	a8644e2a04d9e9c8c0ea6086682999e5	8a38723899881844e2c1513dacd9f80d	A564

2.3.1 NXP reserved keys and objects

Table 7. NXP reserved keys and objects

Key name	Erasable by customer	Identifier	Comment
RESERVED_ID_FEATURE	No	0x7FFF0204	Applet Feature Management Key
NXP reserved key	No	0xF0000020	Only available to NXPs Edgelock2Go
NXP_APPLET_IMPORT_ RFC3394_KEK	No	0xF0003394	Only available to NXPs Edgelock2Go
NXP_MIFARE_CRC	No	0x7FFF020B	Not a key but a binary file for NXP internal implementation purposes

2.4 Variant A

Table 8. Variant A

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
Connectivity Key (Authentication Connectivity Key 0), ECC256, Die Individual	Connectivity Certificate 0	Anybody, Read	No	0xF0000000 (key) 0xF0000001 (cert)
Connectivity Key	Connectivity Certificate 1	Anybody, Read	No	0xF0000002 (key)

Table 8. Variant A*...continued*

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
(Authentication Connectivity Key 1), ECC256, Die Individual				`0xF0000003` (cert)
Attestation key, ECC256, Die Individual	N/A	Anybody Read and Attestation	No	`0xF0000012` (key)

[1] Certificates are always erasable by customer

2.5 Variant C

Table 9. Variant C

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
Connectivity Key (Authentication Connectivity Key 0), ECC256, Die Individual	Connectivity Certificate 0, ECC signed	Anybody, Read	No	`0xF0000000` (key) `0xF0000001` (cert)
Connectivity Key (Authentication Connectivity Key 1), ECC256, Die Individual	Connectivity Certificate 1, ECC Signed	Anybody, Read	No	`0xF0000002` (key) `0xF0000003` (cert)
Cloud connection key 0, RSA2048, Die Individual	Cloud Connectivity Certificate 0, RSA Signed	Default	Yes	`0xF0000110` (key) `0xF0000111` (cert)
Cloud connection key 1, RSA2048, Die Individual	Cloud Connectivity Certificate 1, RSA Signed	Default	Yes	`0xF0000112` (key) `0xF0000113` (cert)
Cloud connection key 0, ECC256, Die Individual	Cloud Connectivity Certificate 0, ECC signed	Default	Yes	`0xF0000100` (key) `0xF0000101` (cert)
Cloud connection key 1, ECC256, Die Individual	Cloud Connectivity Certificate 1, ECC Signed	Default	Yes	`0xF0000102` (key) `0xF0000103` (cert)
Root of Trust signing key, ECC256, Die Individual (used to attest new generated keys)	Attestation Certificate, ECC Signed	Anybody Read and Attestation	No	`0xF0000012` (key) `0xF0000013` (cert)
Root of Trust signing key, RSA2048, Die Individual (used to attest new generated keys)	Attestation Certificate, RSA Signed	Anybody Read and Attestation	No	`0xF0000010` (key) `0xF0000011` (cert)
RSA Key, RSA4096	Cloud Connectivity Certificate 0, RSA Signed	Default	Yes	`0xF0000120` (key) `0xF0000121` (cert)
RSA Key, RSA4096	Cloud Connectivity Certificate 1, RSA Signed	Default	Yes	`0xF0000122` (key) `0xF0000123` (cert)

[1] Certificates are always erasable by customer

3 SE051 W - pre-configuration for secure UWB ranging

3.1 General description

EdgeLock SE051W is a ready-to-use IoT secure element securing ultra wide band (UWB) connections. Secure UWB use cases, for example, are physical or logial access or indoor localization. Applications can be found in Smart Home like Secure UWB Door Locks, Secure UWB Login to computing or gaming devices or in the industrial IoT.

EdgeLock SE051W is pre-integrated with the Trimension SR150 and supports secure ranging operations. Therefore SE051W securely stores long living root keys, sets up secure binding and creates secure channels with SR150, provides session keys and supports dynamic STS (scrambled time stamp).

EdgeLock SE051W is updatable on applet level for feature updates or security maintenance purposes. The EdgeLock SE051W is offered with pre-integrated IoT, SUS and FIRA Lite applet as off-the-shelf variant pre-provisioned for ease of use. This means that for most of the use cases and cloud services customers are not required to program additional credentials. Device public cloud keys or IDs can be read out from the chip (e.g. at manufacturing time) and installed on different Cloud services depending on the respective Cloud Authentication modalities. Additional information on the usage of the credentials can be found in several application notes on the website for SE051 and SE051W. Also see SE051 APDU specification [1], section "SE051 Secure Objects".

For custom variant configuration please contact your NXP representative.

SE051W is based on a SE051 product with the feature set listed in Table 10 In addition, there is SUS and FiRa available for secure ranging.

The applet versions of SE051W products must be checked and, if required, updated using SEMS Lite as per Table 11 to ensure compliance with the latest FiRa specifications.

SEMS Lite update packages are shared using the section “Applet Update” of the NXP Edgelock2Go service [7] and pre-configured update examples named “demo_semslite_FiRaLite” are included in the UWB Middleware for SR150T.

3.1.1 SE051W IoT applet configurations

Table 10. SE051W IoT applet configurations

Categories		SE051W2
ECC Crypto Schemes	ECDSA	x
	ECDH	x
	ECDHE	x
	DH_Mont	
	EdDSA	
	PAKE	
Supported Elliptic Curves	ECC NIST (192 bit to 521 bit)	x
	Brainpool (160 bit to 512 bit)	x
	Koblitz (160 bit to 256 bit)	x
	Twisted Edwards (for Ed25519)	
	Montgomery (Curve25519)	

Table 10. SE051W IoT applet configurations*...continued*

Categories		SE051W2
	Montgomery (Curve448) [Goldilocks]	
RSA	RSA	RSA usage only up to 2k keys. Key injection only, no key generation.
Symmetric Crypto Algorithm	3DES (2K, 3K)	x
	AES (128 bit, 192 bit, 256 bit)	x
AES modes	CBC, CTR, ECB	x
	CCM, GCM	x
Hash Function	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	x
MAC	HMAC, CMAC, GMAC	x
Key Derivation (KDF)	TLS (KDF, PSK)	x
	MIFARE DESFire KDF	x
	PBKDF2	x
	HKDF	x
Secure Channel	Secure Channel Host-SE (Platform SCP)	x
TRNG		NIST SP800-90B, AIS31
DRBG		NIST SP800-90A, AIS20
Memory reliability	up to 100 million write cycles / 25 years	x
User Memory	Full Featured to Max Value	25 kB
User Memory – Full Feature - NV		25 kB
User Memory - RAM (Clear on deselect)		806 Byte
Pre-Provisioned		x
Interfaces	Contactless: ISO/IEC 14443 passive, type A	x
	I^2C Target, up to 3.4 Mbit with clock stretching enabled	x
	I^2C Controller, Fast Mode (400 kbit/s)	x
Power saving modes	Power-Down (with state retention), ~430 µA (ISO7816) - 460 µA (I^2C)	Disabled [1]
	Deep Power-Down (no state retention), <5 µA	x
Temperature	Standard, -25 °C - 85 °C	
	Extended, -40 °C - 105 °C	x
Packaging	Plastic QFN, 3 mm x 3 mm (HX2QFN20)	x
Clock Stretching		Disabled

[1] Power down mode can be enabled in custom part configuration.

3.2 Variant identifier

The identifying information can be read out using the example "get info" from SE051 Plug&Trust MW package. This variant identifier is also known as OEF ID. This will allow to distinguish the delivered configuration.

Table 11. Variant identifiers

Variant	Variant Identifier (OEF ID)	Applet Version	Date code
SE051W2	A739	IoT applet version 7.2 FIRA Lite applet version 1.0.11 SUS applet version 2.0	<2239
SE051W2	A739	IoT applet version 7.2 FIRA Lite applet version 1.0.14 SUS applet version 2.0	>2239

3.3 Common Keys

Table 12. Common objects

Key name	Details and type	Certificate	Erasable by customer	Identifier
Common files	UUID	N/A	No	`0x7FFF0206`
Platform SCP	Default Value needed to perform update of the key	N/A	No	N/A
Recovery SCP	Default Value needed to perform recovery	N/A	No	N/A
ECKey session	Establish an ECC256 based EC key session	N/A	No	`0x7FFF0201`
ECKey import	Used for ImportExternalObject	N/A	No	`0x7FFF0202`

Table 13. Default Platform SCP keys

Configuration	ENC	MAC	DEK	OEF ID
SE051W (Fira)	`18b3b4e340c080d99bebb8b8644b8c52`	`3d0cfac87b967c00e33ba496613838a2`	`680683f94e6bcb9473ecc1567a1bd109`	`A739`

3.4 NXP reserved keys and objects

Table 14. NXP reserved keys and objects

Key name	Erasable by customer	Identifier	Comment
RESERVED_ID_FEATURE	No	`0x7FFF0204`	Applet Feature Management Key
NXP reserved key	No	`0xF0000020`	Only available to NXPs Edgelock2Go
NXP_APPLET_IMPORT_RFC3394_KEK	No	`0xF0003394`	Only available to NXPs Edgelock2Go

Table 14. NXP reserved keys and objects*...continued*

Key name	Erasable by customer	Identifier	Comment
NXP_MIFARE_CRC	No	`0x7FFF020B`	Not a key but a binary file for NXP internal implementation purposes

3.5 Variant W

Table 15. Variant W

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
Connectivity Key (Authentication Connectivity Key 0), ECC256, Die Individual	Connectivity Certificate 0	Anybody, Read	No	`0xF0000000` (key) `0xF0000001` (cert)
Connectivity Key (Authentication Connectivity Key 1), ECC256, Die Individual	Connectivity Certificate 1	Anybody, Read	No	`0xF0000002` (key) `0xF0000003` (cert)
Root of Trust signing key, ECC256, Die Individual	N/A	Anybody Read and Attestation	No	`0xF0000012` (key)

[1] Certificates are always erasable by customer

3.6 Provisioning of FiRa

The root certificate is taken to sign the die individual SC2 and SCP11c certificate provisioned to the FiRa applet.

- NXP Root CA for FiRa

4 SE051 H - pre-configuration for Matter and NFC commissioning

4.1 General description

EdgeLock SE051H is a ready-to-use IoT secure element optimized for the Matter protocol and smart home devices. EdgeLock SE051H supports additional cryptographic mechanisms to be used with the Matter protocol such as SPAKE2+ or a new attestation mechanism (internal signature generation). EdgeLock SE051H also enables device commissioning via NFC. EdgeLock SE051H is tailored for smart home devices who need optimal performances and security for the Matter protocol with an improved user experience using the NFC technology.

EdgeLock SE051H is pre-integrated with the Type 4 Tag Applet which makes the secure element compatible with NFC Type 4 tags. Therefore the secure element can store NDEF messages that can be retrieved from a smartphone or an NFC reader. This can be used for storing the Matter onboarding payload in the secure element in addition or instead of a QR code and read it over NFC.

EdgeLock SE051H is updatable on applet level for future evolutions of the Matter standard or security maintenance purposes. The EdgeLock SE051H is offered with pre-integrated IoT applet as off-the-shelf variant pre-provisioned for ease of use. This means that for most of the use cases and cloud services customers are not required to program additional credentials. Device public cloud keys or IDs can be read out from the chip (e.g. at manufacturing time) and installed on different Cloud services depending on the respective Cloud Authentication modalities. Additional information on the usage of the credentials can be found in several application notes on the website for SE051 and SE051H. Also see SE051 APDU specification [1], section "SE051 Secure Objects".

For custom variant configuration please contact your NXP representative.

SE051H is based on a SE051 product with the feature set listed in Table 16 and with the addition of the T4T Applet.

4.1.1 SE051H IoT applet configurations

Table 16. SE051H IoT applet configurations

Categories		SE051H2
ECC Crypto Schemes	ECDSA	x
	ECDH	x
	ECDHE	x
	DH_Mont	x
	EdDSA	x
	PAKE	x
Supported Elliptic Curves	ECC NIST (192 bit to 521 bit)	x
	Brainpool (160 bit to 512 bit)	x
	Koblitz (160 bit to 256 bit)	x
	Twisted Edwards (for Ed25519)	x
	Montgomery (Curve25519)	x
	Montgomery (Curve448) [Goldilocks]	x
RSA	RSA	up to 2048bit
Symmetric Crypto Algorithm	3DES (2K, 3K)	x
	AES (128 bit, 192 bit, 256 bit)	x

Table 16. SE051H IoT applet configurations*...continued*

Categories		SE051H2
AES modes	CBC, CTR, ECB	x
	CCM, GCM	x
Hash Function	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	x
MAC	HMAC, CMAC, GMAC	x
Key Derivation (KDF)	TLS (KDF, PSK)	x
	MIFARE DESFire KDF	x
	PBKDF2	x
	HKDF	x
Secure Channel	Secure Channel Host-SE (Platform SCP)	x
TRNG		NIST SP800-90B, AIS31
DRBG		NIST SP800-90A, AIS20
Memory reliability	up to 100 million write cycles / 25 years	x
User Memory	Full Featured to Max Value	16 kB
User Memory – Full Feature - NV		16 kB
User Memory - RAM (Clear on deselect)		2221 Byte
Pre-Provisioned		x
Interfaces	Contactless: ISO/IEC 14443 passive, type A	x
	I^{2}C Target, up to 3.4 Mbit with clock stretching enabled	x
	I^{2}C Controller, Fast Mode (400 kbit/s)	x
Power saving modes	Power-Down (with state retention), ~430 µA (ISO7816) - 460 µA (I^{2}C)	Disabled [1]
	Deep Power-Down (no state retention), <5 µA	x
Temperature	Standard, -25 °C - 85 °C	
	Extended, -40 °C - 105 °C	x
Packaging	Plastic QFN, 3 mm x 3 mm (HX2QFN20)	x
Clock Stretching		Disabled

[1] Power down mode can be enabled in custom part configuration.

4.1.2 T4T applet configuration

Table 17. T4T applet configuration

Setting	Value	Permanently locked
Max NDEF record size	1024 bytes	Yes
Read over Contact	Not allowed	Yes
Write over Contact	Allowed	No
Read over Contactless	Allowed	No
Write over Contactless	Allowed	No

4.2 Variant identifier

The identifying information can be read out using the example "get info" from SE051 Plug&Trust MW package. This variant identifier is also known as OEF ID. This will allow to distinguish the delivered configuration.

Table 18. Variant identifiers

Variant	Variant Identifier (OEF ID)	Applet Version
SE051H2	B36A	IoT applet version 7.2.46 T4T Applet version 1.6.0

4.3 Common Keys

Table 19. Common objects

Key name	Details and type	Certificate	Erasable by customer	Identifier
Common files	UUID	N/A	No	0x7FFF0206
Platform SCP	Default Value needed to perform update of the key	N/A	No	N/A
Recovery SCP	Default Value needed to perform recovery	N/A	No	N/A
ECKey session	Establish an ECC256 based EC key session	N/A	No	0x7FFF0201
ECKey import	Used for Import ExternalObject	N/A	No	0x7FFF0202

Table 20. Default Platform SCP Keys

Configuration	ENC	MAC	DEK	OEF ID
SE051H	7a406b4b62e4aa851c323ca855ee4b63	616bc12a4cd4b06a021f3abb62144f1d	540337787696eebe931320f87bde2289	B36A

4.4 NXP reserved keys and objects

Table 21. NXP reserved keys and objects

Key name	Erasable by customer	Identifier	Comment
RESERVED_ID_FEATURE	No	0x7FFF0204	Applet Feature Management Key
NXP reserved key	No	0xF0000020	Only available to NXPs Edgelock2Go
NXP_APPLET_IMPORT_RFC3394_KEK	No	0xF0003394	Only available to NXPs Edgelock2Go
NXP_MIFARE_CRC	No	0x7FFF020B	Not a key but a binary file for NXP internal implementation purposes

4.5 Variant H

Table 22. Variant H

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys) [1]	Identifier
Connectivity Key (Authentication Connectivity Key 0), ECC256, Die Individual	Connectivity Certificate 0	Anybody, Read	No	0xF0000000 (key) 0x F0000001 (cert)
Connectivity Key (Authentication Connectivity Key 1), ECC256, Die Individual	Connectivity Certificate 1	Anybody, Read	No	0xF0000002 (key) 0x F0000003 (cert)
Root of Trust signing key, ECC256, Die Individual	N/A	Anybody Read and Attestation	No	0xF0000012 (key)

[1] Certificates are always erasable by customer

4.6 Provisioning of SPAKE 2+ verifiers and device attestation keypair

The following provisioned objects are all objects with reserved Identifier. The object type and usage is defined in the SE051 APDU spec [1].

Table 23. SPAKE2+ verifiers and device attestation key pair

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
M value for SPAKE2+ P256/SHA256/HMAC/HKDF	N/A	Anybody, Read	No	0x7FFF0210
N value for SPAKE2+ P256/SHA256/HMAC/HKDF	N/A	Anybody, Read	No	0x7FFF0211
Pin codes and salts Die Individual	N/A	Default	Yes	0x7FFF2000
Verifier set #1 w0 for iteration count 1000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2011
Verifier set #1 L for iteration count 1000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2021
Verifier set #1 w0 for iteration count 5000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2012
Verifier set #1 L for iteration count 5000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2022

Table 23. SPAKE2+ verifiers and device attestation key pair*...continued*

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
Verifier set #1 w0 for iteration count 10000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2013
Verifier set #1 L for iteration count 10000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2023
Verifier set #1 w0 for iteration count 50000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2014
Verifier set #1 L for iteration count 50000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2024
Verifier set #1 w0 for iteration count 100000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2015
Verifier set #1 L for iteration count 100000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2025
Verifier set #2 w0 for iteration count 1000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2016
Verifier set #2 L for iteration count 1000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2026
Verifier set #2 w0 for iteration count 5000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2017
Verifier set #2 L for iteration count 5000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2027
Verifier set #2 w0 for iteration count 10000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2018
Verifier set #2 L for iteration count 10000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2028
Verifier set #2 w0 for iteration count 50000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2019
Verifier set #2 L for iteration count 50000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF2029
Verifier set #2 w0 for iteration count 100000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF201A

Table 23. SPAKE2+ verifiers and device attestation key pair*...continued*

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
Verifier set #2 L for iteration count 100000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF202A
Verifier set #3 w0 for iteration count 1000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF201B
Verifier set #3 L for iteration count 1000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF202B
Verifier set #3 w0 for iteration count 5000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF201C
Verifier set #3 L for iteration count 5000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF202C
Verifier set #3 w0 for iteration count 10000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF201D
Verifier set #3 L for iteration count 10000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF202D
Verifier set #3 w0 for iteration count 50000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF201E
Verifier set #3 L for iteration count 50000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF202E
Verifier set #3 w0 for iteration count 100000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF201F
Verifier set #3 L for iteration count 100000, Die Individual.	N/A	Anybody, Key Agreement	No	0x7FFF202F
Device attestation key pair, restricted signature input in 0x 7FFF2031, ECC256, Die Individual	N/A	Anybody, Signing, Forbid external sign input, Read	No	0x7FFF2030

5 Chain of trust and objects configuration

5.1 SE051 Chain of trust certificates

5.1.1 Iot Connectivity

These certificates are used for the services of EdgeLock 2GO.

Consider that their deletion prevents the device from connecting to the EdgeLock 2GO service over TLS.

- SE051A/C/W/H

5.1.2 Cloud Onboarding RSA

- Root
  - Intermediate
    - SE051C2-A8FA. Previous variant: SE051C2-A564

5.1.3 Cloud Onboarding ECC

- Root
  - Intermediate
    - SE051C2-A8FA. Previous variant: SE051C2-A564.

5.1.4 Attestation RSA

- Root
  - Intermediate

5.1.5 Attestation ECC

- Root
  - Intermediate

5.2 SE051 chain of trust for EdDSA certificates

The usage of chain of trust for EdDSA (Ed25519) can be requested only on customer specific types.

5.2.1 Cloud Onboarding Ed25519

- Root
  - Intermediate

5.2.2 Attestation Ed25519

- Root
  - Intermediate

5.3 Secure objects configuration

In case a secure objects gets pre-provisioned according to the above tables, then the secure objects have this configuration:

Table 24. Secure objects configuration

Object ID	File Size	Object Class	AuthObject	Policy (Authentication Object + applied Access Rules)	Auth attempts cntr	Auth attempts limit	TagLen for AEAD	min Output Length	Owner	Origin
0x7FFF0206	18	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0201	32	EC_KEY_PAIR	Yes	Default	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0202	32	EC_KEY_PAIR	Yes	Default	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0204	32	EC_PUB_KEY	Yes	Default	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0210	32	EC_KEY_PAIR	No	0x00000000 ALLOW_READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0211	32	EC_KEY_PAIR	No	0x00000000 ALLOW_READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF2000	108	BINARY_FILE	No	0x00000000 DEFAULT	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0x7FFF2011 - 0x7FFF201F	32	HMAC_KEY	No	0x00000000 ALLOW_KA	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF2021 - 0x7FFF202F	65	HMAC_KEY	No	0x00000000 ALLOW_KA	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF2030	32	EC_KEY_PAIR	No	0x00000000 ALLOW_SIGN, ALLOW_READ, FORBID_EXTERNAL_INPUT_SIGN[0x7FFF2031]	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF020B	1024	BINARY_FILE	No	0x7FFF0204 WRITE DELETE	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0003394	32	AES_KEY	No	0x00000000 WRAP	N/A	N/A	0x10	N/A	0x00000000	PROVISIONED
0xF0000020	32	EC_PUB_KEY	Yes	0xF0000020 READ WRITE	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0xF0000012	32	EC_KEY_PAIR	No	0x00000000 READ ATTESTATION	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000013	467	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL

Table 24. Secure objects configuration*...continued*

Object ID	File Size	Object Class	AuthObject	Policy (Authentication Object + applied Access Rules)	Auth attempts cntr	Auth attempts limit	TagLen for AEAD	min Output Length	Owner	Origin
0xF0000010	256	RSA_KEY_PAIR_CRT	No	0x00000000 READ ATTESTATION	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000011	863	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000000	32	EC_KEY_PAIR	No	0xF0000020 READ WRITE GEN 0x00000000 SIGN VERIFY KA ENC DEC READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000002	32	EC_KEY_PAIR	No	0xF0000020 READ WRITE GEN 0x00000000 SIGN VERIFY KA ENC DEC READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000001	470	BINARY_FILE	No	0xF0000020 READ WRITE 0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000003	470	BINARY_FILE	No	0xF0000020 READ WRITE 0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000100	32	EC_KEY_PAIR	No	Default	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000102	32	EC_KEY_PAIR	No	Default	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000110	256	RSA_KEY_PAIR_CRT	No	Default	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000112	256	RSA_KEY_PAIR_CRT	No	Default	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000120	512	RSA_KEY_PAIR_CRT	No	Default	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000122	512	RSA_KEY_PAIR_CRT	No	Default	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000101	549	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000103	549	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000111	1206	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000113	1206	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000121	1462	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL

5.4 X.509 Certificate storage encoding

This paragraph provides details on the storage of X.509v3 Certificates in Binary Files on the NXP IoT Applet.

The command `ReadSize` can be used to read the size of the complete binary file containing a certificate.

Table 25. Content of Certificate Binary File

Name	Length [bytes]	Description
X.509 Certificate	variable (length encoded in X.509)	DER encoded X.509v3 Certificate. The length can be parsed from the first TLV sequence which spans over the complete certificate.
Zero padding	variable (remaining bytes up to the complete binary file size)	The file size of the binary file is constant over all devices of a type, while the specific device certificate can vary in size per device (due to the ASN.1 encoding of numbers).

6 Note about the source code in the document

Example code shown in this document has the following copyright and BSD-3-Clause license:

7 References

[1] SE051 IoT Applet APDU Specification, document number AN12543. Available on NXP website.

[2] SE051 - Plug & Trust Secure Element Datasheet, document number 5773xx. Available on NXP website.

[3] Secure update of EdgeLock SE051 IoT applet, document number AN12907. Available on NXP website.

[4] How to develop JCOP applets on EdgeLock SE051 using JCOP Tools, document number AN12909. Available on NXP Docstore under 6410xx.

[5] How to use EdgeLock SE051 PERSO applet, document number AN13015. Available on NXP website.

[6] FiRa Lite Applet User Guidance Manual, document number AN13525. Available on NXP Docstore.

[7] NXP Edgelock2Go service, see NXP website.

[8] SE05x T4T APDU specification 1.0, document number AN13788, Available on NXP website.

Abbreviations

Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
CL	Contactless
CMAC	Cipher-based Message Authentication Code
DES	Digital Encryption Standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie–Hellman
ECDHE	Elliptic Curve Diffie–Hellman ephemeral
EdDSA	Edwards Curve Digital Signature Algorithm
HMAC	Keyed-Hash Message Authentication Code
I^2C	Inter-Integrated Circuit
IoT	Internet of Things
JCOP	Java Card Open Platform
KDF	Key Derivation Function
MAC	Message Authentication Code
NIST	National Institute for Standards and Technology
OEF	Order Entry Form
PSK	Pre-Shared Key
RSA	Rivest-Shamir-Adleman
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TPM	Trusted Platform Module

8 Revision history

Revision history

Revision number	Date	Description
AN12973 v.2.0	08 July 2024	• corrected line Power saving modes and added line on AES modes CBC, CTR, ECB in Table 3, Table 10, and Table 16 • updated Legal information
AN12973 v.1.9	10 February 2023	• Updated Table 1 • Add Section 4 with SE051 H pre-configuration
AN12973 v1.8	18 October 2022	• Updated Section 3.1.1 • Updated Section 3.2 • Updated Section 3.1

Revision history*...continued*

Revision number	Date	Description
AN12973 v1.7	22 August 2022	• Updated Section 2.1.1.
AN12973 v1.6	21 April 2022	• Added Section 5.4.
AN12973 v1.5	14 February 2022	• Add Section 1 • Updated Section 2.1 • Updated Section 2.2 • Updated Section 2.3 • Updated links in Section 5.1 • Add Section 3 • Create Section 5 to reorganize the document
AN12973 v1.4	30 March 2021	• Updated Section 2.4 • Updated Section 2.5
AN12973 v1.3	01 February 2021	• Updated Section 2.3
AN12973 v1.2	16 December 2020	• Updated Table 3 • Updated Section 2.3
AN12973 v1.1	17 November 2020	• Updated Table 3
AN12973 v1.0	14 October 2020	Initial version

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

EdgeLock — is a trademark of NXP B.V.

JCOP — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

Tables

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

For more information, please visit: https://www.nxp.com

Document feedback