AN14277

SE052 Configuration Details

Rev. 1.0 — 25 March 2024 Application note

Document information

Information	Content
Keywords	SE052
Abstract	Definition of available SE052 configurations

1 Product Information

The SE052 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 SE05X 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 : `J3R6000373181200`
- The product OS Patch ID
  Example below : `0000000000000000`
- The product ROM ID
  Example below: `B3375FE9B5508BC4`
- The version of the Applet in the format xx.xx.xx (major.minor.patch). Example below: 7.2.22

```
nxp@raspberrypi:~/se_mw/release/04.05.00/simw-top_build/
raspbian_native_se050_t1oi2c/bin $ ./se05x_GetInfo
App   :INFO :PlugAndTrust_v04.05.00_20231201
App   :INFO :Running ./se05x_GetInfo
App   :INFO :If you want to over-ride the selection, use
 ENV=EX_SSS_BOOT_SSS_PORT or pass in command line arguments.
sss   :INFO :atr (Len=35)
01 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 00
01 00 00 00 00 64 13 88 0A 00 65 53 45 30 35 31
00 00 00
App   :WARN :#####################################################
App   :INFO :uid (Len=18)
      04 00 50 01    0B 1B 6C 1C    D0 8E 10 04    2C 02 11 B5
      89 90
App   :INFO :Running ./se05x_GetInfo
App   :INFO :If you want to over-ride the selection, use
 ENV=EX_SSS_BOOT_SSS_PORT or pass in command line arguments.
sss :INFO :atr (Len=35)
01 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 00
01 00 00 00 00 64 13 88 0A 00 65 53 45 30 35 31
00 00 00
sss :INFO :Newer version of Applet Found
sss :INFO :Compiled for 0x70200. Got newer 0x70216
sss   :WARN :Communication channel is Plain.
sss   :WARN :!!!Not recommended for production use.!!!
App :WARN :#####################################################
App   :INFO :Applet Major = 7
App   :INFO :Applet Minor = 2
App   :INFO :Applet patch = 22
App   :INFO :AppletConfig = 26F2
App   :INFO :With    ECDSA_ECDH_ECDHE
App   :INFO :WithOut EDDSA
App   :INFO :WithOut DH_MONT
App   :INFO :With    HMAC
App :INFO :With RSA_PLAIN
App :INFO :With RSA_CRT
```

```
App :INFO :With AES
App :INFO :WithOut DES
App :INFO :With PBKDF
App :INFO :With TLS
App :INFO :WithOut MIFARE
App :INFO :With I2CM
App :INFO :Internal = FFFF
App   :WARN :#####################################################
App   :INFO :Tag value - proprietary data 0xFE = 0xFE
App   :INFO :Length of following data 0x45 = 0x4F
App   :INFO :Tag card identification data (Len=2)
      DF 28
App   :INFO :Length of card identification data = 0x4C
App   :INFO :Tag configuration ID (Must be 0x01) = 0x01
App   :INFO :Configuration ID (Len=12)
      00 05 B5 01    1B 7D B8 1B    89 99 D0 5D
App   :INFO :OEF ID (Len=2)
      B5 01
App   :INFO :Tag patch ID (Must be 0x02) = 0x02
App   :INFO :Patch ID (Len=8)
      00 00 00 00    00 00 00 00
App   :INFO :Tag platform build ID1 (Must be 0x03) = 0x03
App   :INFO :Platform build ID (Len=24)
4A 33 52 36 30 30 30 33 37 33 31 38 31 32 30 30
6D 20 B6 19 7D 63 5E 7C
App :INFO :JCOP Platform ID = J3R6000373181200
App :INFO :Tag FIPS mode (Must be 0x05) = 0x05
App :INFO :FIPS mode var = 0x01
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)
B3 37 5F E9 B5 50 8B C4
App :INFO :Tag JCOP OS Core ID (Must be 0x0A) = 0x0A
App :INFO :JCOP OS Core (Len=8)
55 60 6F D4 BE EC F3 CD
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)
      D6 00
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)
      32 99
App   :INFO :cplc_data.IC_Serial_number (Len=4)
      00 00 08 95
App   :INFO :cplc_data.IC_Batch_identifier (Len=2)
      73 25
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 2C
App :INFO :cplc_data.IC_OS_initialization_date (Len=2)
02 30
App :INFO :cplc_data.IC_OS_initialization_equipment (Len=4)
30 30 30 38
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 SE052F preconfigured variant for ease of use

2.1 General description

EdgeLock SE052F comes with preintegrated IoT applet. This variant with preintegrated IoT applet is offered off-the-shelf preprovisioned for ease of use. This ease of use 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 (for example 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 NXP website. Also see EdgeLock SE05x IoT Applet APDU Specification. EdgeLock SE052F FIPS certified is the only released variant.

2.1.1 IoT applet configurations

Table 1. IoT applet configurations

Categories		SE052F
ECC crypto schemes	ECDSA	x
	ECDH	x
	ECDHE	x
Supported elliptic curves	ECC NIST (192 bit to 521 bit)	x (>=224 bit)
	Brainpool (160 bit to 512 bit)	x (>=224 bit)
	Koblitz (160 bit to 256 bit)	x (>=224 bit)
RSA	RSA (up to 4096 bit)	x (2048 bit, 3072 bit, 4096 bit)
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	SHA1, SHA-224, SHA-256, SHA-384, SHA-512	x
MAC	HMAC, CMAC, GMAC	x
Key derivation (KDF)	TLS (KDF, PSK)	x
	PBKDF2	x
	HKDF	x
Secure channel	Secure Channel Host-SE (Platform SCP)	x (mandatory)
TRNG		NIST SP800-90B, AIS31
DRBG		NIST SP800-90A, AIS20
Memory reliability	up to 120 million write cycles / 25 years	x
User memory NVM		100 kB
User memory - RAM (Clear on deselect)		1100 bytes
Pre-provisioned		x

Table 1. IoT applet configurations...*continued*

Categories		SE052F
Interfaces	Contactless: ISO/IEC 14443 passive, type A	x
	I^2C target, up to 3.4 Mbit	x
	I^2C controller, Fast Mode (400 kbit/s)	x
	Contact: ISO 7816 UART	x
Power-saving modes	Power down (with state retention), ~610 µA (I^2C)	x
	Deep power down (no state retention), <15 µA	x
Temperature	Extended, -40 °C to 105 °C	x
Packaging	Plastic QFN, 4 mm × 4 mm (HVQFN20)	x

Note: *SEMS Lite for applet update is available in the SE052F. However, updating the applet makes the parts non-FIPS compliant.*

2.2 Variant identifier

The identifying information can be read out using the example "get info" from SE052 Plug&Trust MW package. This variant identifier is also known as OEF ID. This will allow to distinguish the delivered configuration.

Table 2. Variant identifiers

Variant	Variant identifier (OEF ID)	Applet version
SE052F	0xB501	IoT 7.2.22

2.3 Common keys

The keys in Table 3 are present in all configurations.

For the value of the Platform SCP keys (set as default in key set 11), please refer to Table 4.

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 SE052 product is deployed in production. For generic products, NXP own the recovery key set. These recovery keys are die individual. 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 3. 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
Mandate platform SCP	Enforce mandatory use of platform SCP	N/A	No	0x7FFF0207

Table 4. Default Platform SCP keys

Configurat	Platform	Key	OEF ID
SE052F	ENC	3ae441c747e32ebc16b3bb2d843c6dd8	0xB501
	MAC	6c18f3d08fee1cb96a3c8de5d3538aaa	
	DEK	b0e6a5697dbd929243a482cf9e4d6522	

2.3.1 NXP reserved keys and objects

Table 5. 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 6. NXP reserved keys and objects for FIPS self-tests

Key name	Erasable by customer	Identifier	Comment
RESERVED_ID_SELFTEST_INFO	No	0x7FFF020C	BinaryFile containing applet self-test information, Read only.
RESERVED_ID_SELFTEST_GCM_ENC_CMD	No	0x7FFF1000	
RESERVED_ID_SELFTEST_GCM_ENC_RESP	No	0x7FFF1001	
RESERVED_ID_SELFTEST_GCM_DEC_CMD	No	0x7FFF1002	
RESERVED_ID_SELFTEST_GCM_DEC_RESP	No	0x7FFF1003	
RESERVED_ID_SELFTEST_TLS_KDF_CMD	No	0x7FFF1004	
RESERVED_ID_SELFTEST_TLS_KDF_RESP	No	0x7FFF1005	
RESERVED_ID_SELFTEST_SP80056C_KDF_CMD	No	0x7FFF1006	
RESERVED_ID_SELFTEST_SP80056C_KDF_RESP	No	0x7FFF1007	
RESERVED_ID_SELFTEST_PBKDF2_CMD	No	0x7FFF1008	
RESERVED_ID_SELFTEST_PBKDF2_RESP	No	0x7FFF1009	
RESERVED_ID_SELFTEST_GCM_KEY	No	0x7FFF100A	
RESERVED_ID_SELFTEST_TLS_KDF_KEY	No	0x7FFF100B	
RESERVED_ID_SELFTEST_PBKDF2_KEY	No	0x7FFF100C	

2.4 Variant F

Table 7. Variant F

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	No	0xF0000110 (key) 0xF0000111 (cert)
Cloud connection key 1, RSA2048, Die Individual	Cloud Connectivity Certificate 1, RSA Signed	Default	No	0xF0000112 (key) 0xF0000113 (cert)
Cloud connection key 0, ECC256, Die Individual	Cloud Connectivity Certificate 0, ECC signed	Default	No	0xF0000100 (key) 0xF0000101 (cert)
Cloud connection key 1, ECC256, Die Individual	Cloud Connectivity Certificate 1, ECC Signed	Default	No	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	No	0xF0000120 (key) 0xF0000121 (cert)
RSA Key, RSA4096	Cloud Connectivity Certificate 1, RSA Signed	Default	No	0xF0000122 (key) 0xF0000123 (cert)

[1] Certificates are always erasable by customer

SE052F has been FIPS 140-3 certified with Security Level 3 for OS and Applet, and Security Level 4 related to Physical Security of the HW. The SE052F requires a specific configuration according to the certification, as indicated in Table 1. Some features are not available, such as:

- RSA 1024 Bit
- SHA1 digital signature
- ECC Keys below 224B

Furthermore, the following applies for SE052F:

• 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 4 MUST be updated.

For the SE052F Variant the Product Information according to Section 1 is:

- The product OS configuration (Platform build ID): J3R6000373181200
- The product OS Patch ID: 0000000000000000
- The product ROM ID: B3375FE9B5508BC4
- The version of the Applet (major.minor.patch): 7.2.22

In order to use the SE052F, NXP recommends to use the respective user guidelines for the SE052F in NXP website.

2.5 SE052 chain of trust certificates

2.5.1 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.

- SE052F

2.5.2 Attestation RSA

- Root
  - Intermediate

2.5.3 Attestation ECC

- Root
  - Intermediate

2.5.4 Cloud onboarding RSA

- Root
  - Intermediate
    - SE052F

2.5.5 Cloud Onboarding ECC

- Root
  - Intermediate
    - SE052F

2.6 Secure objects configuration

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

Table 8. Secure objects configuration

Object ID	Plurality*	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
0x7FFF0201	DI	32	EC_KEY_PAIR	Yes	Default	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0202	DI	32	EC_KEY_PAIR	Yes	Default	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0204	TI	32	EC_PUB_KEY	Yes	Default	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0206	DI	18	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF0207	TI	16	AES_KEY	Yes	Default	0x00	0x00	N/A	NA	0x00000000	PROVISIONED
0x7FFF020B	TI	1024	BINARY_FILE	No	0x7FFF0204 WRITE DELETE	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF020C	TI	16	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1000	TI	117	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1001	TI	88	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1002	TI	135	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1003	TI	73	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1004	TI	102	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1005	TI	56	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1006	TI	163	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1007	TI	40	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1008	TI	63	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF1009	TI	67	BINARY_FILE	No	0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF100A	TI	16	AES_KEY	No	0x00000000 READ ENC DEC	N/A	N/A	0x10	N/A	0x00000000	PROVISIONED
0x7FFF100B	TI	48	HMAC_KEY	No	0x00000000 READ TLS_KDF_EXT_RANDOM	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0x7FFF100C	TI	22	HMAC_KEY	No	0x00000000 READ PBKDF	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0003394	DI	32	AES_KEY	No	0x00000000 WRAP	N/A	N/A	0x10	N/A	0x00000000	PROVISIONED
0xF0000020	TI	32	EC_PUB_KEY	Yes	0xF0000020 READ WRITE 0x00000000 READ	0x00	0x00	N/A	N/A	0x00000000	PROVISIONED
0xF0000012	DI	32	EC_KEY_PAIR	No	0x00000000 READ ATTESTATION	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED

Table 8. Secure objects configuration*...continued*

Object ID	Plurality*	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
0xF0000013	DI	467	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000010	DI	256	RSA_KEY_ PAIR_CRT	No	0x00000000 READ ATTESTATION	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000011	DI	863	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000000	DI	32	EC_KEY_PAIR	No	0xF0000020 READ WRITE GEN 0x00000000 SIGN VERIFY READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000002	DI	32	EC_KEY_PAIR	No	0xF0000020 READ WRITE GEN 0x00000000 SIGN VERIFY READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000001	DI	470	BINARY_FILE	No	0xF0000020 READ WRITE 0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000003	DI	470	BINARY_FILE	No	0xF0000020 READ WRITE 0x00000000 READ	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000100	DI	32	EC_KEY_PAIR	No	0xF0000020 READ WRITE 0x00000000 SIGN VERIFY READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000102	DI	32	EC_KEY_PAIR	No	0xF0000020 READ WRITE 0x00000000 SIGN VERIFY READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000110	DI	256	RSA_KEY_ PAIR_CRT	No	0xF0000020 READ WRITE 0x00000000 ENC DEC READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000112	DI	256	RSA_KEY_ PAIR_CRT	No	0xF0000020 READ WRITE 0x00000000 ENC DEC READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000120	DI	512	RSA_KEY_ PAIR_CRT	No	0xF0000020 READ WRITE 0x00000000 ENC DEC READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000122	DI	512	RSA_KEY_ PAIR_CRT	No	0xF0000020 READ WRITE 0x00000000 ENC DEC READ	N/A	N/A	N/A	N/A	0x00000000	PROVISIONED
0xF0000101	DI	549	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000103	DI	549	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000111	DI	1206	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000113	DI	1206	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000121	DI	1462	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL
0xF0000123	DI	1462	BINARY_FILE	No	Default	N/A	N/A	N/A	N/A	0x00000000	EXTERNAL

Note: *Plurality is one of the following values: DI = die individual, TI = type individual*

2.7 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 9. 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)

3 References

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-Share Key
RSA	Rivest-Shamir-Adleman
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TPM	Trusted Platform Module

4 Note about the source code in the document

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

Copyright 2024 NXP Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials must be provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5 Revision history

Table 10. Revision history

Document ID	Release date	Description
AN14277 v.1.0	25 March 2024	• 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.

Contents

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

Date of release: 25 March 2024
Document identifier: AN14277