AN12436

SE050 configurations

Rev. 2.1 — 21 April 2022 Application note

543821

Document information

Information	Content
Keywords	SE050
Abstract	Definition of available SE050 configurations

Revision history

Revision history

Revision number	Date	Description
2.1	20220421	• Add Section 3.13. • Add Section 3.14.
2.0	20220328	• Update Section 2 • Update Section 3.4 • Update Section 3.2 • Add Section 3.6 • Add Section 3.3
1.9	20211104	• Add Section 3.11.5.1
1.8.2	20210902	• Add hexadecimal format of Platform build ID in the FIPS certificate in Section 2.1
1.8.1	20210721	• Added section Product Information in Section 1 • Added Product Information for SE050F in Section 2.1
1.8	20210628	• Add variant SE050F2 in Section 2, Section 3.4, Section 3.2, Section 3.11.4, Section 3.11.5 • Add Section 3.7 • Adapt Section 2.1
1.7	20210412	• Add Section 2.1
1.6	20210330	• updated Section 3.8 • updated Section 3.9 • updated Section 3.10
1.5	20201216	• updated legal disclaimer • updated Table 1 • add Section 3.11
1.4	20200827	• Added section Section 3.5 • Minor changes
1.3	20200708	added variant SE050D2 in • Table 1 • Section 3.8 update key description in Table 4
1.2	20200227	added Section 3.11.1
1.1	20191127	updated Table 6
1.0	20191011	Initial release

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
ECDAA	Elliptic Curve Direct Anonymous Attestation
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-Share Key
RSA	Rivest-Shamir-Adleman
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TPM	Trusted Platform Module

1 Product Information

The SE050 product identification can be obtained out by sending a dedicated command to the secure element.

The Plug & Trust Middleware (nxp.com) includes a utility called ‘se05x_GetInfo’ to retrieve detailed product information from the connected SE050 derivative. It is available as a Windows binary (binaries\ex\VCOM-se05x_GetInfo.exe) and in source code. The html documentation included with the Plug & Trust Middleware package (section ‘Demo & Examples’ > ‘SE05X Get Info example’) provides additional information on using and compiling the utility.

The information retrieved by se05x_GetInfo is a superset of what is required to determine whether an entry in the errata sheet is applicable to the product.

The exact product identification is covered by two parameters:

- The product OS configuration (Platform build ID) in the format JXXXXXXXXXXXXXXX.
  Example below : `J3R351021EEE0400`
- The product OS Patch ID
  Example below : `0000000000000001`
- The product ROM ID
  Example below: `2E5AD88409C9BADB`
- The version of the Applet in the format xx.xx.xx (major.minor.patch). Example below: 3.1.0

```
C:\<MW install Dir>\binaries\ex>VCOM-se05x_GetInfo.exe
COM<port>
App   :INFO :PlugAndTrust_v03.00.04_20200928
App   :INFO :Running se05x_GetInfo.exe
App   :INFO :Using PortName='COM<port>' (CLI)
Opening COM Port '\\.\COM<port>'
sss   :INFO :atr (Len=35)
      00 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 08
      01 00 00 00    00 64 00 00    0A 4A 43 4F    50 34 20 41
      54 50 4F
App   :WARN :No SemsLite Applet Available.
App   :INFO :Running se05x_GetInfo.exe
App   :INFO :Using PortName='COM<port>' (CLI)
Opening COM Port '\\.\COM34'
sss   :INFO :atr (Len=35)
      00 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 08
      01 00 00 00    00 64 00 00    0A 4A 43 4F    50 34 20 41
      54 50 4F
sss   :WARN :Communication channel is Plain.
sss   :WARN :!!!Not recommended for production use.!!!
App   :WARN :############################################
App   :INFO :uid (Len=18)
      04 00 50 01    43 E7 C2 90    7A BD 8B 04    42 0A 59 55
      00 00
App   :WARN :############################################
App   :INFO :Applet Major = 3
App   :INFO :Applet Minor = 1
App   :INFO :Applet patch = 0
App   :INFO :AppletConfig = 6FFF
App   :INFO :With ECDAA
App   :INFO :With ECDSA_ECDH_ECDHE
App   :INFO :With EDDSA
```

```
App   :INFO :With DH_MONT
App   :INFO :With HMAC
App   :INFO :With RSA_PLAIN
App   :INFO :With RSA_CRT
App   :INFO :With AES
App   :INFO :With DES
App   :INFO :With PBKDF
App   :INFO :With TLS
App   :INFO :With MIFARE
App   :INFO :With I2CM
App   :INFO :Internal = 010B
App   :WARN :###########################################
App   :INFO :Tag value - proprietary data 0xFE = 0xFE
App   :INFO :Length of following data 0x45 = 0x45
App   :INFO :Tag card identification data (Len=2)
      DF 28
App   :INFO :Length of card identification data = 0x42
App   :INFO :Tag configuration ID (Must be 0x01) = 0x01
App   :INFO :Configuration ID (Len=12)
      00 04 A1 F4    45 88 4F 17    E5 19 C0 69
App   :INFO :OEF ID (Len=2)
      A1 F4
App   :INFO :Tag patch ID (Must be 0x02) = 0x02
App   :INFO :Patch ID (Len=8)
      00 00 00 00    00 00 00 01
App   :INFO :Tag platform build ID1 (Must be 0x03) = 0x03
App   :INFO :Platform build ID (Len=24)
      4A 33 52 33    35 31 30 32    31 45 45 45    30 34 30 30
      BC 03 04 79    33 8D 18 10
App   :INFO :JCOP Platform ID = J3R351021EEE0400
App   :INFO :Tag FIPS mode (Must be 0x05) = 0x05
App   :INFO :FIPS mode var = 0x00
App   :INFO :Tag pre-perso state (Must be 0x07) = 0x07
App   :INFO :Bit mask of pre-perso state var = 0x00
App   :INFO :Tag ROM ID (Must be 0x08) = 0x08
App   :INFO :ROM ID (Len=8)
      2E 5A D8 84    09 C9 BA DB
App   :INFO :Status Word (SW) (Len=2)
      90 00
App   :INFO :se05x_GetInfoPlainApplet Example Success !!!...
App   :WARN :###########################################
App   :INFO :cplc_data.IC_fabricator (Len=2)
      47 90
App   :INFO :cplc_data.IC_type1 (Len=2)
      D3 21
App   :INFO :cplc_data.Operating_system_identifier (Len=2)
      47 00
App   :INFO :cplc_data.Operating_system_release_date (Len=2)
      00 00
App   :INFO :cplc_data.Operating_system_release_level (Len=2)
      00 00
App   :INFO :cplc_data.IC_fabrication_date (Len=2)
      91 69
App   :INFO :cplc_data.IC_Serial_number (Len=4)
      00 03 23 95
App   :INFO :cplc_data.IC_Batch_identifier (Len=2)
      36 73
App   :INFO :cplc_data.IC_module_fabricator (Len=2)
      00 00
App   :INFO :cplc_data.IC_module_packaging_date (Len=2)
```

```
      00 00
App   :INFO :cplc_data.ICC_manufacturer (Len=2)
      00 00
App   :INFO :cplc_data.IC_embedding_date (Len=2)
      00 00
App   :INFO :cplc_data.IC_OS_initializer (Len=2)
      01 42
App   :INFO :cplc_data.IC_OS_initialization_date (Len=2)
      0A 30
App   :INFO :cplc_data.IC_OS_initialization_equipment (Len=4)
      30 33 32 33
App   :INFO :cplc_data.IC_personalizer (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_date (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_equipment_ID (Len=4)
      00 00 00 00
App   :INFO :cplc_data.SW (Len=2)
      90 00
App   :INFO :ex_sss Finished
```

2 Configuration Table

Table 1. SE050 configuration

		SE050E2	SE050F2	SE050A1 SE050A2 SE050D2	SE050B1 SE050B2	SE050C1 SE050C2 OM-SE050ARD Dev Kit	OM-SE050ARD-E Dev Kit
RSA	RSA (up to 4096)		x (>= 2048 bit) (no RSA plain)		x	x	
Supported Elliptic Curves	NIST (192 to 521 bit)	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	x
	Twisted Edwards (Ed25519)	x				x	x
	Montgomery (Curve25519)	x				x	x
	Montgomery (Curve448) [Goldilocks]	x					x
ECC Crypto Schemes	ECDSA	x	x	x		x	x
	ECDH	x		x		x	x
	ECDHE	x		x		x	x
	ECDAA	x				x	x
	EdDSA	x				x	x
	PAKE						
Symmetric Crypto Algorithm	3DES (2K, 3K)	x	x (only 3K)	x	x	x	x
	AES (128, 192, 256)	x	x	x	x	x	x
AES Modes	CBC,CTR, EBC	x	x	x	x	x	x
	CCM, GCM	x					x
Hash Function	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	x	x (no SHA-1 digital signature)	x	x	x	x
MAC	HMAC, CMAC	x	x	x	x	x	x
	GMAC	x					x

Table 1. SE050 configuration*...continued*

		SE050E2	SE050F2	SE050A1 SE050A2 SE050D2	SE050B1 SE050B2	SE050C1 SE050C2 OM-SE050ARD Dev Kit	OM-SE050ARD-E Dev Kit
Key Derivation (KDF)	TLS KDF, TLS PSK	x		x	x	x	x
	MIFARE DESFire KDF	x		SE050D2 only		x	x
	Wi-Fi KDF (PBKDF2)	x		x	x	x	x
	OPC_UA KDF	x		x	x	x	x
TRNG	NIST SP800-90B, AIS31	x	x	x	x	x	x
DRBG	NIST SP800-90A, AIS20	x	x	x	x	x	x
TPM Functionalities		x		x	x	x	x
Pre-Provisioned		x	x	x	x	x	x
Interfaces	I^2C Target	x	x	x	x	x	x
	I^2C Controller Frequency	up to 1 Mbit/s	up to 3.4 Mbit/s	up to 3.4 Mbit/s	up to 3.4 Mbit/s	up to 3.4 Mbit/s	up to 1 Mbit/s
	I^2C Controller	x	x			x	x
	ISO14443 CL		x			x	
Temperature Range		-40 to +105°C	-40 to +105°C	**SE050A1:** -25 to +85°C **SE050A2:** -40 to +105°C **SE050D2:** -40 to +105°C	**SE050B1**: -25 to +85°C **SE050B2**: -40 to +105°C	**SE050C1**: -25 to +85°C **SE050C2**: -40 to +105°C **OM-SE050ARD Dev Kit**: -40 to +105°C	-40 to +105°C

2.1 SE050F Configuration - FIPS Certified

SE050 has been FIPS 140-2 certified with Security Level 3 for OS and Applet, and Security Level 4 related to Physical Security of the HW. The SE050F requires a specific configuration according to the certification, as indicated in Table 1. Some features are not available, such as:

- RSA 1024 Bit
- RSA in plain. RSA can only be used in CRT.
- 3DES with 2K
- SHA1 digital signature
- ECC Keys below 224B

Furthermore, the following applies for SE050F:

- SCP03 is mandatory. In order to make it mandatory, NXP provisioned a random RESERVED_ID_PLATFORM_SCP key with Identifier 0x7FFF0207 which cannot be modified/deleted. The default Platform SCP Keys on Table 6 MUST be updated
- RSA4096 Key Generation is disabled

For the SE050F Variant the Product Information according to Section 1 is:

- The product OS configuration (Platform build ID): `J3R3510264571100`[1]
- The product OS Patch ID: `0000000000000001`
- The product ROM ID: `2E5AD88409C9BADB`
- The version of the Applet (major.minor.patch): 3.6.0

In order to use the SE050F, NXP recommends to use the respective user guidelines for the SE050F [3].

1 The Platform build ID in the FIPS certificate is in hexadecimal format [4A335233353130323634353731313030034D67740BE14219]

3 SE050 – pre-configuration for ease of use – Plug & Trust

3.1 General description

All SE050 variants 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 www.nxp.com. Also see APDU Specification, section 3.2.

3.2 Variant identifier

The identifying information can be read out using the example "get info" from SE050 Plug&Trust MW package.

Table 2. Variant identifiers

Variant	Variant Identifier (OEF ID)
SE050E2	A921
SE050F2	A92A
SE050E Development Board	A921
SE050F Development Board	A92A
Previous Generation	
SE050A1	A204
SE050A2	A205
SE050D2	A43B
SE050B1	A202
SE050B2	A203
SE050C1	A200
SE050C2	A201
SE050F2	A77E[1]
Development Board	A1F4

[1] All SE050F2 with variant A77E have date code in year 2021. All the SE050F2 with date code in the year 2022 have the variant identifier A92A.

3.3 Variant Specific Documentation

NXP always recommend to consult and deploy the documentation below prior to start an end solution development.

Table 3. Variant Specific Documentation

Variant	User Guidelines	APDU Spec
A,B,C,D	[4][5]	[1]
F	[3]	[1]
E	[2]	[6]

3.4 Common keys

The keys in Table 4 are present in all configurations.

For the value of the Platform SCP please refer to Table 6.

Table 4. Common keys

Key name	Details and type	Certificate	Erasable by customer	Identifier
Platform SCP	Default Value needed to perform update of the key	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 5. Default Platform SCP keys for new generation of SE050 products

Configuration	OEF ID	ENC	MAC	DEK
SE050E2	A921	d2db63e7a0a5aed72a6460c4dfdcaf64	738d5b798ed241b0b24768514bfba95b	6702dac30942b2c85e7f47b42ced4e7f
SE050F2	A92A	b50e1f12b81fe53b6c3b5387912a1a5a	71936959d37f2b22c5a0c34919a2bc1f	869593239854dc0d869900500ca79c15
SE050E Development Board	A921	d2db63e7a0a5aed72a6460c4dfdcaf64	738d5b798ed241b0b24768514bfba95b	6702dac30942b2c85e7f47b42ced4e7f
SE050F Development Board	A92A	b50e1f12b81fe53b6c3b5387912a1a5a	71936959d37f2b22c5a0c34919a2bc1f	869593239854dc0d869900500ca79c15

Table 6. Default Platform SCP keys for Previous Generation of SE050 Products

Configuration	OEF ID	ENC	MAC	DEK
SE050A1	A205	34AE0967E329E9518E7265D5ADCC01C2	52B253CADF472BDB3D0FB38E09770099	ACC91431FE26811B5ECBC845620D8344
SE050A2	A204	46A9C48C34EFE344A522E66744F8996A	1203FF61DFBC9C86196A2274AEF4ED28	F7561C6F48336119EE39439AAB34098E
SE050D2	A43B	DE4A88D78478C5ECB4BC6E0528E370BF	DA947FC73A4C192AECBBE4F568930AEA	5120E50A8BC83BD37E99A5DCA76F8250
SE050B1	A203	D499BC90DEA542CF78D25E13D64CBB1F	0815559643FB79EB8501A0DC833D901F	BE7DDFB406E81AE4E9665A9FED64267C
SE050B2	A202	5FA43D8202D25E9A85B1FE7E2D26478D	105CEA2219F52BD167A07463C69379C3	D7028157F2AD372C74BE969BCC390627
SE050C1	A201	852B5962E9CCE5D0BE746B833BCC6287	DB0AA319A408696C8E107AB4E3C26B47	4C2F75C6A278A4AEE5C9AF7C50EEA80C
SE050C2	A200	BD1DE20A81EAB2BF3B709A9D69A31254	9A761B8DBA6BEDF22741E45D8D4236F5	9B993B600F1C64F5ADC063192A96C947
SE050F2	A77E	9188da8cf369cfa9a00891627b65345a	cb20f809c7a03932bc203b0a01816c81	278e619d83518e14c6f1e4fa968be51c
Development Board	A375	35C256458958A34F6136155F8209D6CD	AF177D5DBDF7C0D5C10A05B9F1607F78	A1BC8438BF77935B361A4425FE79FA29

3.4.1 NXP reserved keys

Table 7. NXP reserved keys

Key name	Erasable by customer	Identifier
NXP reserved key 1	No	0x7FFF0204
NXP reserved key 2	No	0x7FFF0209
NXP reserved key 3	No	0xF0000030
NXP reserved key 4	No	0xF0000020

3.5 Applet version

The applet version used in the secure element can be read out using the example "se05x_GetInfo" from the Plug&Trust MW package.

The minimum applet version delivered in the types A,B,C and D is 3.1.0, ICs with date code after January 2020 have applet variant 3.1.1. Customer individual types can have other applet versions.

In 2022 NXP has launched a new generation of SE050 products. The new variant is called SE050E and it contains a new applet with version number 7.2.

The applet version differences are listed in the SE050 APDU Spec [1].

3.6 Variant E

Table 8. Variant E

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

[1] Certificates are always erasable by customer

3.7 FIPS Variant F

Table 9. Variant F

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
Default Connectivity Key (Authentication Connectivity Key 0), ECC256, Die Individual	Connectivity Certificate 0, ECC signed	Anybody, Read	No	`0xF0000000` (key) `0xF0000001` (cert)
Default Connectivity Key (Authentication Connectivity Key 1), ECC256, Die Individual	Connectivity Certificate 1, ECC Signed	Anybody, Read	No	`0xF0000002` (key) `0xF0000003` (cert)

Table 9. Variant F*...continued*

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
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

3.8 Variant A / D

Table 10. Variant A

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

3.9 Variant B

Table 11. Variant B

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
Default Connectivity Key (Authentication Connectivity Key 0), RSA2048, Die Individual	Connectivity Certificate 0	Anybody, Read	No	0xF0000004 (key) 0xF0000005 (cert)
Default Connectivity Key (Authentication Connectivity Key 1), RSA2048, Die Individual	Connectivity Certificate 1	Anybody, Read	No	0xF0000006 (key) 0xF0000007 (cert)
Root of Trust signing key, RSA2048, Die Individual	N/A	Anybody, Read, and Attestation	No	0xF0000010 (key)

[1] Certificates are always erasable by customer

3.10 Variant C

Table 12. Variant C

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

Table 12. Variant C*...continued*

Key name and type	Certificate	Usage policy (keys)	Erasable by customer (keys)[1]	Identifier
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

3.11 SE050 Chain of trust certificates

3.11.1 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.

- SE050E/F/Dev Kit E and F variant
- SE050A/D/C/Dev Kit C variant
- SE050B

3.11.2 Attestation RSA

- Root
  - Intermediate

3.11.3 Attestation ECC

- Root
  - Intermediate

3.11.4 Cloud Onboarding RSA

- Root
  - Intermediate
    - SE050C1
    - SE050C2
    - SE050F2/Dev Kit F variant
    - Development Kit C variant

3.11.5 Cloud Onboarding ECC

- Root
  - Intermediate
    - SE050E2/Dev Kit E variant
    - SE050F2/Dev Kit F variant
    - ~~SE050C1~~
    - ~~SE050C2~~
    - Development Kit C variant

3.11.5.1 SE050 certificates revocation

The crossed out intermediate certificates above have been revoked.

Table 13 shows the SE050 variant and corresponding intermediate certificate.

Table 13. SE050 variants

SE050 Variant	Common Name of Intermediate Certificate
SE050C1HQ1/Z01SCZ	CloudConn-Intermediate-040050010001A200-ECC
SE050C2HQ1/Z01SDZ	CloudConn-Intermediate-040050010001A201-ECC

The underlying signed leaf certificates in the devices have the following ID:

- File: 0xF0000101 (Device individual)
- File: 0xF0000103 (Device individual)

These leaf certificates shall not be trusted. This means, that they should not be used to establish secure communication nor authenticate a SE050C device.

However, the underlying public keys with the following IDs can be trusted:

- 0xF0000100
- 0xF0000102

Furthermore, these product variants contain other die individual certificates which can be trusted.

The following certificates present in the SE050C configuration can be trusted:

Table 14. SE050C trusted certificate

Certificate Identifier
0xF0000001 [1]
0xF0000003 [1]
0xF0000111
0xF0000113
0xF0000121
0xF0000123

[1] These certificates are also used for the NXP EdgeLock 2GO services. Take this into consideration in case of deletion of these certificates.

Use a certificate/key from Table 14 different that is than File: 0xF0000101 or File: 0xF0000103 to authenticate the SE050 device, due to the intermediate certificate

revocation mentioned above. After successful authentication, only communication channels based on one of these certificates shall be trusted and used.

3.12 SE050 Chain of Trust for EdDSA certificates

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

3.12.1 Cloud Onboarding Ed25519

- Root
  - Intermediate

3.12.2 Attestation Ed25519

- Root
  - Intermediate

3.13 Secure objects configuration

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

Table 15. 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
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
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

Table 15. 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
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

3.14 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 16. 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)

4 References

[1] SE050 IoT Applet APDU Specification, document number AN12413. Available on NXP website.

[2] SE050E - User Guidelines, document number AN13483. Available on NXP website.

[3] SE050F - User Guidelines, document number AN13482. Available on Docstore.

[4] SE050 - User Guidelines, document number AN12514, v.1.4. Available on NXP website.

[5] SE050 - User Guidelines, document number AN12514, v.1.5. Available on Docstore.

[6] SE051 IoT applet APDU Specification, document number AN12543. Available on NXP website.

5 Legal information

5.1 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.

5.2 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 http://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 data sheet 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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a 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.

5.3 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.

Tables

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 21 April 2022
Document identifier: AN12436
Document number: 543821