SE051

Plug & Trust Secure Element

Rev. 1.4 — 28 March 2022
577314
Product data sheet

1 Introduction

The SE051 is a ready-to-use IoT secure element solution. It provides a root of trust at the IC level and it gives an IoT system state-of-the-art, edge-to-cloud security capability right out of the box.

SE051 is updatable on applet level for feature updates or security maintenance purposes.

SE051 allows for securely storing and provisioning credentials and performing cryptographic operations for security critical communication and control functions. SE051 is versatile in IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or protection of sensor data.

SE051 has an independent Common Criteria EAL 6+ security certification up to OS level and supports both RSA & ECC asymmetric cryptographic algorithms with high key length and future proof ECC curves. The latest security measures protect the IC even against sophisticated non-invasive and invasive attack scenarios.

The SE051 is a turnkey solution that comes with Java Card operating system and an updatable applet optimized for IoT security use cases pre-installed. This is complemented by a comprehensive product support package, enabling fast time to market & easy design-in with Plug & Trust middleware for host applications, easy to use development kits, reference designs, and extensive documentation for product evaluation.

The SE051 is a product platform that comes in several pin-to-pin compatible product variants, see [4].

Additional information on the integration can be found in several application notes on the NXP website. Also see [3].

For additional information on guidelines for the usability of SE051 and the security recommendations for using the module, see [7].

To implement inclusive language, the terms "master/slave" has been replaced by "controller/target", following the recommendation of MIPI.

1.1 SE051 use cases

- Secure connection to public/private clouds, edge computing platforms, infrastructure
- Device-to-device authentication
- Secure data protection
- Secure commissioning support
- Secure CL/MIFARE/Wi-Fi interactions
- Device ID for blockchain
- Secure key storage
- Secure provisioning of credentials

- Ecosystem protection
- Qi 1.3 wireless charging authentication

1.2 SE051 target applications

- Smart Industry
- Smart Home
- Smart Cities
- Smart Supply Chains

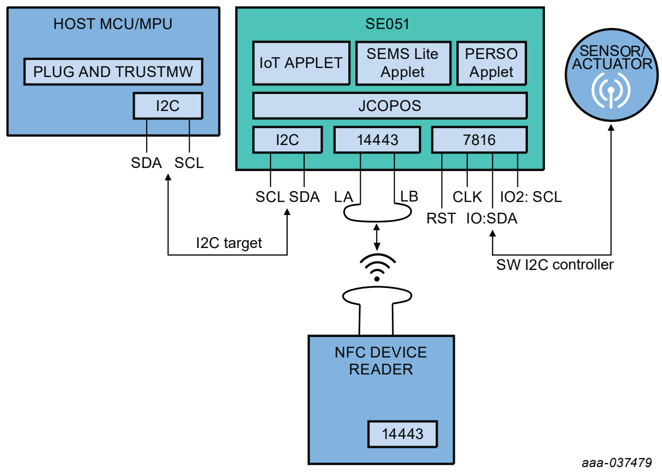


Figure 1. SE051 solution block diagram

Note: *SE051 is designed to be used as a part of an IoT system. It works as an auxiliary security device attached to a host controller. The host controller communicates with SE051 through an I²C interface (with the host controller being the controller and the SE051 being the target). Besides the mandatory connection to the host controller, the SE051 device can optionally be connected to a sensor node or similar element through a separate I²C interface. In this case, the SE051 device is the controller and the sensor node the target. Lastly, SE051 has a connection for a native contactless antenna, providing a wireless interface to an external device like a smartphone.*

1.3 SE051 naming convention

The following table explains the naming conventions of the commercial product name of the SE051 platform. Every SE051 product gets assigned a commercial name, which includes application specific data.

The SE051 commercial names have the following format.

SE05yagddd/Zrrff

All letters are explained in Table 1 .

Table 1. SE051 commercial name format

Variable	Meaning	Values	Description
y	JCOP version	1	

Table 1. SE051 commercial name format_...continued_

Variable	Meaning	Values	Description
a	Product Config	A C P	Configuration options with different key provisioning options, see [4]
g	Temperature range	1 2	standard operational ambient temperature 1 = -25 °C - 85 °C , 2 = -40 °C - 105 °C
ddd	Delivery Type	HQ1	HX2QFN20
Zrrff		Letters and numbers	NXP internal code to identify individual configurations

2 Features and benefits

2.1 Key benefits

- Plug & Trust for fast and easy design with complete product support package
- Updatability for feature upgrades and security maintenance in the field
- Easy integration with different MCU & MPU platforms and OSs (Linux, RTOS, Windows, Android, etc.)
- Turnkey solution ideal for system-level security without the need to write security code
- Secure credential injection for root of trust at IC level
- Secure, zero-touch connectivity to public & private clouds
- Real end-to-end security, from sensor to cloud
- Ready-to-use example code for each of the key use cases

2.2 Key features

The SE051 is based on NXP's Integral Security Architecture 3.0 providing a secure and efficient protection against various security threats. The efficiency of the security measures is proven by a Common Criteria EAL6+ certification.

Dependent on the ordered product configuration the feature set can vary. For more information, see [4]. Within this document the superset is described.

- SE051A/C includes pre-installed IoT applet for fast deployment
- SE051P supports proprietary applet development for custom products
- SE051W for secure UWB ranging comes with related applets and the IoT applet pre-installed

The SE051 operates fully autonomously based on an integrated Javacard operating system and applets. Direct memory access is possible by the fixed functionalities of the NXP IoT applet only. With that, the content from the memory is fully isolated from the host system.

- Built on NXP Integral Security Architecture 3.0
- CC EAL 6+ certified HW and OS as environment to run NXP IoT applications, supporting fully encrypted communications and secured lifecycle management
- SESIP Level 3 certified with full physical attack resistance for the NXP IoT applications and secure lifecycle management
- Suitable for industrial IoT use cases with IEC62443-4-2 certified for the applicable requirements and product development lifecycle is compliant to IEC62443-4-1 certified secure process with maturity level 3
- Effective protection against advanced attacks, including Power Analysis and Fault Attacks of various kinds
- Multiple logical and physical protection layers, including metal shielding, end-to-end encryption, memory encryption, tamper detection
- Applet updatability feature for multicast applet updates or upgrades and additional applet loading in the field (see [8])
- Support for secure UWB ranging in combination with Trimension products (FIRA compliant)
- Matter Ready: SE051 provides the necessary cryptographic functions to support the upcoming Matter standard for connecting smart home devices.

- Support for RSA and ECC asymmetric cryptography algorithms, future proof curves and high key length, e.g. Brainpool, Edwards and Montgomery curves
- Support for AES and DES symmetric cryptographic algorithms for encryption and decryption
- Support for AES Modes:CBC, ECB, CTR, GCM, CCM
- HMAC, CMAC, GMAC, SHA-1, SHA-224/256/384/512 operations
- Various options for key derivation functions, including HKDF, MIFARE KDF, PRF (TLS-PSK)
- Optional extended temperature range for industrial applications (-40 °C to +105 °C)
- Small footprint HX2QFN20 package (3x3 mm)
- Standard physical interface I^2C target (High-speed mode, 3.4 Mbit/s), I^2C controller (Fast mode, 400 kbit/s). Both can be active at the same time
- Dedicated ISO14443-A passive contactless wireless interface for IoT use cases simplifying configuration set-up, maintenance in the field and late stage configuration
- Secured user flash memory ranging from 45 kB full featured up to 101 kB for secure data or key storage
- Support for SCP03 protocol (bus encryption and encrypted credential injection) to securely bind the host with the secure element
- TRNG compliant to NIST SP800-90B
- DRBG compliant to NIST SP800-90A
- Support for applet level secure messaging channels to allow end-to-end encrypted communication in multi-tenant ecosystems
- Support for automatic detection of the I^2C T=1 protocol implementation based on the initial message prologue. Supported protocols:
  – NXP SE05x T=1 Over I^2C Specification. See [1].
  – APDU Transport over SPI/I2C v1.0 | GPC_SPE_172. See [6].

3 Functional description

3.1 Functional diagram

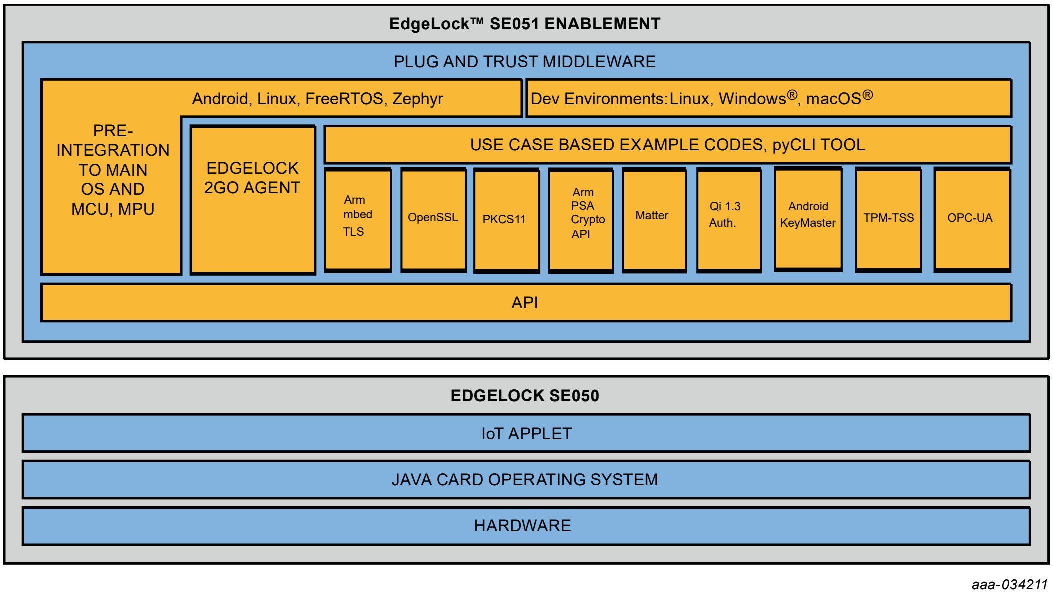


Figure 2. SE051 functional diagram - example Open SSL

The SE051 uses I^{2}C as communication interface. Section 4 gives more details. The SE051 commands are wrapped using the Smartcard T=1 over I^{2}C (T=1o I^{2}C) protocol or the APDU Transport over SPI/I^{2}C v1.0 | GPC_SPE_172. Per default automatic detection of the I^{2}C T=1 protocol implementation based on the initial message prologue is activated. The detailed documentation of the SE051 commands (see [3]) and T=1 over I^{2}C protocol encapsulation is available on [1]. You may also check the APDU Transport over SPI/I2C v1.0 | GPC_SPE_172, in [5].

In order to simplify the product usage a middleware which abstracts for SE051 commands and T=1 over I^{2}C protocol encapsulation is provided. The host library supporting various platforms is available for download including complete source code on the SE051 website.

SE051 IoT applet features a generic file system capable of securely storing secure objects and associated privilege management. All objects can either be stored in persistent memory or in RAM with the capability to securely export and import them to be stored in an externally provided storage. All secure objects feature basic file operations such as write, read, delete and update.

3.2 IoT Applet Functionality

3.2.1 Supported secure object types

A secure object is an entry in the file system of SE051. Each secure object has certain features and capabilities. The following secure object types are available (for more details on the objects refer to [3]:

- Symmetric Key (AES, 3DES)
- ECC Key
- RSA Key
- HMAC Key
- Binary File
- User ID
- Counter
- Hash-Extend register

3.2.2 Access control

Each secure object can be linked to object specific access control policies. An access control policy associates a user identified by an authentication with a set of privileges such as read, write, allowed cryptographic operations and more. For details refer to [3].

To scale the functionality into a broad range of ecosystems, a set of different authentication options is provided:

- User-ID based authentication
- Symmetric key based authentication with secure messaging
- Asymmetric key based authentication with secure messaging
  At creation of a secure object, an optional set of policies is associated with that secure object. Each policy assigns a set of allowed operations on that object to an authentication object.

3.2.3 Locking the Device Configuration

The creation of new secure objects as well as the deletion or modification of existing secure objects can be controlled via a credential.

3.2.4 Sessions and multi-threading

The SE051 IoT applet is prepared for ecosystems where multi-threading and multi-tenant use cases are needed on APDU level. To enable that, the applet supports 2 simultaneous sessions that can span full secure messaging sessions, self-authenticated APDUs for tenants not requiring long-lasting sessions and on top one default session for single tenant use cases .

3.2.5 Attestation and trust provisioning

SE051 applet comes with a set of trust provisioned root credentials allowing the owner of the device to securely attest all generated secure keys. Next to that, a customer has the possibility to define own attestation keys.

Attestation certificates signed by an attestation CA are included in certain SE051 configs as documented in [4].

3.2.6 Application support

For specific ecosystems, SE051 IoT applet has built-in crypto features to simplify the deployment of specific use cases such as

- MIFARE SAM functionality
- Wi-Fi password protection

- ECC-Key and RSA-Key based cloud connectivity (TLS)
- Secure Sensor readout using I^2C controller
- Remote attestation and trust provisioning
- Platform Configuration Registers

3.2.7 Random numbers

The SE051 IoT Applet provides random numbers using an AIS20 compliant pseudo random number generator (PRNG) with class DRG.3 generator initialized by a TRNG compliant to NIST SP800-90B class PTG.2. The PRNG is implemented according to NIST SP800-90A.

3.2.8 Credential Storage & Memory

Within SE051, all credentials and secure objects are stored inside a dynamic file structure. At creation, a user has to associate a file identifier with the object created. This identifier is then used in subsequent operations to access the object. The number of objects that can be allocated is only limited by the available memory in the system. After usage, objects can be deleted and the associated memory is freed up again.

There is also the possibility to create transient objects. Transient objects have an object descriptor stored in non-volatile memory, but the object content is stored in RAM. Together with the import/export functionality of SE051, transient objects can be used securely store secret keys in a remote memory system.

3.3 PERSO applet

The NXP Perso applet provides the possibility to reconfigure SE051 devices. The configuration options include communication parameter settings of I2C, ISO14443 and ISO7816 interface as well as the deletion of unused operating system (cryptography) modules in order to gain additional credential memory. Please refer to [6] for details.

3.4 SEMS Lite

SEMS Lite is a capability built in SE051. NXP may issue security updates at its discretion. OEMs can leverage SEMS to deploy these applet updates in the field, after having fully assessed impact, as well as tested and validated the update on their product.

Security upgrades including an upgrade of functionality of SE051 are subject to commercial agreements with NXP on a case by case basis and are only available on specific SE051 variants.

3.5 Applet Updatability

The Applet Updatability feature is introduced with SE051 enabled by the SEMS-Lite feature and provides upgrade functionality of applets whilst preserving on device credentials. This can be used for security maintenance in the field by enabling applet updates with additional security features or bug fixes. This feature can also be used to upload additional applets in the field. See [8].

On the P Product Configuration, this features is leveraged to allow customer applet development on the SE051.

3.6 Secure UWB ranging

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 logical 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. SE051W is based on a SE051 product with the feature set listed in [4]. In addition, there is SUS and FiRa available for secure ranging.

For more information, see [4].

3.7 Ease of use configuration

SE051 variants with pre-provisioned credentials for ease of use are available and can be used during development phase or in the field. With this customers have all keys pre-injected in SE051 that are required for the main use cases as e.g. cloud onboarding. For more information, see: [4]

3.8 Startup behaviour

If a supply voltage is applied to pins V_{in}, V_{cc} within the specified supply voltage operating range or a RF field according to ISO/IEC 14443 is applied to antenna pins LA, LB the IC boots up.

During boot the IC checks for active interface according list below (in the order of the list):

- ISO7816: If interface available for this product type, check CLK to be toggling, then wait for RST to be high
- ISO14443: If interface available for this product type, check of RF field on LA, LB antenna pins
- I^2C: If interface available for this product type, check if both I^2C_SDA, I^2C_SCL pins are at high level (internal weak pull-up active)

The chosen interface is the only interface the SE051 will receive commands for processing. To select a different interface the IC needs to be reset.

4 Communication interfaces

4.1 I^2C Interfaces

The SE051 has one I^2C interface supporting target and one I^2C interface supporting controller mode.

The I^2C target interface is the main communication interface of the device and is used by the host controller to send arbitrary APDUs to the device. It supports clock frequencies up to 3.4 MHz when operated in High-Speed Mode (HS). The I^2C interface is using the Smartcard T=1 over I^2C protocol.

The default target address of the SE051 is configured to 0x48.

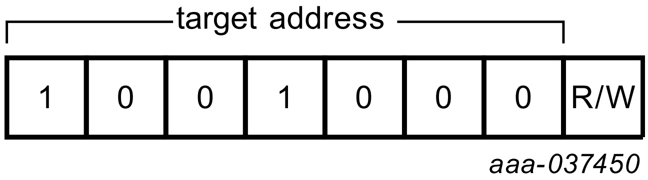


Figure 3. target address

The I^{2}C controller interface is supposed to be used with target devices that need to be securely written and read. This interface features a maximum SCL clock rate of 400 kHz.

I^{2}C controller can only be used when the I^{2}C target interface is active.

4.1.1 Supported I^{2}C frequencies

The SE051 I^{2}C target interface supports the I^{2}C high-speed mode with a maximum SCL clock of up to 3.4 MHz when clock stretching is enabled.

In case clock stretching is disabled the maximum supported SCL clock frequency is 1.0 MHz.

The SE051 I^{2}C controller interface supports maximum 400 kHz SCL clock frequency.

4.1.2 Default I^{2}C Communication Parameters

The default I^{2}C interface parameters of the SE051 devices are chosen with the highest compatibility in mind:

- The used I^{2}C protocol is detected automatically on the first received frame amongst the two possible protocols:
  - NXP SE05x T=1 Over I^{2}C Specification. See [1].
  - APDU Transport over SPI/I2C v1.0 | GPC_SPE_172. See [5].
- Clock Stretching is disabled, which allows SCL frequencies up to 1 MHz
- Automatically entering into the Power saving mode is disabled by default. Power down can be explicitly requested by the host via an "End of APDU session request" (according to [1]) respectively "RELEASE request" from GP T=1oI2C [5].

A In order to change the I^{2}C settings of the device the PERSO applet can be used.

4.2 ISO7816 and ISO14443 Interface

The SE051 supports in addition to the I^{2}C interface ISO7816 [1] and ISO14443 type A Smartcard interfaces. For the ISO7816 interface SmartCard protocols T=0 and T=1 are supported. For the ISO14443 interface protocol T=CL is used. The supported resonance input capacitance is 56 pF.

The RST_N pin can only be used as external reset source if the ISO7816 interface is enabled. If only the I^{2}C interface is enabled, the RST_N pad has no effect. If the SE051 is kept in reset state the current consumption is as defined for idle, see Table 11.

1 ISO7816 is not enabled in generic SE051 configurations (see [4], AN12973) but available on customer request.

5 Power-saving modes

The device provides two power-saving operation modes. The Power-down mode (with state retention) and the Deep Power-down mode (no state retention). These modes are activated via pad ENA (Deep Power-down mode) or by the SW (Power-down mode).

5.1 Power-down mode

The Power-down mode has the following properties:

- All internal clocks are frozen
- CPU enters power-saving mode with program execution being stopped
- CPU registers keep their contents
- RAM keeps its contents

The SE051 enters into Power-down mode by receiving "End of APDU session request" (according to [1]) respectively "RELEASE request" (according to GP T=1oI2C [5]. The automatic power down mode can be enabled using the PERSO applet. In Power-down mode, all internal clocks are frozen. The IOs hold the logical states they had at the time Power-down mode was activated.

To exit from the Power-down mode an external interrupt edge must be triggered by a falling edge on I^2C_SDA[2].

5.2 Deep Power-down mode

The SE051 provides a special power-saving mode offering maximum power saving. This mode is activated by pulling enable PIN (ENA) to a logic zero level.

While in Deep Power-down mode the internal power and V_{OUT} is switched off completely and only the I^2C pads stay supplied.

To leave the Deep Power-down mode pad ENA has to be pulled up to to a logic „1" level.

For usage of Deep Power-down mode the SE051 must be supplied via pin V_{in} and pin V_{cc} needs to be supplied by pin V_{out}.

6 Ordering information

Table 2. Ordering information

12NC	Type number	SE051 Variant	Orderable part number
935414457472	SE051C2HQ1/Z01XD	SE051C2	SE051C2HQ1/Z01XDZ
935414458472	SE051A2HQ1/Z01XE	SE051A2	SE051A2HQ1/Z01XEZ
935428464472	SE051W2HQ1/Z019T	SE051W2	SE051W2HQ1/Z019TZ
935409596472	SE051P2HQ1/Z011A	SE051P2	SE051P2HQ1/Z011AZ

2 In case ISO7816 is enabled a reset signal on RST_N exits the Power-down mode. After wake-up from Power-down mode via RST_N the device is in idle mode (see Table 11)

7 Pinning information

7.1 Pinning

7.1.1 Pinning HX2QFN20

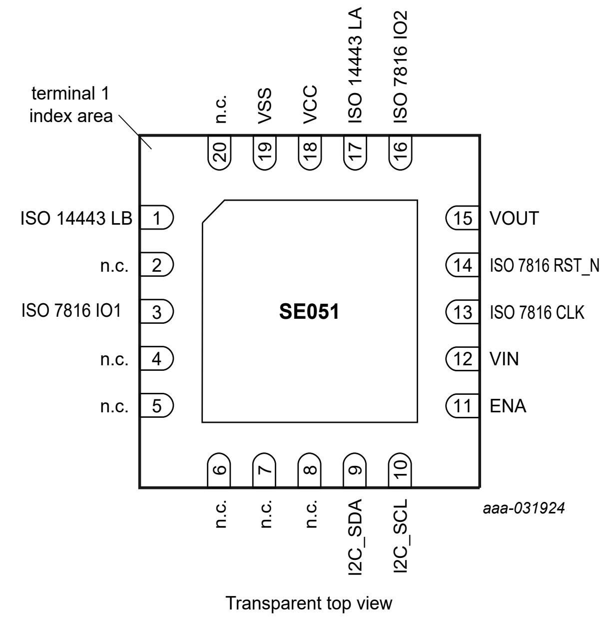


Figure 4. Pin configuration for HX2QFN20 (SOT1969-1)

Note: *Terminal 1 index area is marked on the bottom with a notch on the center pad and on the top with a printed dot.*

Table 3. Pin description HX2QFN20

Symbol	Pin	Description
ISO 14443 LB	1	ISO14443 Antenna Connection, if not used connect to V_{SS}
n.c.	2	not connected
ISO 7816 IO1	3	ISO 7816 IO or I^2C controller SDA, if not used n.c (recommended) or connect to V_{CC}
n.c.	4	not connected
n.c.	5	not connected
n.c.	6	not connected
n.c.	7	not connected
n.c.	8	not connected
I^2C_SDA	9	I^2C target data, if not used n.c.
I^2C_SCL	10	I^2C target clock, if not used n.c.
ENA	11	Deep Power-down mode enable, if not used then connect to V_{CC}
V_{IN}	12	power supply voltage input for I^2C pads and ISO 7816 interface and logic supply in case Deep Power-down mode is used

Table 3. Pin description HX2QFN20...*continued*

Symbol	Pin	Description
ISO 7816 CLK	13	ISO 7816 clock input, if not used then n.c (recommended) or connect to V_{CC}
ISO 7816 RST_N	14	ISO 7816 reset input low active, if not used then connect to Vcc or Vss
V_{OUT}	15	supply voltage output to be connected with pad V_{CC} on PCB level, if Deep Power-down mode is used. N. c. if not used.
ISO 7816 IO2	16	ISO7816 IO2 pad or I^2C controller SCL. I if not used n.c (recommended) or connect to V_{OUT}.
ISO 14443 LA	17	ISO14443 antenna connection, if not used then connect to V_{SS}
V_{CC}	18	logic and ISO7816/ISO14443 interface power supply voltage input, to be connected with pad V_{OUT} on PCB level, if Deep Power-down mode to be used
V_{SS}	19	ground
n.c.	20	not connected

The center pad of the IC is not connected, although it is recommended to connect it to ground for thermal reasons.

Reference voltage for ISO 7816 IO1, CLK, RST is V_{CC}; for I^2C SDL and SCL reference voltage is V_{IN} and for IO2 it is V_{OUT}.

8 Package

SE051 is offered in HX2QFN20 package. The dimensions are 3 mm x 3 mm x 0,32 mm with a 0,4 mm pitch.

Please refer to the package data sheet [2], SOT1969-1.

9 Marking

Table 4. Marking codes

Type number	Marking code
Sx051...	Line A: S51 Line B: **** (**** = 4-digit Batch code) Line C: nDyww D: RHF-2006 indicator n: Assembly Center Y: Year WW: Week

10 Packing information

10.1 Reel packing

The SE051 product is available in tape on reel.

Table 5. Reel packing options

Symbol	Parameter	Numbers of units per reel
HX2QFN20	7" tape on reel	3000

11 Electrical and timing characteristics

The electrical interface characteristics of static (DC) and dynamic (AC) parameters for pads and functions used for I^2C are in accordance with the NXP I^2C specification (see [1]).

12 Limiting values

Table 6. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134). Voltages are referenced to V_{SS} (ground = 0 V).

Symbol	Parameter	Conditions		Min	Max	Unit
V_{IN}, V_{cc}	supply voltage			-0.3	+6 [1]	V
V_I	input voltage	any signal pad		-0.3	+6	V
I_I	input current	pad I^2C_SDA, I^2C_SCL		-	10	mA
I_O	output current	pad I^2C_SDA, I^2C_SCL		-	10	mA
I_{lu}	latch-up current	V_I < 0 V or V_I > V_{IN}, V_{cc}		-	100	mA
V_{esd_hbm}	electrostatic discharge voltage (Human Body Model)	pads V_{CC}, V_{SS}, RST_N, I^2C_SDA, I^2C_SCL, IO1, IO2, CLK	[2]		± 2.0	kV
V_{esd_cdm}	electrostatic discharge voltage (Charge Device Model)	pads V_{CC}, V_{SS}, RST_N, I^2C_SDA, I^2C_SCL, IO1, IO2, CLK	[3]		± 500	V
P_{tot}	Total power dissipation		[4]	-	600	mW
T_{stg}	Storage temperature			-55	+125	°C

[1] Maximum supported supply voltage is 6 V. The SE051 is characterized for the specified operating supply voltage range of 1.62 V to 3.6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 µA is not guaranteed.
[2] MIL Standard 883-D method 3015; human body model; C = 100 pF, R = 1.5 kΩ; T_{amb} = -40 °C to +105 °C.
[3] JESD22-C101, JEDEC Standard Field induced charge device model test method.
[4] Depending on appropriate thermal resistance of the package.

13 Recommended operating conditions

The SE051 is characterized by its specified operating supply voltage range of 1.62 V to 3.6 V.

Table 7. Recommended operating conditions

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{IN}, V_{CC}	Supply voltage	Nominal supply voltage	1.62	1.8	3.6 [1]	V

Table 7. Recommended operating conditions*...continued*

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_I	DC input voltage on digital inputs and digital I/O pads	-	-0.3		V_{CC}/V_{IN} [2] +0.3	V
H	Field strength	Maximum field strength at ambient temperature <= 85 °C[3]	1.5		7.5	A/m
H	Field strength	Maximum field strength at ambient temperature 85...105 °C [3]	1.5		3.5	A/m
T_{amb}	Operating ambient temperature[4]		-40		+105	°C

[1] Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 μA is not guaranteed.
[2] IO1, CLK, RST has V_{CC} as reference, SDA, SCL, IO2 and ENA has V_{IN} as reference
[3] The field strength is valid for an Class 1 antennas.
[4] All product properties and values specified within this data sheet are only valid within the operating ambient temperature range.

Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 μA is not guaranteed.

Figure 5. Characteristic supply voltage operating range

14 Characteristics

14.1 Thermal Characteristics

Table 8. Thermal characteristics

Rating	Board Type [1]	Symbol	Value	Unit
Junction to Ambient Thermal Resistance [2]	JESD51-9, 2s2p	$R_{\theta JA}$	70.2	°C/W
Junction to Package Top Thermal [2]	JESD51-9, 2s2p	Ψ_{JT}	8.3	°C/W
Junction to Case Thermal Resistance [3]	JESD51-9, 1s	$R_{\theta JC}$	32.9	°C/W

[1] Thermal test board meets JEDEC specification for this package (JESD51-9)
[2] Determined in accordance to JEDEC JESD51-2A natural convection environment. Thermal resistance data in this report is solely for a thermal performance comparison of one package to another in a standardized specified environment. It is not meant to predict the performance of a package in an application-specific environment
[3] Junction-to-Case thermal resistance determined using an isothermal cold plate. Case is defined as the bottom of the packages (exposed pad)

14.2 DC characteristics

Measurement conventions

Testing measurements are performed at the contact pads of the device under test. All voltages are defined with respect to the ground contact pad VSS. All currents flowing into the device are considered positive.

14.2.1 General and General Purpose I/O interface

Table 9. Electrical DC characteristics of Input/Output: IO1/IO2. Conditions: V_{CC} = 1.62 V to 3.6 V (see ; V_{SS} = 0 V; T_{amb} = -40 °C to + 105 °C, unless otherwise specified

In Table 9 V_{CC} means for IO1 voltage on V_{CC} pin, for IO2 voltage on V_{IN} pin

Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 µA is not guaranteed.

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{IH}	HIGH level input voltage			0.7 V_{CC}		V_{CC} + 0.3	V
V_{IL}	LOW level input voltage			-0.3		0.25 V_{CC}	V
I_{IH}	HIGH level input current in "weak pull-up" input mode	0.7 $V_{CC} \le V_I \le V_{CC}$ Test conditions for the maximum absolute value: $I_{IH(max)}$:V_I = 0.7 V_{CC}, V_{CC}=$V_{CC(max)}$				-20	µA
I_{IL}	LOW level input current	0 V ≤ VI ≤ 0.3 V_{CC}; Test conditions for the maximum absolute value: $I_{IL(max)}$:V_I = 0 V, V_{CC} = $V_{CC(max)}$				-50	µA
I_{TL}	HIGH-to-LOW transition input current (only "quasi-bidirectional" mode)	0.3 $V_{CC} < V_I \le V_{CC}$; Test conditions for the maximum absolute value: V_I = 0.5 V_{CC}, V_{CC} = $V_{CC(max)}$	[1]			-250	µA
I_I	Input current in "weak pull-up" input mode	0 V ≤ V_I ≤ V_{CC}; Test conditions for the maximum absolute value: $I_{I(max)}$:V_I = 0 V, V_{CC} = $V_{CC(max)}$		0		-50	µA
I_{ILIH}	Leakage input current at input voltage beyond V_{CC} in "weak pull-up" input mode	$V_{CC} < V_I \le V_{CC}$ + 0.3 V; -40 °C ≤ T_{amb} ≤ +105 °C; Test conditions: V_I = V_{CC} + 0.3 V; V_{CC} = $V_{CC(max)}$$T_{amb}$ = +105 °C				20	µA
I_{ILIL}	Leakage input current at input voltage below V_{SS} in "weak pull-up" input mode	-0.3 V ≤ V_I < 0 V; -40 °C ≤ T_{amb} ≤ +30 °C; Test conditions: V_I = -0.3 V; V_{CC}= $V_{CC(max)}$$T_{amb}$ = +30 °C				-50	µA

Table 9. Electrical DC characteristics of Input/Output: IO1/IO2. Conditions: V_{CC} = 1.62 V to 3.6 V (see ; V_{SS} = 0 V; T_{amb} = -40 °C to + 105 °C, unless otherwise specified*...continued*

In Table 9 V_{CC} means for IO1 voltage on V_{CC} pin, for IO2 voltage on V_{IN} pin

Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 µA is not guaranteed.

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
		-0.3 V ≤ V_I < 0 V;+30 °C ≤ T_{amb} ≤ +105 °C Test conditions: V_I = -0.3 V; V_{CC}= $V_{CC(max)}$$T_{amb}$ = +105 °C				-1000	µA
I_{ILIHQ}	Leakage input current at input voltage beyond V_{CC} (only in "quasi-bidirectional" mode)	V_{CC} < V_I ≤ V_{CC} + 0.3 V; -40 °C ≤ T_{amb}≤ +105 °C Test conditions: V_I = V_{CC} + 0.3 V;V_{CC} = $V_{CC(max)}$; T_{amb} = +105 °C				100	µA
I_{ILILQ}	Leakage input current at input voltage below V_{SS} (only in "quasi-bidirectional" mode)	-0.3 V ≤ V_I < 0 V; -40 °C ≤ T_{amb} ≤ +30 °C Test conditions: V_I = -0.3 V; V_{CC} = $V_{CC(max)}$$T_{amb}$= +30 °C				-120	µA
		-0.3 V ≤ V_I < 0 V;+30 °C ≤ T_{amb} ≤ +105 °C Test conditions: V_I = -0.3 V; V_{CC} = $V_{CC(max)}$$T_{amb}$= +105 °C				-1000	µA
V_{OH}	HIGH level output voltage	I_{OH} = -20 µA;	[2]	0.7 V_{CC}			V
V_{OL}	LOW level output voltage	I_{OL} = 1.0 mA I_{OL} = 0.5 mA				0.3 0.15 V_{CC}	V

[1] IO1/IO2 source a transition current when being externally driven from HIGH to LOW. This transition current (I_{TL}) reaches its maximum value when the input voltage V_I is approximately 0.5 V_{CC}. Current IIL is tested at input voltage V_I= 0.3 V.

[2] External pull-up resistor 20 kΩ to V_{CC} assumed. The worst case test condition for parameter V_{OH} is present at minimum V_{CC}.

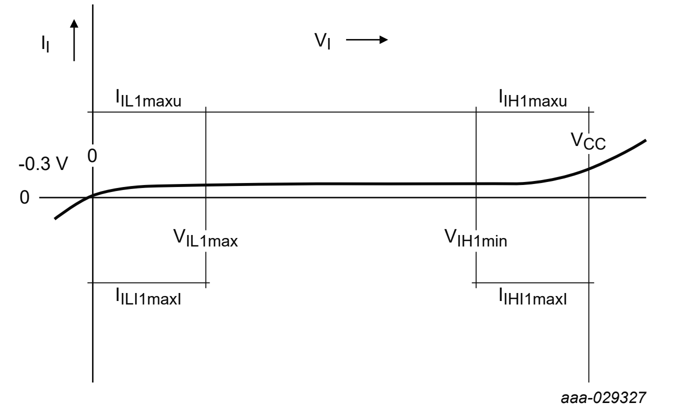


Figure 6. Input characteristic of RST_N

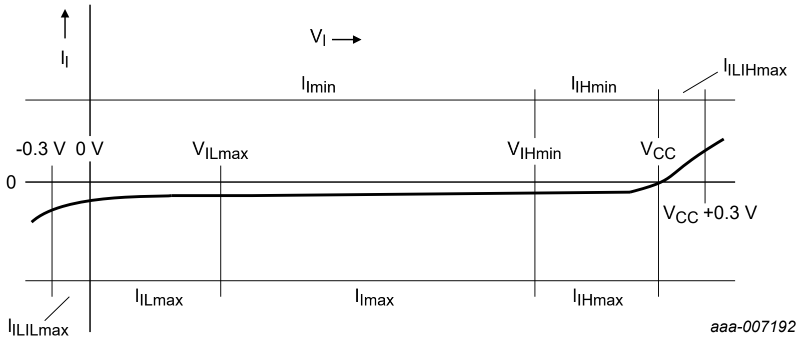


Figure 7. Input characteristic of IO1/IO2

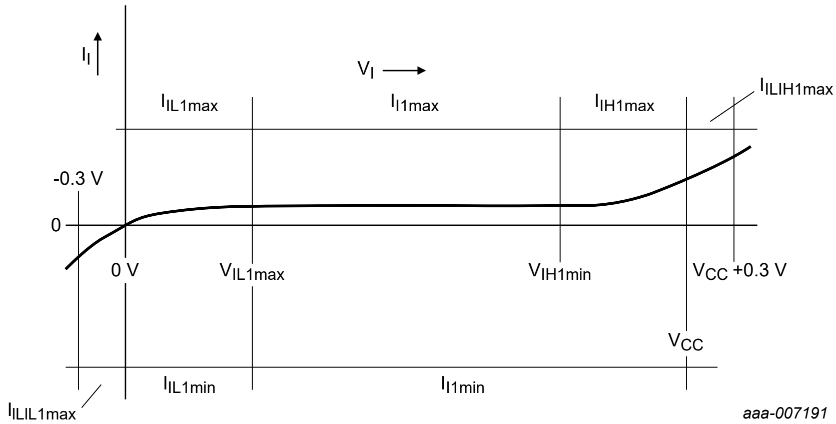


Figure 8. Input characteristic of CLK when the IC is not in reset

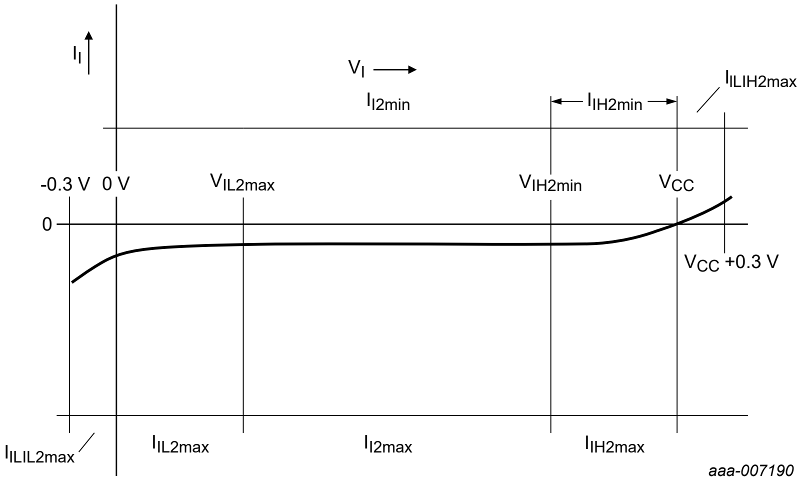


Figure 9. Input characteristic of CLK during IC reset

14.2.2 I²C Interface

Table 10. Electrical DC characteristics of I²C pads SDA, SCL. Conditions: V_{cc}, V_{IN} = 1.62 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to + 105 °C, unless otherwise specified*

Maximum supported supply voltage is 6 V. In case of supply voltages above 3.6 V, Deep Power-down mode current <5 µA is not guaranteed.

SSCL, SDA pads are in open-drain mode.

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{IH}	HIGH level input voltage			0.7 V_{IN}		V_{IN} + 0.3	V
V_{IL}	LOW level input voltage			-0.3		0.25 V_{IN}	V
V_{HYS}	Input hysteresis voltage	-		0.081 V			V
$V_{OL(OD)}$	Low level output voltage (open-drain mode)	I_{OL} = 3.0 mA		0		0.4	V
$I_{OL(OD)}$	Low level output current (open-drain mode)	V_{OL} = 0.6 V		0.6			mA
I_{WPU}	weak pull-up current	V_{IO} = 0 V		-265	-180	-70	µA
I_{ILIH}	Leakage input current high level	V_{SDA} = 3.6 V, V_{SCL} = 3.6 V			0.27	15	µA

14.2.3 Power consumption

Table 11. Electrical characteristics of IC supply voltage V_{CC}; V_{SS} = 0 V; T_{amb} = -40 °C to +105 C

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
Supply						
V_{CC}	supply voltage range	V_{CC} = 1.62 - 3.6 V	1.62	1.80	3.6	V
	operating mode: Idle mode					
I_{DD}	operating mode: typical CPU					
		during Communication	-	3.0	3.7	mA
		during non asymmetric crypto operation	-	6.5	7.5	mA

Table 11. Electrical characteristics of IC supply voltage V_{CC}; V_{SS} = 0 V; T_{amb} = -40 °C to +105 C*...continued*

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
		during asymmetric crypto operation	-	14.4	16.5	mA
$I_{DD\ (PD-ISO7816)}$	supply current Power-down mode (ISO7816 clock-stop)	$V_{CCmin} \leq V_{CC} \leq V_{CCmax;}$ Clock to input CLK stopped, T_{amb}= 25 °C		430	480	µA
$I_{DDD\ (DPD)}$	supply current Deep Power-down mode	$V_{CCmin} \leq V_{IN} \leq V_{CCmax;}$ T_{amb}= 25 °C		3	5	µA
$I_{DD\ (PD-I2C)}$	supply current I^2C Power-down mode (I^2C wake-up source)	$V_{CCmin} \leq V_{CC} \leq V_{CCmax}$; Clock to input SCL stopped, Tamb= 25 °C SDA, SCL pads in pull-up Typical value with V_{CC}= 1.8 V		450	500	µA

14.3 AC characteristics

Table 12. Non-volatile memory timing characteristics

Conditions: V_{CC} = 1.62 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to +105 °C, unless otherwise specified.

Symbol	Parameter	Conditions		Min	Typ[1]	Max	Unit
t_{EEP}	FLASH erase + program time		[2]		2.3		ms
t_{EEE}	FLASH erase time				0.9		ms
t_{EEW}	FLASH program time				1.4		ms
t_{EER}	FLASH data retention time	T_{amb} = +55 °C		25			years
N_{EEC}	FLASH endurance (maximum number of programming cycles applied to the whole memory block performed by NXP static and dynamic wear leveling algorithm)			20×10^6	100×10^6		cycles

[1] Typical values are only referenced for information. They are subject to change without notice.
[2] Given value specifies physical access times of FLASH memory only.

Table 13. Electrical AC characteristics of I^2C_SDA, I^2C_SCL, and RST_N[1]; V_{CC} = 1.8 V ± 10 % or 3 V ± 10 % V; V_{SS} = 0 V; T_{amb} = -40 °C to +105 °C°C

SCL, SDA pads in open-drain mode.

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
Input/Output: I^2C_SDA, I^2C_SCL in open-drain mode							
tr_{IO}	I/O Input rise time	Input/reception mode	[2]			1	µs
tf_{IO}	I/O Input fall time	Input/reception mode	[2]			1	µs
tf_{OIO}	I/O Output fall time	Output/transmission mode; C_L = 30 pF	[2]			0.3	µs
f_{CLK}	External clock frequency in I^2C applications	t_{CLKW}, T_{amb} and V_{CC} in their specified limits		-		3.4	MHz
t_{PD}	Power down duration time (I^2C wake-up)	CPU clock = 48 MHz	[3]		67		µs

Table 13. Electrical AC characteristics of I^2C_SDA, I^2C_SCL, and RST_N[1]; V_{CC} = 1.8 V ± 10 % or 3 V ± 10 % V; V_{SS} = 0 V; T_{amb} = -40 °C to +105 °C°C*...continued*

SCL, SDA pads in open-drain mode.

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
t_{WKPD}	Wake-up from power down duration time (I^2C wake-up)	CPU clock = 48 MHz	[4]		97		μs
C_{PIN}	Pin capacitances RST_N, I^2C_SDA, /I^2C_SCL	Test frequency = 1 MHz; Tamb = 25 °C		-		10.5	pF
t_{ENalt}	ENA low time and Vout, V_{cc} low time for entering deep power down mode		[5]		2		μs
R_{on}	Resistance of power switch	T_{amb}=105 °C, I_{load}=25 mA, V_{in}=1.62 V				1.1	Ohm
I_{out}	maximum current driving capability of pin V_{out}	T_{amb}=105 °C				25	mA
Inputs: RST_N (active only if ISO7816 UART interface is enabled)							
t_{RW}	Reset pulse width (RST_N low) without entering Power-down mode			40		400	μs
t_{RDSLP}	Reset pulse width (RST_N low) to enter Power-down mode			500			μs
t_{WKP}	Wake-up time from Power-down mode	$f_{CLKmin} < f_{CLK} < f_{CLKmax}$		-	8	10	μs
t_{WKPIO}	Pad LOW time for wake-up from Power-down mode	level triggered ext.int.		-	8	10	μs
		edge triggered ext.int.		-	8	10	μs
t_{WKPRST}	RST_N LOW time for wake-up from Power-down mode			40		-	μs
C_{PIN}	Pin capacitances RST_N, I^2C_SDA, /I^2C_SCL	Test frequency = 1 MHz; T_{amb} = 25 °C		-		10.5	pF

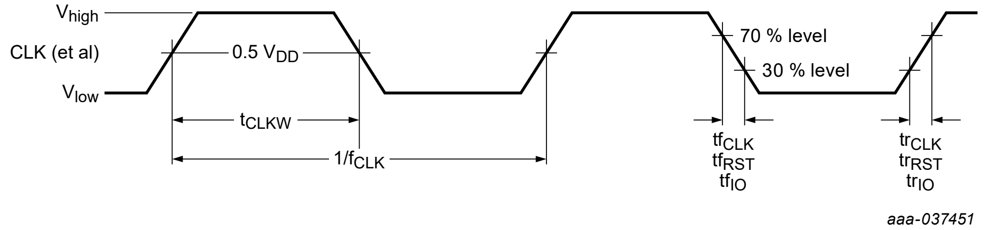
[1] All appropriately marked values are typical values and only referenced for information. They are subject to change without notice.

[2] t_r is defined as rise time between 30 % and 70 % of the signal amplitude.
t_f is defined as fall time between 70 % and 30 % of the signal amplitude.

[3] Wakeup from power down: if clock stretching disabled and I^2C_SCL=400 kHz; the wakeup time will not be sufficient under the rare condition where host sends the first command during the time where SE is just entering power down; in this case the SE will send an R block to request retransmission from the host.
SE051 (while using the GP T1I2C protocol [5]) will need to be restarted when the following conditions apply:
- An empty I2C write frame is sent
- A valid (non-empty) I2C write is sent while SE051 transitions into power down mode

[4] Wakeup from power down: if clock stretching disabled and I^2C_SCL=1 MHz; the wakeup time will not be sufficient to receive the first host command; the SE will send an R block to request retransmission from the host

[5] Low glitches below 0.4 V on pin ENA and Vin, V_{out}, V_{cc} larger than 30 ns cause Power-On-Reset, respectively entering deep power-down mode.



1) During AC testing the inputs RST_N, I^2C_SDA, I^2C_SCL are driven at 0 V to +0.3 V for a LOW input level and at V_{CC} -0.3 V to V_{CC} for a HIGH input level. Clock period and signal pulse (duty cycle) timing is measured at 50 % of V_{CC}.

2) t_r is defined as rise time between 30 % and 70 % of the signal amplitude. tf is defined as fall time between 70 % and 30 % of the signal amplitude.

Figure 10. External clock drive and AC test timing reference points of I^2C_SDA, I^2C_SCL, and RST_N (see 1) and 2)) in open-drain mode

Table 14. Electrical AC characteristics of IO1, IO2, CLK and RST_N (ISO7816 interface)

Conditions: V_{CC} = 1.8 V ± 10 % or 3 V ± 10 % V; V_{SS} = 0 V; T_{amb} = -40 °C to +105 °C, unless otherwise specified. Typical values are only referenced for information. They are subject to change without notice.

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
Input/Output: IO1/IO2							
tr_{IO}	I/O Input rise time	Input/reception mode	[1] [2]			1	µs
			[3] [2]			0.25 x t_{IOWx_min}	µs
tf_{IO}	I/O Input fall time	Input/reception mode	[1] [2]			1	µs
			[3] [2]			0.25 x t_{IOWx_min}	µs
tr_{OIO}	I/O Output rise time	Output/transmission mode; CL = 30 pF	[2]			0.1	µs
tf_{OIO}	I/O Output fall time	Output/transmission mode; CL = 30 pF	[2]			0.1	µs
Inputs: CLK and RST_N							
f_{CLK}	External clock frequency in ISO/IEC 7816 UART applications	t_{CLKW}, t_{amb} and V_{CC} in their specified limits	[4]	0.85		11.5	MHz
t_{CLKW}	Clock pulse width i.r.t. clock period (positive pulse duty cycle of CLK)			40		60	%
tr_{CLK}	CLK input rise time		[5]			[6]	
tf_{CLK}	CLK input fall time		[2] [6]			[6]	
tr_{RST}	RST_N input rise time		[2]			400	µs
tf_{RST}	RST_N input fall time		[2] [7]			400	µs

[1] At minimum IO1 input signal HIGH or LOW level voltage pulse width of 3.2 µs. This timing specification applies to ISO7816 configurations down to a minimum etu duration of 16 CLK cycles at a maximum CLK frequency of 5 MHz (TA1=0x96, (Fi/Di)=(512/32)), for example.
[2] tr is defined as rise time between 10 % and 90 % of the signal amplitude.
[3] At minimum IO1 input signal HIGH or LOW level voltage pulse width of less than 3.2 µs. This timing specification applies to ISO7816 configurations beyond the conditions listed in note [2], down to a minimum etu duration of 8 CLK cycles at a maximum CLK frequency of 5 MHz (TA1=0x97, (Fi/Di)=(512/64)), for example. An 8 CLKs/etu @ fclk = 5 MHz configuration results in tIOWx_min = 1.6 µs, and in a time of 400 ns for trIO_max and tfIO_max, matching the (Fi/Di)=(512/64) speed enhancement requirements of ETSI TS 102 221.
[4] ISO/IEC 7816 I/O applications have to supply a clock signal to input CLK in the frequency range of 1 MHz to 10 MHz nominal. A ± 15 % tolerance range yields the allowed limits of 0.85 MHz and 11.5 MHz.
[5] During AC testing the inputs CLK, RST_N, and IO1 are driven at 0 V to +0.3 V for a LOW input level and at V_{CC} − 0.3 V to V_{CC} for a HIGH input level. Clock period and signal pulse (duty cycle) timing is measured at 50 % of V_{CC}, see Figure 18.
[6] The maximum CLK rise and fall time is 10 % of the CLK period 1/fCLK - with the following exception: In the CLK frequency range of 1 MHz to 5 MHz the maximum allowed CLK rise and fall time is 50 ns, if 10 % of the CLK period is shorter than 50 ns.
[7] The ETSI TS102 221/GSM 11.1x specifications specify a maximum reset signal (RST_N) rise time and fall time of 400,000 µs, respectively.

Note: *tf is defined as fall time between 90 % and 10 % of the signal amplitude.*

Table 15. Electrical AC characteristics of LA, LB; Conditions: T_{amb} = -40 °C to 105 °C, unless otherwise specified

Conditions: T_{amb} = -25 °C to +85 °C, unless otherwise specified.

Symbol	Parameter	Conditions		Typ[1]	Max	Unit
Input/Output: LA, LB						
C_{LALB}[2]	Pin capacitance LA, LB Bare die (SO28 empty package ground-off)					
	Configured for antenna input with 56 pF capacitance Test frequency = 13.56 MHz; T_{amb}= 25 °C	$V_{LA,LB}$ = 2.1 V (rms) $V_{LA,LB}$ = 0.3 V (rms)	[3] [4] [4]	54.3 50.1		pF
R_{LALB}[2]	Configured for antenna input with 56 pF capacitance. Test frequency = 13.56 MHz; T_{amb}= 25 °C	$V_{LA,LB}$ = 2.1 V (rms)	[3] [4] [5]	0.913		kΩ
f_{LALB}	Operating frequency LA, LB	level triggered ext.int.		13.56		MHz

[1] Typical values (± 10 %) are only referenced for information. They are subject to change without notice.
[2] The CLALB and RLALB values stated here assume a parallel RC equivalent circuit for the chip.
[3] The value stated here was measured at estimated start of chip operation and is comparable to the values stated in other SmartMX3 family member data sheets.
[4] Measured with sine wave at LA, LB.
[5] Parameter is valid in contactless ISO14443 compliant operation valid only.

14.4 I²C Bus Timings

Parameters defined in this chapter replace the parameter definitions of I²C bus, for specification see [9].

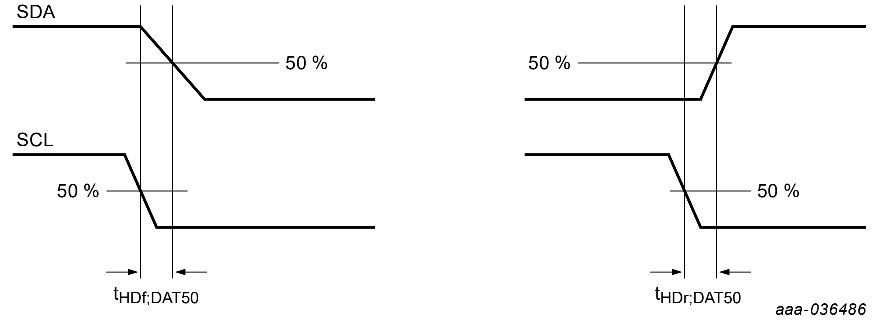


Figure 11. I²C Bus Timings

Table 16. I²C Bus Timing Specification

Symbol	Parameter	Condition	Min	Max	Unit
$t_{HDf;DAT50}$[1]	data hold time 50% SCL - 50% SDA level	Fast mode	8		ns
$t_{HDr;DAT50}$[2]	data hold time 50% SCL - 50% SDA level	Fast mode	24		ns
$t_{HDf;DAT50}$[1]	data hold time 50% SCL - 50% SDA level	Hs mode	8		ns
$t_{HDr;DAT50}$[2]	data hold time 50% SCL - 50% SDA level	Hs mode	9		ns

[1] $t_{HDf;DAT50}$, as defined in Figure 11, replaces parameter $t_{HD;DAT}$ defined in [9]
[2] $t_{HDr;DAT50}$, as defined in Figure 11, replaces parameter $t_{HD;DAT}$ defined in [9]

14.5 EMC/EMI

EMC and EMI resistance according to IEC 61967-4.

15 Abbreviations

Table 17. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CL	Contactless
CLK	External clock signal input contact pad
CC	Common Criteria
CMAC	Cipher-based MAC
CRC	Cyclic Redundancy Check
CRI	Cryptography Research Incorporated
DES	Digital Encryption Standard
DPA	Differential Power Analysis
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EMC	Electromagnetic compatibility
EMI	Electro Magnetic Immunity
FM	Fast-Mode
FM+	Fast-Mode+
GP	Global Platform
GPIO	General-purpose input/output
HS	High-Speed-Mode
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Keyed-Hash Message Authentication Code
HW	Hardware
IC	Integrated Circuit
I^2C	Inter-Integrated Circuit
I/O	Input/Output
IoT	Internet of Things
JCOP	Java Card Open Platform
LA	ISO 14443 Antenna Pad
LB	ISO 14443 Antenna Pad
NFC	Near Field Communication
MAC	Message Authentication Code
MCU	Microcontroller unit
MPU	Microprocessor

Table 17. Abbreviations...*continued*

Acronym	Description
MW	Middleware
OS	Operating System
NIST	National Institute for Standards and Technology
PCB	Printed Circuit Board
PKI	Public Key Infrastructure
PRF	Pseudo Random Function
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman
RST	Reset
SAM	Secure Access Module
SCL	Serial clock
SDA	Serial data
SPA	Simple Power Analysis
SFI	Single Fault Injection
SHA	Secure Hash Algorithm
SW	Software
TLS	Transport Layer Security
VCC	Supply Voltage Input
VIN	Voltage Input
VOUT	Voltage Output
VSS	Ground

16 References

[1] NXP SE05x T=1 Over I^2C Specification User Manual, Document Number 11225. Available on NXP website

[2] SOT1969-1; HX2QFN20; Reel packing and package data sheet. Available on NXP website.

[3] SE051 IoT Applet APDU Specification, document number AN 12543. Available on NXP website.

[4] SE051 configurations Application Note, document number AN12973. Available on NXP website.

[5] APDU Transport over SPI/I2C v1.0 | GPC_SPE_172. Available here.

[6] How to use EdgeLock SE051 PERSO applet, SE051 Application Note AN13015. Available on NXP website.

[7] SE051 - User Guidelines Application Note, document numerb AN12730. Available on NXP website.

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

[9] I2C-bus specification and user manual, document number UM10204. Available on NXP website.

17 Revision history

Table 18. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
577314	220328	Product data sheet		577313
Modifications	• Update Figure 2 • Add Section 3.6 • Update references in whole document • Update Section 6 • Update Section 2.2			
577313	220221	Product data sheet		577312
Modifications	• Updated Section 2.2 • Updated Features in detail • Updated Section 3.2.7 • Updated Section 6 • Updated Section 14.3 • Updated Section 1 • Updated Figure 2 Updates for intermediate update on 210415 • Updated Section 2.2 • Moved technical information on secure objects in Section 3.2.1 to the APDU specification [3] • Replace "master/slave" by "controller/target" • Update Figure 1			
577312	201215	Product data sheet		577311
Modifications	• Updated Table 1 • Updated legal disclaimer and references • Figure 2			
577311	201117	Product data sheet		577310
Modifications	Corrected Table 1			
577310	201028	Objective data sheet		-
Modifications	Initial version			

18 Legal information

18.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.
[2] The term 'short data sheet' is explained in section "Definitions".
[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

18.2 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.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

18.3 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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

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.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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.

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.

18.4 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

18.5 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.

I2C-bus — logo is a trademark of NXP B.V.

JCOP — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

Tables

Figures

Contents

Date of release: 28 March 2022
Document number: 577314