SE052

EdgeLock family

Rev. 1.5 — 3 June 2024 Product data sheet
789115

1 Introduction

EdgeLock SE052 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 a state-of-the-art edge-to-cloud security capability right out of the box.

The SE052 is a turnkey solution that comes with an updatable applet optimized for IoT security use cases preinstalled. A comprehensive product support package, complements this solution. This package enables fast time to market and easy design-in with Plug and Trust middleware for host applications, a development kit, and documentation for product evaluation.

SE052 has a FIPS 140-3 level three certification [FIPS 140-3 validated, Certificate #4679] and an independent Common Criteria EAL 6+ security certification up to OS level and supports both RSA and ECC asymmetric cryptographic algorithms with high key length. The latest security measures are targeting to protect the IC even against sophisticated noninvasive and invasive attack scenarios.

1.1 SE052 Use Cases

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

1.2 Applications

- Smart Industry
- Smart Home
- Smart Cities
- Healthcare

2 General description

The SE052 is based on NXPs 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. It represents NXPs next generation of secure elements and forms the essence of more than 15 years of experience.

EdgeLock SE052 is a platform. The SE052F variant is FIPS 140-3 certified. For more information about the released configuration, see the Configuration Sheet. [1]

2.1 Key benefits

- Plug & Trust Middleware for fast and easy design with complete product support package
- Easy integration with different MCU and MPU platforms and OSs (Linux, RTOS, Windows, Android, and so on)
- 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 and private clouds
- Real end-to-end security, from sensor to cloud
- Ready-to-use example code for each of the key use cases

3 Features and benefits

3.1 Product-specific features

The SE052 operates fully autonomously based on an integrated Javacard operating system and applets. With the NXP IoT applet, 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 Life-Cycle management
- FIPS 140-3 Lv 3 Certified Module with level 4 for physical security
- 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
- Support for RSA and ECC asymmetric cryptography algorithms
- Support for AES Modes: CBC, ECB, CTR, GCM, CCM
- HMAC, CMAC, GMAC, SHA-224/256/384/512 (only in combination with, HMAC and/or PBKDF) operations
- Various options for key derivation functions, including HKDF, PRF (TLSPSK)
- Extended temperature range for industrial applications (-40 °C to 105 °C)
- HVQFN20 package (4 mm × 4 mm)
- Communication interfaces supported for different product configurations:
  - I^2C target up to 3.4 Mbit/s
  - I^2C controller up to 400 kbit/s
  - ISO14443-A passive contactless wireless interface for IoT use cases simplifying configuration set-up, maintenance in the field and late stage configuration
- 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 multitenant ecosystems
- 100 kB of free user memory
- SEMS Lite for Applet update available.
  Note: *Updating the applet will make the parts non-FIPS compliant and they will require a FIPS recertification of the new applet version.*

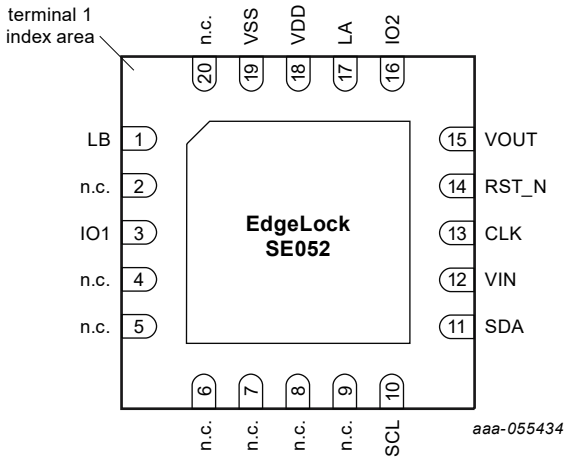
4 Ordering information

Table 1. Ordering information

Variant Identifier (OEF ID)	12NC	Type Number	Orderable Part Number
B501	9354 551 73118	SE052F2HN2/Z019H	SE052F2HN2/Z019HJ

5 Pinning

5.1 Pin description HVQFN20



Transparent top view

Table 2. Pin description for SE052

Symbol	Pin	Description
LB	1	Antenna coil connection
n.c.	2	not connected
IO1	3	I^2C controller SDA (or ISO 7816 UART GPIO)
n.c.	4-9	not connected
SCL	10	I^2C clock
SDA	11	I^2C data
VIN	12	Power supply voltage input for SCL, SDA pads, IO2 when not in DPD mode, logic supply for I^2C
CLK	13	not connected (or ISO 7816 UART CLK)
RST_N	14	Low level on RST_N pin is triggering device reset. The reset is also triggered without a clock signal on the CLK-pin, this functionality might be in conflict with ISO/IEC 7816 negative tests.
VOUT	15	Supply voltage output to be connected to pad VDD on PCB level
IO2	16	I^2C controller SCL (or ISO 7816 UART GPIO2)
LA	17	Antenna coil connection LA
VDD	18	Power supply voltage input
VSS	19	Ground (reference voltage) input
n.c.	20	not connected

6 Package

SE052 is offered in an HVQFN20 package. The dimensions are 4 mm x 4 mm x 0.85 mm with a 0.5 mm pitch.

Refer to the package data sheet SOT917-7.pdf.

7 Marking

Table 3. Marking codes

Type number	Marking code
SE052...	Line A: SE52 Line B: **** (**** = 4-digit Batch code) Line C: snDywwA s: Diffusion center n: Assembly center D: RHF-2006 indicator Y: Year WW: Week A: Mask layout version

8 Packing information

8.1 Reel packing

The SE052 product is available in tape on reel.

Table 4. Reel packing options

Symbol	Parameter	Number of units per reel
HVQFN20	13" tape on reel	6000

9 I²C interface

9.1 Introduction

The SE052 offers an I²C interface supporting target mode with data rates up to 3.4 Mbit/s when operated in High-Speed Mode (HS). The I²C interface is using the T=1 over I²C.

When the IC is in power saving modes Power Down or Deep Power Down the system wakes up on I²C bus activity. After wakeup from DPD mode I²C HS mode has to be enabled vis HS preamble similar to power on reset.

Figure 1 is showing an abstract on how to integrate the SE052 in a system using I²C interface.

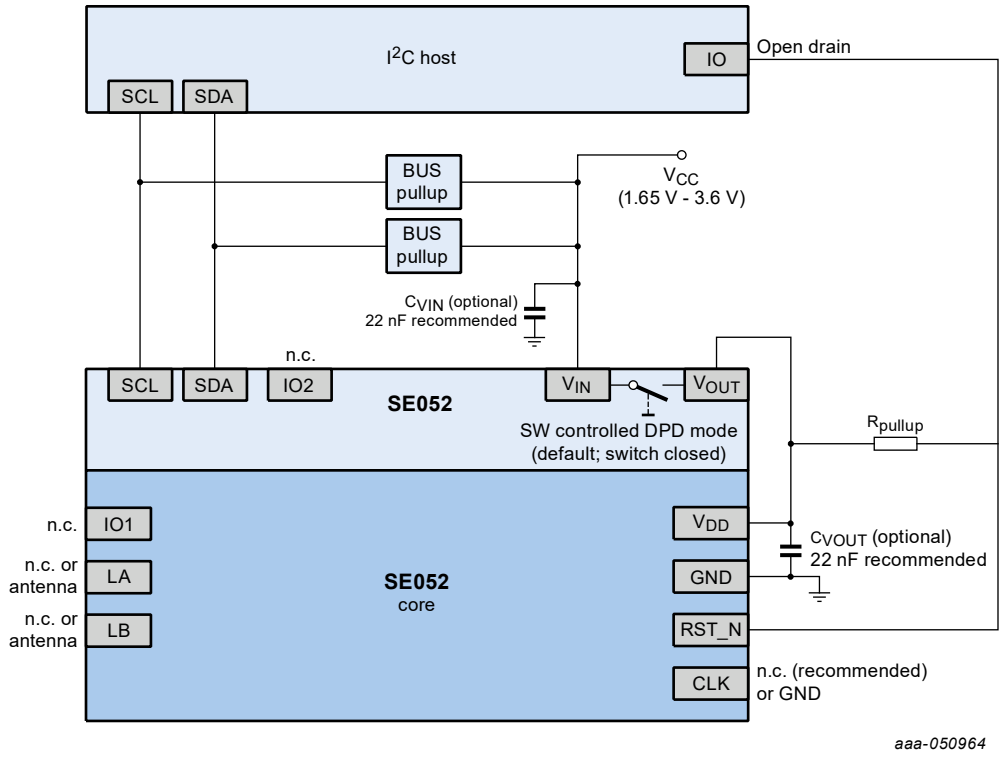


Figure 1. SE052 using I²C

10 Power-saving modes

10.1 Introduction

The device provides two power-saving operation modes. The Power-down mode (with state retention) and the Deep Power-down mode (no state retention).

10.2 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 SE052 enters into Power-down mode by receiving "End of APDU session request" (according to [2]) respectively "RELEASE request" (according to GP T=1oI2C [3]). 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 I2C_SDA2.

10.3 Deep Power-down mode

The SE052 provides a special power-saving mode offering maximum power saving. This mode is activated by sending a T=1oI2C command for deep power down (S-Block 0xDF).

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

With the next command adressed to the I^2C interface of the device, it will wakeup from Deep Power down mode, which means booting up and then is available to process the next received command.

For usage of Deep Power-down mode the SE052 must be supplied via pin Vin and pin VDD needs to be supplied by pin Vout.

11 Limiting values

Table 5 and Table 6 show the limiting values for the SE052.

Table 5. 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_{DD}	supply voltage	pad V_{DD}	-0.3	6	V
V_I	input voltage	pads V_{DD}, V_{SS}, CLK, RST_N, IO1	-0.3	6	V
I_I	input current	pad IO	-20		mA
I_O	output current	pad IO	-	30	mA
I_{lu}	latch-up current	$V_I < 0$ V or $V_I > V_{DD}$	-	± 100	mA
V_{esd}	electrostatic discharge voltage (HBM)	pads VDD, VSS, CLK,RST_N, IO1 [1]		± 4	kV
		pads LA, LB [1]		± 3	kV
	electrostatic discharge voltage (CDM)	all pads [2]		750	V
P_{tot}	Total power dissipation	[3]	-	600	mW
$E_{opt, max}$	Irradiance [4]	perpendicular illumination from backside of unprotected chip; light from a black body radiation source in the optical wavelength range between 400 nm and 1100 nm at 25 °C ambient temperature [3]	-	3	W/m^2
T_{stg}	Storage temperature		-55	125	°C

[1] In accordance with ANSI/ESDA/JEDEC JS-001-2011, ESDA/JEDEC Joint Standard for Electrostatic Discharge Sensitivity Testing - Human Body Model (HBM) - Component Level.
[2] In accordance with JEDEC JESD22-C101 for Charged-Device Model (CDM)
[3] Depending on appropriate thermal resistance of the package.
[4] Irradiance is a radiometric parameter and shall not be confused with photometric illuminance measured in lux.

Table 6. Limiting values (V_{IN}, V_{OUT}, SDA, SCL, IO2)

Additional parameter for pads V_{IN}, V_{OUT}, SDA, SCL, IO2

Symbol	Parameter	Conditions	Min	Max	Unit
V_{IN}	supply voltage for pads SDA, SCL, IO2, V_{out}		-0.3	3.63	V
V_I	input voltage	pads SDA, SCL, IO2	-0.3	3.63	V
I_i	input current	pads SDA, SCL, IO2	-10	-	mA
I_o	output current	pads SDA, SCL, IO2	-	10	mA
V_{esd}	electrostatic discharge voltage (HBM)	pads VIN, VOUT, SDA, SCL, IO2	-	2	kV
C_{VOUT}	capacitive load at node V_{out}-V_{DD}		-	47[1]	nF

[1] Capacitive load at node V_{out}-V_{DD} will lead to increased Inrush currents at startup which needs to be supplied by node Vin. In case the current cannot be supplied at Vin the startup time of the IC will increase.

12 Recommended operating conditions

Table 7. Recommended operating conditions

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{DD} (5 V)	Supply voltage [1]	Nominal supply voltage contact interface operation	4.5	5	5.5	V
V_{DD} (3 V)		Class B/3 V nominal supply voltage contact interface operation	2.7	3	3.3	V
V_{DD} (1.8 V)		Class C/1.8 V nominal supply voltage contact interface operation	1.62	1.8	1.98	V
V_I	DC input voltage on digital inputs and digital I/O pads	pads RST_N, CLK, IO1	-0.3		V_{DD} + 0.3	V
H	Field strength	Contactless interface operation for 25 °C to 85 °C[2]	1.5	-	7.5	A/m
		Contactless interface operation for -40 °C to 105 °C	1.5	-	3.5	A/m
T_{amb}	Operating ambient temperature [3]		-40	-	105	°C

[1] All described supply voltages according to ISO/IEC 7816-3.
[2] Values apply to antenna Class-1 PICC, antenna field strength range for higher Class antennas according ISO14443.
[3] All product properties and values specified within this data sheet are only valid within the operating ambient temperature range.

The supported operating supply voltage ranges limited by exception sensors covers the whole range of classes A, B and C. The SE052 devices operate within the full voltage range described in Figure 3.

Figure 2. Operating conditions over voltage range (V_{DD})

Table 8. Recommended operating conditions (V_{IN}, SDA, SCL, IO2)

Additional parameter for pads V_{IN}, V_{OUT}, SDA, SCL, IO2

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{IN}	supply voltage for pads SDA, SCL, IO2, V_{out}	Nominal supply voltage	1.65	1.8	3.6	V
V_I	DC input voltage on digital inputs and digital I/O pads	pads SDA, SCL, IO2	-0.3	V_{IN}	3.63	V

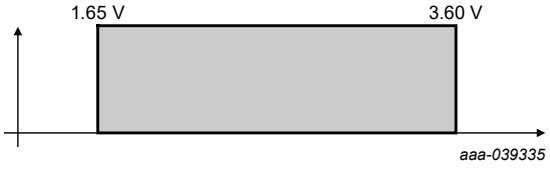


Figure 3. Operating conditions over voltage range (V_{IN})

13 Static characteristics

13.1 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 Secure Element are considered positive.

13.2 Level and currents

13.2.1 General and ISO7816 I/O interface

Table 9. Electrical DC characteristics of Input/Output: IO1/IO2

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{in} = 1.65 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified
In Table 9 V_{DD} means for IO1 voltage on V_{DD} pin, for IO2 voltage on V_{IN} pin

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{IH}	HIGH level input voltage	[1]	0.7 × V_{DD}	-	V_{DD} + 0.3	V
V_{IL}	LOW level input voltage		-0.3	-	0.25 × V_{DD}	V
I_{IH}	HIGH level input current in "weak pull-up" input mode	0.7 V_{DD} ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{IH(max)}$: V_I = 0.7 V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C	-20	-	-	µA
I_{IL}	LOW level input current	0 V ≤ V_I ≤ 0.3 V_{DD}; Test conditions for the maximum absolute value: $I_{IL(max)}$: V_I = 0 V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C	-50	-	-	µA
I_{TL}	HIGH-to-LOW transition input current (only in "quasi-bidirectional" mode)	0.3 V_{DD} < V_I ≤ V_{DD}; Test conditions for the maximum absolute value: V_I = 0.5 V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B, or C[2]				
		Class A	-300	-	-	µA A
		Class B	-250	-	-	µA
		Class C	-200	-	-	µA
I_I	Input current in "weak pull-up" input mode	0 V ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{I(max)}$: V_I = 0 V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B, or C	-50	-	-	µA
I_{ILIH}	Leakage input current at input voltage beyond V_{DD} in "weak pull-up" input mode	V_{DD} < V_I ≤ V_{DD} + 0.3 V; -40 °C ≤ T_{amb} ≤ 105 °C; Test conditions: V_I = V_{DD} + 0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B, or C; T_{amb} = 105 °C		A	25	µA
				B, C	20	µA

Table 9. Electrical DC characteristics of Input/Output: IO1/IO2*...continued*

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{in} = 1.65 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified
In Table 9 V_{DD} means for IO1 voltage on V_{DD} pin, for IO2 voltage on V_{IN} pin

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
I_{ILIL}	Leakage input current at input voltage below V_{SS} in "weak pull-up" input mode	Test conditions: V_I = -0.3 V; V_{DD} = $V_{DD(max)}$, of the respective supply voltage class A, B or C				
		-0.3 V ≤ V_I < 0 V; -40 °C ≤ T_{amb} ≤ 30 °C, T_{amb} = 30 °C	-100	-	-	µA
		-0.3 V ≤ V_I < 0 V; 30 °C ≤ T_{amb} ≤ 85 °C, T_{amb} = 85 °C	-400	-	-	µA
		-0.3 V ≤ V_I < 0 V; 85 °C ≤ T_{amb} ≤ 105 °C, T_{amb} = 105 °C	-600	-	-	µA
I_{ILIHQ}	Leakage input current at input voltage beyond V_{DD} (only in "quasi-bidirectional"mode)	V_{DD} < V_I ≤ V_{DD} + 0.3 V; -40 °C ≤ T_{amb} ≤ 105 °C Test conditions: V_I = V_{DD} + 0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = 105 °C	-	-	100	µA
I_{ILILQ}	Leakage input current at input voltage below V_{SS} (only in "quasi-bidirectional"mode)	Test conditions: V_I = -0.3 V; V_{DD} = $V_{DD(max)}$; of the respective supply voltage class A, B or C				
		-0.3 V ≤ V_I < 0 V; -40 °C ≤ T_{amb} ≤ 30 °C, T_{amb} = 30 °C	-100	-	-	µA
		-0.3 V ≤ V_I < 0 V; 30 °C ≤ T_{amb} ≤ 85 °C, T_{amb} = 85 °C	-400	-	-	µA
		-0.3 V ≤ V_I < 0 V; 85 °C ≤ T_{amb} ≤ 105 °C, T_{amb} = 105 °C	-600	-	-	µA
V_{OH}	HIGH level output voltage	I_{OH} = -20 µA; Class A condition [3]	3.8	-	-	V
		I_{OH} = -20 µA; Class B or C condition [3]	0.7 × V_{DD}	-	-	V
V_{OL}	LOW level output voltage	Class A or B condition; I_{OL} = 1 mA	-	-	0.3	V
		Class C condition				
		I_{OL} = 1 mA	-	-	0.3	V
		I_{OL} = 0.5 mA	-	-	0.15 × V_{DD}	V

[1] V_{DD} = V_{OUT} for High level input voltage on IO2 (IO2: VIH max. = 3.63 V)
[2] IO1 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_{DD}. Input current I_{TL} is tested at input voltage V_I = 0.5 V_{DD}. Current IIL is tested at input voltage V_I = 0.3 V. Figure 4 shows the input characteristic of this quasi-bidirectional port mode.
[3] External pull-up resistor 20 kΩ to V_{DD} assumed. The worst case test condition for parameter V_{OH} is present at minimum V_{DD}. For class A supply voltage conditions V_{DD} = 4.5 V is the worst case with respect to the fix specification limit $V_{OH(min)}$ = 3.8 V (0.844 V_{DD}). The supply voltage related limit "0.7 V_{DD}"is a stricter requirement than the fix value 3.8 V at high V_{DD} values (0.7 V_{DD} = 3.85 V at V_{DD} = 5.5 V). So, in the V_{DD} range 4.5 V to 5.5 V, $V_{OH(min)}$ is specified as "the larger value of 0.7 V_{DD} and 3.8 V, respectively". The V_{OHmin} value (0.7 V_{DD}) cannot be guaranteed in "quasi-bidirectional" mode at an output current of I_{OH} = -20 µA - the strong output drive mode must be used.

Table 10. Electrical DC characteristics of Inputs CLK and RST_N

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
Inputs CLK and RST_N						
V_{IH}	HIGH level input voltage		0.7 × V_{DD}	-	V_{DD} + 0.3	V
V_{IL}	LOW level input voltage		-0.3	-	0.25 × V_{DD}	V
I_{IH}	HIGH level input current	0.7 V_{DD} ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{IH(max)}$: V_I = 0.7 V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B, or C	-20	-	-	µA
I_{IL}	LOW level input current	0 V ≤ V_I ≤ 0.3 V_{DD}; Test conditions for the maximum absolute value: $I_{IL(max)}$: V_I = 0V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C	-20	-	-	µA
I_I	Input current	0 V ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{I(max)}$: V_I = 0 V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B, or C	-20	-	-	µA
I_{ILIH}	Leakage input current at input voltage beyond V_{DD}	V_{DD} < V_I ≤ V_{DD} + 0.3 V; -40 °C ≤ T_{amb} ≤ 105 °C Test conditions: V_I = V_{DD} + 0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = 105 °C	-	-	20	µA
I_{ILIL}	Leakage input current at input voltage below V_{SS}	Test conditions: V_I = -0.3 V; V_{DD} = $V_{DD(max)}$; of the respective supply voltage class A, B or C;				
		-0.3 V ≤ V_I < 0 V; -40 °C ≤ T_{amb} ≤ 30 °C; T_{amb} = 30 °C	-100	-	-	µA
		-0.3 V ≤ V_I < 0 V; 30 °C ≤ T_{amb} ≤ 85 °C; T_{amb} = 85 °C	-300	-	-	µA
		-0.3 V ≤ V_I < 0 V; 85 °C ≤ T_{amb} ≤ 105 °C; T_{amb} = 105 °C	-450	-	-	µA

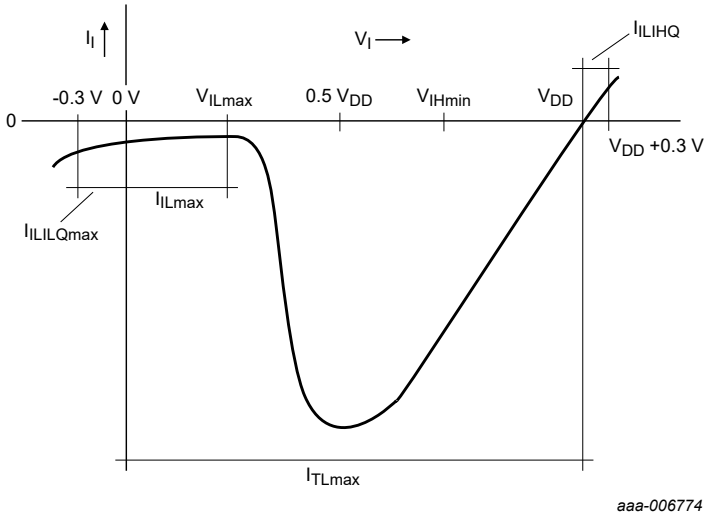


Figure 4. Input characteristic of IO1/IO2 in “quasi-bidirectional” mode

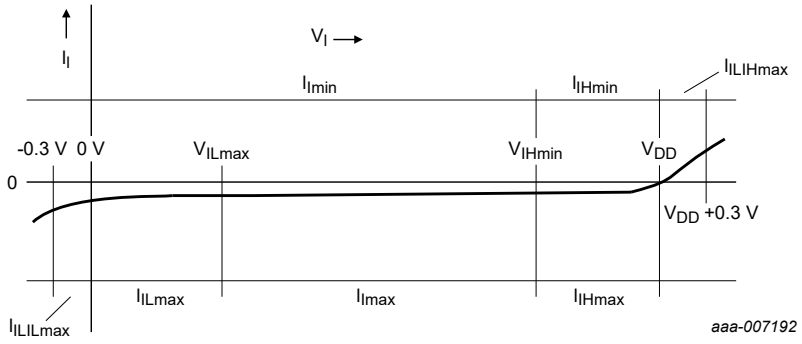


Figure 5. Input characteristic of IO1/IO2 in “weak pull-up” input mode

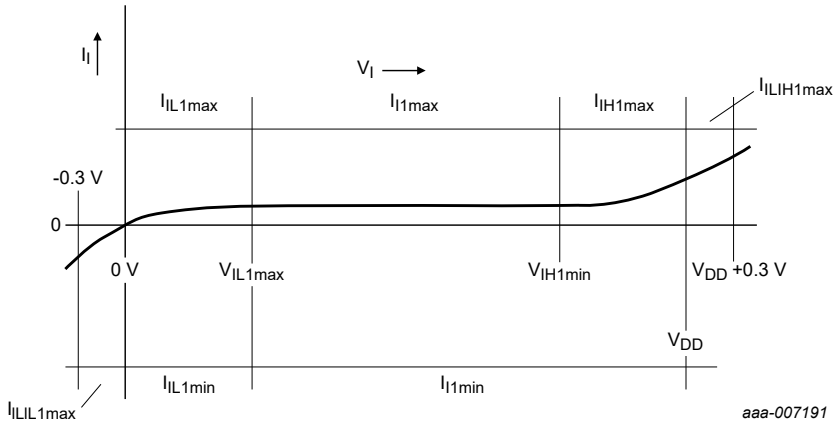


Figure 6. Input characteristic of CLK when the IC is not in reset and of RST_N

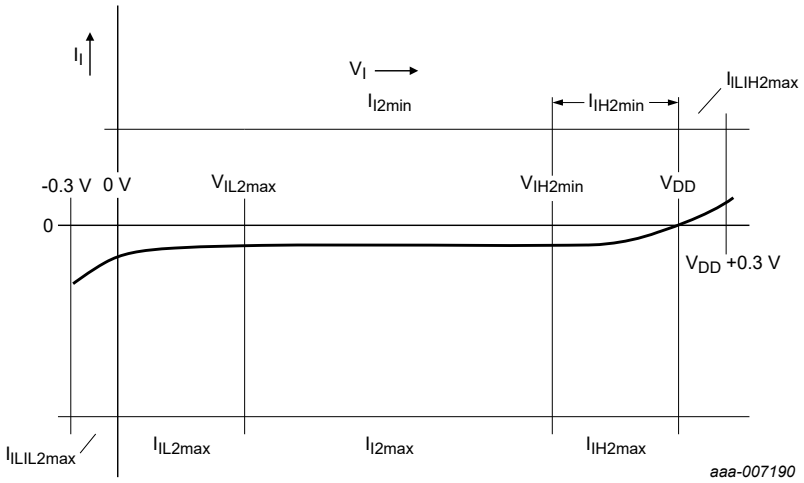


Figure 7. Input characteristic of CLK during IC reset

13.2.1.1 Pads SDA and SCL

Table 11. Electrical DC characteristics of pads SDA, SCL.

Conditions: V_{DD}, V_{IN} = 1.65 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified. SCL, SDA pads are in open-drain mode, unless otherwise specified.

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{IH}	HIGH level input voltage		0.7 V_{IN}	-	V_{IN} + 0.3 (max. 3.63 V)	V
V_{IL}	LOW level input voltage		-0.3	-	0.25 × V_{IN}	V
V_{HYS}	Input hysteresis voltage	-	0.05	-	-	V_{DD}
$V_{OL(OD)}$	Low level output voltage (open-drain mode)	I_{OL} = 3.0 mA; V_{IN} = 3.6 V to 2 V	0	-	0.4	V
		I_{OL} = 2.0 mA; V_{IN} = 2 V to 1.65 V	0	-	0.2 × V_{DD}	V
$I_{OL(OD)}$	Low level output current (open-drain mode)	V_{OL} = 0.4 V; V_{IN} = 1.65 V to 3.6 V	5	-	-	mA
		V_{OL} = 0.6 V; V_{IN} =1.65 V to 3.6 V	6	-	-	mA
$V_{OH(PP)}$	High level output voltage (push-pull/GPIO mode)	I_{OH} = 3 mA	0.7	-	-	V_{IN}
$V_{OL(PP)}$	Low level output voltage (push-pull/GPIO mode)	I_{OL} = 3 mA, V_{IN} > 2 V	-	-	0.4 × V	V
		I_{OL} = 3 mA, V_{IN} <= 2 V:	-	-	0.2 × V_{IN}	V
I_{IH}	High level input current	0 V ≤ V_I ≤ V_{DD}(max); −40 °C ≤ T_{amb} ≤ 105 °C; Test conditions: V_I = V_{DD} ; V_{DD} = V_{DD} (max); T_{amb} = 105 °C	-	-	1	µA
I_{IL}	Low level input current	0 V ≤ V_I ≤ V_{DD} (max); −40 °C ≤ T_{amb} ≤ 105 °C; Test conditions: V_I = VDD; V_{DD} = 0 V; T_{amb} = 105 °C	-1	-	-	µA
I_{WPU}	weak pull-up current		-300	-	-70	µA
I_{WPD}	weak pull-down current		80	-	350	µA

13.3 Configuration settings

The applied EdgeLock SE052 OS configuration is shown below.

Table 12. Configuration parameters

Configuration parameter	Value	Description
TCL_ATS_IF	0x0578779102	This are the first bytes in the ATS before the Historical Characters. (T0, [TA1], [TB1], [TC1]) The first byte defines the length (excl. length byte).
TCL_L3_ACTIVATION_CONTROL	0x04	L3 Activation Control Parameter = 0x04: Use UID stored in Security Row. (even if "ATQA select" selects a different source for ATQA).
TCL_ATS_CURRENT_HISTLEN	0x05	Actually used length of the historical characters in configuration item TCL_ ATS_HISTCHARS
TCL_ATS_HISTCHARS	0x8073C82110000000000 00000000000000000000	Byte array (max 20 bytes): Historical characters used for T=CL.
TCL_ATQA_MSB	0x00	1-byte value: ATQA MSB byte only used for CIU
TCL_ATQA_LSB	0x48	1-byte value: ATQA LSB byte only used for CIU
TCL_SAK_COMPLETE	0x20	1-byte value: SAK in case of incomplete UID, only used for CIU.
TCL_SAK_INCOMPLETE	0x24	1-byte value: SAK in case of complete UID, only used for CIU.
MAX_SUPPORTED_RSA_KEYLEN_ BIT	0x1000	Maximum RSA key size in bits.
COMM_BEHAVIOR	0x54	Entry to configure comm behaviour. Bit6 - 1=Extended Length APDU Lock enabled(extended APDU will NOT reach standard applets which do NOT implement Extended Length Interface) Bit5 - 0=NAK handling enabled on the first command after L3 activation, Bit4 - 1=strong modulation enabled Bit3 - 0=No EMV SB114 warning support for T=0 Bit2 - 1=I-Block number check is enabled on contactless Bit1 - 0=EMVCO incompatible
PPS_HANDLING	0x03	Entry to configure comm behaviour for PPS handling Bit1 - 1=override ATS and allow PPS. Bit0 - 1=override ATR and allow PPS.

Table 12. Configuration parameters*...continued*

Configuration parameter	Value	Description
ATR_I2C_IF_BYTES	0x1801A0000003960403E800FE020B 03E80001000000000641388	ATR definition for I^2C interface. Length of the data = 0x18 (excl. length byte) ---------- Protocol Version = 0x01 RID according to [7816-4] = 0xA00000 0396 Length of Data Link Layer Parameters = 0x04 ---------- Block Waiting Time (in ms) = 0x03E8 Maximum Information Field Size of the SE (in bytes) (i.e. initial value) = 0x00FE ---------- Physical Layer ID = 0x02 (= I^2C) Length of Physical Layer Parameters = 0x0B ---------- Maximal Clock Frequency at which the SE may operate (in kHz) = 0x03E8 Configuration = 0x00 => HS (High Speed) mode not supported Minimum Polling Time (conditional to Polling Mode support) (in ms) = 0x01 IRQ Clear Time (conditional on Interrupt Mode support) (in µs) = 0x00 Maximum SE Access Length (in bytes) = 0x0000 Secure Element Guard Time (in µs) = 0x0064 Wake-Up Time (in µs) = 0x1388 (when receiving a Wake-Up Byte, time after which the SE is ready to receive a command)

Table 12. Configuration parameters*...continued*

Configuration parameter	Value	Description
CIP_I2C_SPI_IF_BYTES	0x150104630700930208000503E8FF0100640403E800FE00000000	Length of the CIP data = 0x15 (excl. length byte) Protocol Version = 0x01 Length of the following IIN bytes = 0x04 Issuer Identification Number (according to [7812-1], BCD encoded) = 0x63070093 Physical Layer ID = 0x02 (= I^2C) --- Length of Physical Layer Parameters (8 byte PLP) = 0x08 Physical Layer Parameters for I^2C: Configuration = 0x00 => Clock stretching not supported Power Wake Up Time (PWT) (in ms) = 0x05 Maximal Clock Frequency (MCF) (in kHz) = 0x03E8 => depends on Clock Stretching enabled or disabled. Clock Stretching enabled: up to 3.4 MHz Clock Stretching disabled: up to 1.0 MHz Power Saving Timeout (PST) (0x00-0xFE ms or 0xFF) = 0xFF => (0xFF is a special value - SE enters power saving mode only afer reception of S(RELEASE block)) Minimum Polling Time (MPOT)(in ms) = 0x01 R/W Guard Time (RWGT)(in µs) = 0x0064 --- Length of Data Link Layer Parameters (4 byte DLLP) = 0x04 Block Waiting Time (in ms) = 0x03E8 Maximum Information Field Size of the SE (in bytes) (i.e. initial value) = 0x00FE --- RFU = 0x00000000
ATR_CIP_I2C_SPI_HIST_CHARS	0x0A00655345303531000000000000000	Historical Character definition for I^2C and SPI interface. Config item holds the following information: Length of Historical Bytes = 0x0A Historical Bytes = 0x00655345303531 00000000000000
VHBR_ENABLED	0xA5	VHBR: Disabled

Table 12. Configuration parameters*...continued*

Configuration parameter	Value	Description
PERSISTENT_DATA_ENUM_ EXTERNAL_FEATURES	0x0202020200000000	FEATURE_SELECT_FILE_WITH_ INVALID_AID: FEATURE_GP_ COMPLIANT FEATURE_SELECT_FILE_WHILE_ ALREADY_SELECTED: FEATURE_ GP_COMPLIANT FEATURE_SELECT_MANAGE_ CHANNEL_INVALID_CLASS: FEATURE_GP_COMPLIANT FEATURE_EXTENDED_APDU_ ORIGIN_DEFAULT: FEATURE_GP_ COMPLIANT
NR_OF_LOGICAL_CHANNELS	0x02	Maximum number of supported logical channels.
OS_TIMER_INIT	0xF9B8	Enable Timer on Contactless Interface Enable Timer on Contact Interface Enable Timer on I^2C
I2C_SPI_PARAMS	0x000E	Target clock stretching = clock stretching disabled Enable power saving mode after sending End of APDU Session response = power save mode enabled Select flavour of T1I2C protocol = GP 0.39 flavour Select the T1I2C protocol communication mode = Blocking Communication
I2C_SLAVE_ADDRESS	0x48	1-byte value: I^2C target address of product.

13.4 General A/5 V, class B/3 V, or class C/1.8 V class operation

Table 13. Electrical characteristics of IC supply current

[1] Conditions: V_{DD} = 1.62 V to 5.5 V; V_{IN} = 1.65 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified

Symbol	Parameter	Conditions	Supply voltage class	Min	Typ	Max	Unit
Supply							
V_{DD}	supply voltage range	Class A: 5 V range	A (5 V)	4.5	5	5.5	V
		Class B: 3 V range	B (3 V)	2.7	3	3.3	V
		Class C: 1.8 V range	C (1.8 V)	1.62	1.8	1.98	V
	operating mode: Idle mode						
V_{IN}	supply voltage range	$V_{DD} = V_{OUT}$	V_{IN}	1.65	1.8	3.6	V

Table 13. Electrical characteristics of IC supply current...*continued*

[1] Conditions: V_{DD} = 1.62 V to 5.5 V; V_{IN} = 1.65 V to 3.6 V; V_{SS} = 0 V; T_{amb} = -40 °C to 105 °C, unless otherwise specified

Symbol	Parameter	Conditions	Supply voltage class	Min	Typ	Max	Unit
I_{DD}	supply current Idle mode	f_{CPU} = 48 MHz, f_{MST} = 96 MHz	all	1.3	2	3.3	mA
	operating mode: typical CPU						
	no coprocessor active	f_{CPU} = 48 MHz, f_{MST} = 96 MHz	all	4.5	5	6.5	mA
	AES coprocessor active (AES 48 MHz)	CPU in Idle mode	all	6.7	7.5	8.7	mA
	Assymmetric coprocessor active (FAME 48 MHz)	CPU in Idle mode	all	13.5	15.2	17	mA
	DES coprocessor active (DES 48 MHz)	CPU in Idle mode	all	7	7.7	9	mA
$I_{DD(PD-ISO7816)}$	supply current CLOCKSTOP mode	$V_{DD(min)} \leq V_{DD} \leq V_{DD(max)}$; Clock to input CLK at "high" level stopped, T_{amb} = 25 °C, I^2C not selected in OEF	A (5 V)	300	400	470	µA
			B (3 V) C (1.8 V)	280	390	430	µA
$I_{DD\ (PD-I^2C)}$	supply current I^2C Power-down mode	$V_{IN(min)} <= V_{IN} <= V_{IN(max)}$; $V_{DD} = V_{OUT}$ Clock to input SCL stopped, T_{amb} = 25 °C, SDA, SCL pads in pull-up Typical value with V_{DD} = 1.8 V	V_{IN}	500	610	660	µA
$I_{DD(DPD)}$	Deep Power-down mode (without state retention)	$V_{IN(min)} <= V_{IN} <= VIN(max)$; $V_{DD} = V_{OUT}$; DPD timer stopped; I^2C clock stopped	V_{IN}	3	10	15	µA

[1] Typical values are only referenced for information. They are subject to change without notice.

14 Dynamic characteristics

14.1 General, ISO/IEC 7816, ISO/IEC 14443 I/O and I^2C I/O

Table 14. Electrical AC characteristics of I/O1, CLK, and RST_N

Conditions: V_{DD} = 1.62 V to 5.5 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						
$t_{r(i)(IO)}$	I/O Input rise time	Input/reception mode [1] [2]	-	-	1	µs
		Input/reception mode [3] [2]	-	-	0.25 × t_{IOWx_min}	µs
$t_{f(i)(IO)}$	I/O Input fall time	Input/reception mode [1] [2]	-	-	1	µs
		Input/reception mode [3] [2]	-	-	0.25 × t_{IOWx_min}	µs

Table 14. Electrical AC characteristics of I/O1, CLK, and RST_N *...continued*

Conditions: V_{DD} = 1.62 V to 5.5 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
$t_{r(o)(IO)}$	I/O Output rise time	Output/transmission mode; C_L = 30 pF [2]	-	-	0.1	µs
$t_{f(o)(IO)}$	I/O Output fall time	Output/transmission mode; C_L = 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_{DD} 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)	[5]	40	-	60	%
$t_{r(i)(CLK)}$	CLK input rise time	[6] [2]	-	-	[6]	
$t_{f(i)(CLK)}$	CLK input fall time	[6] [2]	-	-	[6]	
$t_{r(i)(RST)}$	RST_N input rise time	[7] [2]	-	-	400	µs
$t_{f(i)(RST)}$	RST_N input fall time	[7] [2]	-	-	400	µs
t_{RW}	Reset pulse width (RST_N low)		40	-	-	µs
Inputs: CLK, RST_N, IO1						
C_{PIN}	Pin capacitances CLK, RST_N, IO1	Test frequency = 1 MHz; T_{amb} = 25 °C	-	-	20	pF

[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] t_r is defined as rise time between 10 % and 90 % of the signal amplitude.
t_f is defined as fall time between 90 % and 10 % 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 t fclk = 5 MHz configuration results in $t_{IOWx(min)}$ = 1.6 µs, and in a time of 400 ns for $t_{r(IO)(max)}$ and $t_{f(IO)(max)}$, 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_{DD} − 0.3 V to V_{DD} for a HIGH input level. Clock period and signal pulse (duty cycle) timing is measured at 50 % of V_{DD} (see Figure 8).

[6] The maximum CLK rise and fall time is 10 % of the CLK period $1/f_{CLK}$ - 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.

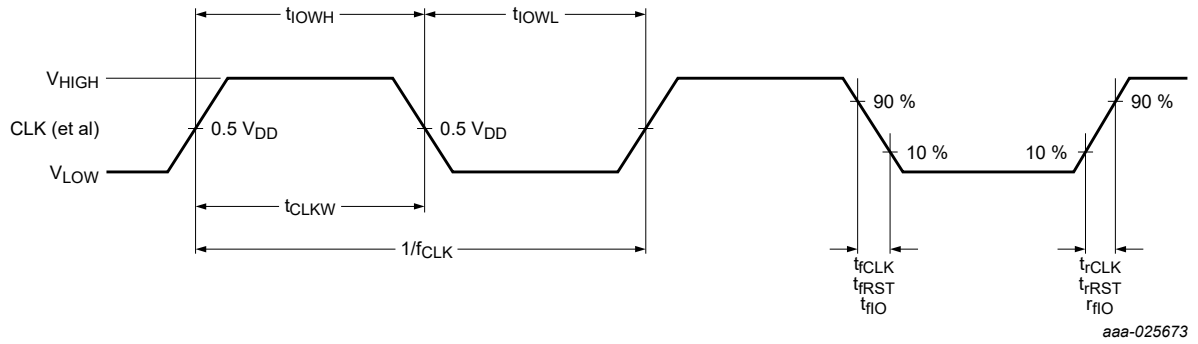


Figure 8. External clock drive and AC test timing reference points of CLK, RST_N, IO1

Table 15. Electrical AC characteristics of I/O2, SDA, SCL, SDI (CLK), and V_{OUT}

Conditions: V_{DD}, V_{IN} = 1.65 V to 3.6 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: IO2						
$t_{r(i)(IO)}$	I/O Input rise time	Input/reception mode [1]	-	-	1	µs
$t_{f(i)(IO)}$	I/O Input fall time	Input/reception mode [1]	-	-	1	µs
$t_{r(o)(IO)}$	I/O Output rise time	Output/transmission mode;CL = 30 pF [1]	-	-	0.1	µs
$t_{f(o)(IO)}$	I/O Output fall time	Output/transmission mode;CL = 30 pF [1]	-	-	0.1	µs
Input/Output: SDA, SCL according to [2]						
$t_{f(i)(IO)}$	SDA Input fall time	Input/reception mode [2]	-	-	80	ns
	SCL Input fall time	Input/reception mode [2]	-	-	40	ns
$t_{r(o)(IO)}$	SDA/SCL Output rise time	Output/transmission mode, GPIO mode, CL = 150 pF [2]	-	-	50	ns
$t_{f(o)(IO)}$	SDA/SCL Output fall time	Output/transmission mode, GPIO mode, CL = 150 pF [2]	-	-	50	ns
$t_{f(o)(IO)}$	SDA Output fall time	Output/transmission mode, open-drain mode, CL = 100 pF [2]	-	-	80	ns
$t_{f(o)(IO)}$	SDA Output fall time	Output/transmission mode, open-drain mode, CL = 400 pF [2]	-	-	160	ns
$t_{SU:DAT\_HS}$	data set-up time (I^2C HS mode)	CPU clock = 48 MHz	20	-	-	ns
General						
t_{PD}	Power down duration time (I^2C/SPI wake-up)	CPU clock = 48 MHz [3]	-	-	60	µs
C_{PIN}	Pin capacitances IO2, SDA, SCL	Test frequency = 1 MHz; T_{amb} = 25 °C	-	-	11	pF
R_{on}	Resistance of power switch	T_{amb} = 105 °C, V_{in} = 1.65 V	-	-	1.1	Ω
I_{out}	maximum current driving capability of pin Vout	T_{amb} = 105 °C	-	-	25	mA

Table 15. Electrical AC characteristics of I/O2, SDA, SCL, SDI (CLK), and V_{OUT} *...continued*

Conditions: V_{DD}, V_{IN} = 1.65 V to 3.6 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
General - I^2C specific						
f_{CLK}	External clock frequency on pad SCL in I^2C applications	tCLKW, T_{amb} and V_{DD} in their specified limits, CPU clock = 48 MHz	-	-	3.4	MHz
t_{DPD}	Deep Power down duration time (I^2C wake-up)	CPU clock = 48 MHz [4]	-	-	300	µs

[1] t_r is defined as rise time between 10 % and 90 % of the signal amplitude. t_f is defined as fall time between 90 % and 10 % of the signal amplitude.
[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: A wakeup request shall not be sent during this timeframe as this prevents SE052 entering power down mode.
[4] Wakeup from deep power down: A wakeup request shall not be sent during this timeframe as this prevents SE052 entering the deep power down mode.

Table 16. Electrical AC characteristics of LA, LB

Conditions: T_{amb} = -40 °C to 105 °C, unless otherwise specified

Symbol	Parameter	Conditions	Typ [1]	Unit
Input/Output: LA, LB				
C_{LALB} [2]	Pin capacitance LA, LB Bare die (SO 28, empty package ground-off)	Configured for antenna input with 56 pF capacitance, test frequency = 13.56 MHz; T_{amb} = 25 °C, $V_{LA, LB}$ = 2.25 V (rms) [3] [4]	59	pF
		Configured for antenna input with 56 pF capacitance, test frequency = 13.56 MHz; T_{amb} = 25 °C, $V_{LA, LB}$ = 0.35 V (rms) [3] [4]	52.8	pF
R_{LALB} [2]	Pin resistance LA, LB Bare die (SO 28, empty package ground-off)	Configured for antenna input with 56 pF capacitance [5] (SO 28) test frequency = 13.56 MHz; T_{amb} = 25 °C, $V_{LA, LB}$ = 2.25 V (rms) [3] [4]	0.5	kΩ
f_{LALB}	Operating frequency LA, LB		13.56	MHz

[1] Typical values (± 10 %) are only referenced for information. They are subject to change without notice.
[2] The C_{LALB} and R_{LALB} 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 family member data sheets
[4] Measured with sine wave at LA, LB.
[5] 56 pF selection supports all data rates with ID1 antenna (Class 1), however, only 106 kbit/s with 1/2 ID1 antenna (Class 2).

14.2 Non-volatile memory

Table 17. Non-volatile memory characteristics

Conditions: V_{DD} = 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		-	1.4	-	ms
t_{EEW}	FLASH program time		-	0.9	-	ms
t_{EER}	FLASH data retention time	T_{amb} = 55 °C	25	-	-	years
N_{EECM}	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	120×10^6	-	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.

15 References

[1] Application Note, SE052 Configuration Details, document number AN14277. Available on NXP website.
[2] NXP SE05x T=1 Over I^2C Specification User Manual, document number 11225. Available on NXP website.
[3] APDU Transport over SPI/I^2C v1.0 | GPC_SPE_172. Available via Global platform.

16 Revision history

Table 18. Revision history

Document ID	Release date	Description
SE052 v.1.5	03 June 2024	Product data sheet
Modification	• Amended FIPS certification specification in Section 1	
SE052 v.1.4	16 April 2024	Product data sheet
Modification	• Updated in Section 6 the link from SOT917-7 (DD) to SOT917-7 • Removed in Section 10 references to SE051 • added trademarks for EdgeLock, and I^2C to the legal information	
SE052 v.1.3	03 April 2024	Product data sheet
Modification	• Updated pin 14 RST to RST_N • Updated the link to the SOT number, see Section 6 • refrased the last paragraph in the Introduction topic	
SE052 v.1.2	21 March 2024	Product data sheet
Modification	• moved "SE052F preconfigured variant for ease of use" to AN14277 • added Healthcare, to Applications • added link to AN14277 in General Description • added bullet to Section 3.1 • updated Section 4 • corrected the number of units per reel in Section 8.1 from 3000 to 6000 • changed status to public	

Table 18. Revision history...*continued*

Document ID	Release date	Description
SE052 v.1.1	23 November 2023	Objective data sheet
Modification	• removed temperature setting: Standard, 25 °C to 85 °C, in Table 1 • added chain of trust certificates, Secure objects configuration, and X.509 Certificate Storage encoding	
SE052 v.1.0	23 November 2023	Objective data sheet

Legal information

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 https://www.nxp.com.

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.

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 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.

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 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.

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

Contents

1 Introduction 1
1.1 SE052 Use Cases 1
1.2 Applications 1
2 General description 2
2.1 Key benefits 2
3 Features and benefits 3
3.1 Product-specific features 3
4 Ordering information 3
5 Pinning 4
5.1 Pin description HVQFN20 4
6 Package 5
7 Marking 5
8 Packing information 5
8.1 Reel packing 5
9 I2C interface 6
9.1 Introduction 6
10 Power-saving modes 7
10.1 Introduction 7
10.2 Power-down mode 7
10.3 Deep Power-down mode 7
11 Limiting values 8
12 Recommended operating conditions 9
13 Static characteristics 10
13.1 Measurement conventions 10
13.2 Level and currents 10
13.2.1 General and ISO7816 I/O interface 10
13.2.1.1 Pads SDA and SCL 14
13.3 Configuration settings 15
13.4 General A/5 V, class B/3 V, or class C/1.8 V class operation 18
14 Dynamic characteristics 19
14.1 General, ISO/IEC 7816, ISO/IEC 14443 I/O and I2C I/O 19
14.2 Non-volatile memory 23
15 References 23
16 Revision history 23
Legal information 25

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

Date of release: 3 June 2024
Document identifier: SE052
Document number: 789115