AN12436

SE050 configurations

Rev. 1.6 — 30 March 2021 Application note

543816

Document information

Information	Content
Keywords	SE050
Abstract	Definition of available SE050 configurations

Revision history

Revision history

Revision number	Date	Description
1.6	2021-03-30	• updated Section 2.4 • updated Section 2.5 • updated Section 2.6
1.5	2020-12-16	• updated legal disclaimer • updated Table 1 • add Section 2.7
1.4	2020-08-27	• Added section Section 2.3 • Minor changes
1.3	2020-07-08	added variant SE050D2 in • Table 1 • Section 2.4 update key description in Table 2
1.2	2020-02-27	added Section 2.7.1
1.1	2019-11-27	updated Table 3
1.0	2019-10-11	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 Configuration Table

Table 1. SE050 configuration

		SE050A1 SE050A2 SE050D2	SE050B1 SE050B2	SE050C1 SE050C2	OM-SE050ARD Dev Kit
RSA	RSA (up to 4096)		x	x	x
Supported Elliptic Curves	NIST (192 to 521 bit)	x		x	x
	Brainpool (160 to 512 bit)	x		x	x
	Koblitz (160 to 256 bit)	x		x	x
	Barreto-Naehrig (256 bit)			x	x
	Twisted Edwards (Ed25519)			x	x
	Montgomery (Curve25519)			x	x
ECC Crypto Schemes	ECDSA	x		x	x
	ECDH	x		x	x
	ECDHE	x		x	x
	ECDAA			x	x
	EdDSA			x	x
Symmetric Crypto Algorithm	3DES (2K, 3K)	x	x	x	x
	AES (128, 192, 256)	x	x	x	x
Hash Function	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	x	x	x	x
MAC	HMAC, CMAC	x	x	x	x
Key Derivation (KDF)	TLS KDF, TLS PSK	x	x	x	x
	MIFARE DESFire KDF	SE050D2 only		x	x
	Wi-Fi KDF (PBKDF2)	x	x	x	x
	OPC_UA KDF	x	x	x	x
TPM Functionalities		x	x	x	x
Pre-Provisioned		x	x	x	x
Interfaces	I2C Slave	x	x	x	x
	I2C Master			x	x
	ISO14443 CL			x	x
Temperature Range		• **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	-40 to +105 °C

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

2.1 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.

2.2 Common keys

The keys in Table 2 are present in all configurations.

For the value of the Platform SCP please refer to Table 3.

Table 2. 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 3. Default Platform SCP keys

Configuration	ENC	MAC	DEK
SE050A1	34AE0967E329E9518E7265D5ADCC01C2	52B253CADF472BDB3D0FB38E09770099	ACC91431FE26811B5ECBC845620D8344
SE050A2	46A9C48C34EFE344A522E66744F8996A	1203FF61DFBC9C86196A2274AEF4ED28	F7561C6F48336119EE39439AAB34098E
SE050D2	DE4A88D78478C5ECB4BC6E0528E370BF	DA947FC73A4C192AECBBE4F568930AEA	5120E50A8BC83BD37E99A5DCA76F8250
SE050B1	D499BC90DEA542CF78D25E13D64CBB1F	0815559643FB79EB8501A0DC833D901F	BE7DDFB406E81AE4E9665A9FED64267C
SE050B2	5FA43D8202D25E9A85B1FE7E2D26478D	105CEA2219F52BD167A07463C69379C3	D7028157F2AD372C74BE969BCC390627
SE050C1	852B5962E9CCE5D0BE746B833BCC6287	DB0AA319A408696C8E107AB4E3C26B47	4C2F75C6A278A4AEE5C9AF7C50EEA80C
SE050C2	BD1DE20A81EAB2BF3B709A9D69A31254	9A761B8DBA6BEDF22741E45D8D4236F5	9B993B600F1C64F5ADC063192A96C947
Development Board	35C256458958A34F6136155F8209D6CD	AF177D5DBDF7C0D5C10A05B9F1607F78	A1BC8438BF77935B361A4425FE79FA29

2.2.1 NXP reserved keys

Table 4. 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

2.2.2 Variant identifier

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

Table 5. Variant identifiers

Variant	Variant Identifier (OEF ID)
SE050A1	A204
SE050A2	A205
SE050D2	A43B
SE050B1	A202
SE050B2	A203
SE050C1	A200
SE050C2	A201
Development Board	A1F4

2.3 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.

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

2.4 Variant A / D

Table 6. 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)

Table 6. Variant A*...continued*

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

[1] Certificates are always erasable by customer

2.5 Variant B

Table 7. 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

2.6 Variant C

Table 8. 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)

Table 8. Variant C*...continued*

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

2.7 SE050 Chain of trust certificates

2.7.1 Iot Connectivity

- SE050A/D/C/Dev Kit
- SE050B

2.7.2 Cloud Onboarding RSA

- Root
  - Intermediate
    - SE050C1
    - SE050C2
    - Development Kit

2.7.3 Cloud Onboarding ECC

- Root
  - Intermediate
    - SE050C1
    - SE050C2
    - Development Kit

2.7.4 Attestation RSA

- Root
  - Intermediate

2.7.5 Attestation ECC

- Root
  - Intermediate

2.8 SE050 Chain of Trust for EdDSA certificates

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

2.8.1 Cloud Onboarding Ed25519

- Root
  - Intermediate

2.8.2 Attestation Ed25519

- Root
  - Intermediate

3 References

1. SE050 IoT Applet APDU Specification, document number AN 12413. Available on NXP website.

4 Legal information

4.1 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.

4.2 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.

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.

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 or documented vulnerabilities. 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.

4.3 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.

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: 30 March 2021
Document identifier: AN12436
Document number: 543816