A71CL

Plug & Trust Secure Element

Rev. 3.1 — 10 September 2020
512331

Product short data sheet
COMPANY PUBLIC

1. Introduction

The A71CL is a ready-to-use solution providing a root of trust at the IC level and proven, chip-to-cloud security right out of the box. It is a platform capable of securely storing and provisioning credentials, securely connecting IoT devices to cloud services and performing cryptographic node authentication.

The A71CL solution provides security measures protecting the IC against physical and logical attacks. The solution is meant to be integrated with a host platform and running operating systems adding a chain of trust for a broad range of applications. The product is delivered with a manual and documents to provide guidance on its integration.

2. General description

2.1 A71CL naming conventions

The following table explains the naming conventions of the commercial product name of the A71CL products. Every A71CL product gets assigned such a commercial name, which includes also customer and application specific data.

The A71CL basic type names have the following format.

A71CLxagpp(p)

The 'A71CL' is a constant, all other letters are variables, which are explained in Table 1.

Table 1. A71CL commercial name format

Variable	Meaning	Values	Description
x	IC hardware specification code	1	standard operational ambient temperature: –25 °C to +85 °C I^2C interface supported
		2	standard operational ambient temperature: –40 °C to +90 °C I^2C interface supported
a	embedded operating system code	C	Java card operating system
g	embedded application firmware (applet) code	L	L is a fixed value = IoT security applet pre installed
pp(p)	package type code dd(d)= Delivery Type, TK2= HVSON8 (4x4)		

2.2 I^2C interface

The A71CL has an I^2C interface in slave mode, supporting data rates up to 400 kbit/s operating in Fast-Mode (FM). The I^2C interface is using the Smartcard I^2C protocol as defined in Ref. 3 which is based on SMBus.

Depending on the interface pins state at boot, see Section 7 "Pinning information" for more details; the default I^2C address after power-on-reset is 0x90 for Write, and 0x91 for Read.

2.3 Security licensing

NXP Semiconductors has obtained a patent license for SPA and DPA countermeasures from Cryptography Research Incorporated (CRI). This license covers both hardware and software countermeasures. It is important to customers that countermeasures within the operation system are covered under this license agreement with CRI. Further details can be obtained on request.

3. Features and benefits

3.1 Key benefits

- Secure, zero-touch connectivity
- End-to-end security, from chip to edge to cloud
- Secure credential injection for IC-level root of trust
- Fast design-in with complete product support package
- Easy to integrate with different MCU platforms

3.2 Security features

The A71CL security concepts includes many security measures to protect the chip.

The A71CL operates fully autonomously based on an integrated Javacard operating system and applet. Direct memory access is possible by the fixed functionalities of the applet only. With that, the content from the memory is fully isolated from the host system.

Attack protection by integrated design measures in the chip layout, the logic and the functional blocks.

3.3 Cryptography features

- Message digest with SHA1, SHA224, SHA256
- Random number generator
- Asymmetric key storage type: RSA Standard or RSA CRT
- Auto RSA key generator ranges from 512-bit key length to 2048-bit key length. Either RSA Standard or RSA CRT.
- Symmetric encryption/decryption with DES_CBC_NOPADDING, DES_ECB_NOPADDING, AES_CBC_NOPADDING, AES_ECB_NOPADDING.
- Symmetric signature/verification with DES_CBC_ISO9797_M1, DES_CBC_ISO9797_M2, AES_CBC_ISO9797_M1, AES_CBC_ISO9797_M2.
- Asymmetric encryption/decryption with RSA_NOPADDING, RSA_ PKCS1.
- Asymmetric signature/verification with RSA_SHA1(PKCS1), RSA_SHA256.
- Service data storage: the storage data read and write is protected by SCP.
- SCP 02 service with option “i” = ‘55’.

3.4 Functional features

- 400 kbit/s I^2C Fast-mode interface
- –40 °C to +90 °C operational ambient temperature (A7102)
- On-chip Javacard operating system
- 40 μA typical sleep mode current with I^2C pads in tristate mode
- 10 μA max deep sleep mode current with I^2C pads in tristate mode
- High-performance Public Key Infrastructure (PKI)
- EEPROM with min 500,000 cycles endurance and min 25 years retention time
- HVSON8 package

4. Applications

4.1 Use Cases and target applications

- A710xCL EXAMPLE USE CASES
  - Secure connection to public/private clouds, edge computing platforms, infrastructure
  - Secure commissioning
  - Device-to-device authentication
  - Proof of origin / anti-counterfeiting
  - Key storage and data protection
- A710xCL TARGET APPLICATIONS
  - Connected industrial devices
  - Sensor networks
  - IP cameras
  - Home gateways
  - Home appliances

5. Ordering information

5.1 Ordering options

Table 2. Ordering information

Type number[1]	Package		
	Name	Description	Version
A7101agTK2/...	HVSON-8	plastic thermal enhanced very thin small outline package; no leads; 8 terminals; body 4 × 4 × 0.85 mm	SOT909-1
A7102agTK2/...			

[1] a = A or C, g = G, C or A, according to the A71CL type classification see Section 2.1 “A71CL naming conventions”

Table 3 gives an overview of available A71CL product types.

Table 3. A71CL feature table

Product type[1]	Operational ambient temperature	Interface option
A7101CLpp(p)	−25 °C to +85 °C	I^2C
A7102CLpp(p)	−40 °C to +90 °C	

[1] HN1, according the A71CL type classification see Section 2.1 “A71CL naming conventions”

Table 4. A71CL type description

Orderable type	Product type number	12NC	Operational ambient temperature	Description
A7101CLTK2/T0BC2—[1]	A7101CLTK2/T0BC2BY	935380944118	−25 °C to +85 °C	Customer Programmable[1]
A7101CLTK2/T0BC27J	A7101CLTK2/T0BC27F	935372576118	−25 °C to +85 °C	Baidu Cloud credential
A7102CLTK2/T0BC2AJ[1]	A7102CLTK2/T0BC2XQ	935379153118	−40 °C to +90 °C	

[1] product can be made available, please consult our sales for more details

5.1.1 Ordering A71CL samples

Samples can be ordered from NXP Semiconductors from the NXP website.

Note that NXP Semiconductors can provide up to 5 pieces free of charge. Larger quantities have to be ordered separately.

6. Functional description

6.1 I²C Interface

The A71CL uses I²C as communication interface as described in the following section. The A71CL commands are wrapped using the Smartcard I² protocol (SCI2C). The detailed documentation for the A71CL commands in the APDU Specification and SCI2C encapsulation (Ref. 3) is available in NXP DocStore.

The A71CL has an I²C interface in slave mode, supporting data rates up to 400 kbit/s operating in Fast-Mode (FM). The I²C interface is using the Smartcard I²C protocol as defined in Ref. 3 which is based on SMBus. Depending on the interface pins state at boot, see Section 7 for more details. The default I²C address after power-on-reset depends on the bootup condition as shown in Table 5.

6.2 Automatic Communication Mode detection at Power on

The IC configures its interface according to the pin state as shown in the table below. The host system must keep the voltage levels stable at these pins for at least 500 µs after power-on-reset.

Table 5. I²C address

Value at startup				I²C address	
IF0	IF1	I2C_SCL	I2C_SDA	Write	Read
0	x	0	0	n.a.	n.a.
1	0	1	1	0x90	0x91
1	1	1	1	0x92	0x93

6.3 Power-saving modes

The device provides two power-saving operation modes, the SLEEP mode and the DEEP SLEEP mode. These modes are activated via pad RST_N (DEEP SLEEP mode) or by the device.

6.3.1 SLEEP mode

The SLEEP 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 A71CL enters automatically into SLEEP mode and also wakes up automatically from SLEEP mode. In SLEEP mode, all internal clocks are stopped. The IOs hold the logical states they had at the time IDLE was activated. During SLEEP mode security sensors HVS, LVS, LTS, HTS, Light Sensors, Glitch Sensors and Active Shielding are disabled.

There are two ways to exit from the SLEEP mode:

- A reset signal on RST_N
- An External Interrupt edge triggered by a falling edge on I2C_SDA

6.3.2 DEEP SLEEP mode

The A71CLx provides a special sleep mode offering maximum power saving. It is reached by pulling RST_N to a logic zero level for more than 500 µs.

While in deep sleep mode the internal power is completely switched off and only the IO pads stay supplied. All digital pads will stay in high-Z mode.

To leave the DEEP SLEEP mode RST_N has to be released and set to a logic „1“ level.

7. Pinning information

7.1 Pinning

7.1.1 Pinning HVSON8

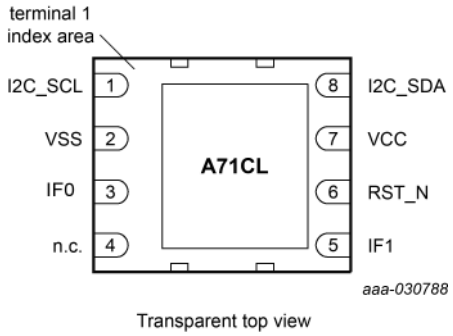


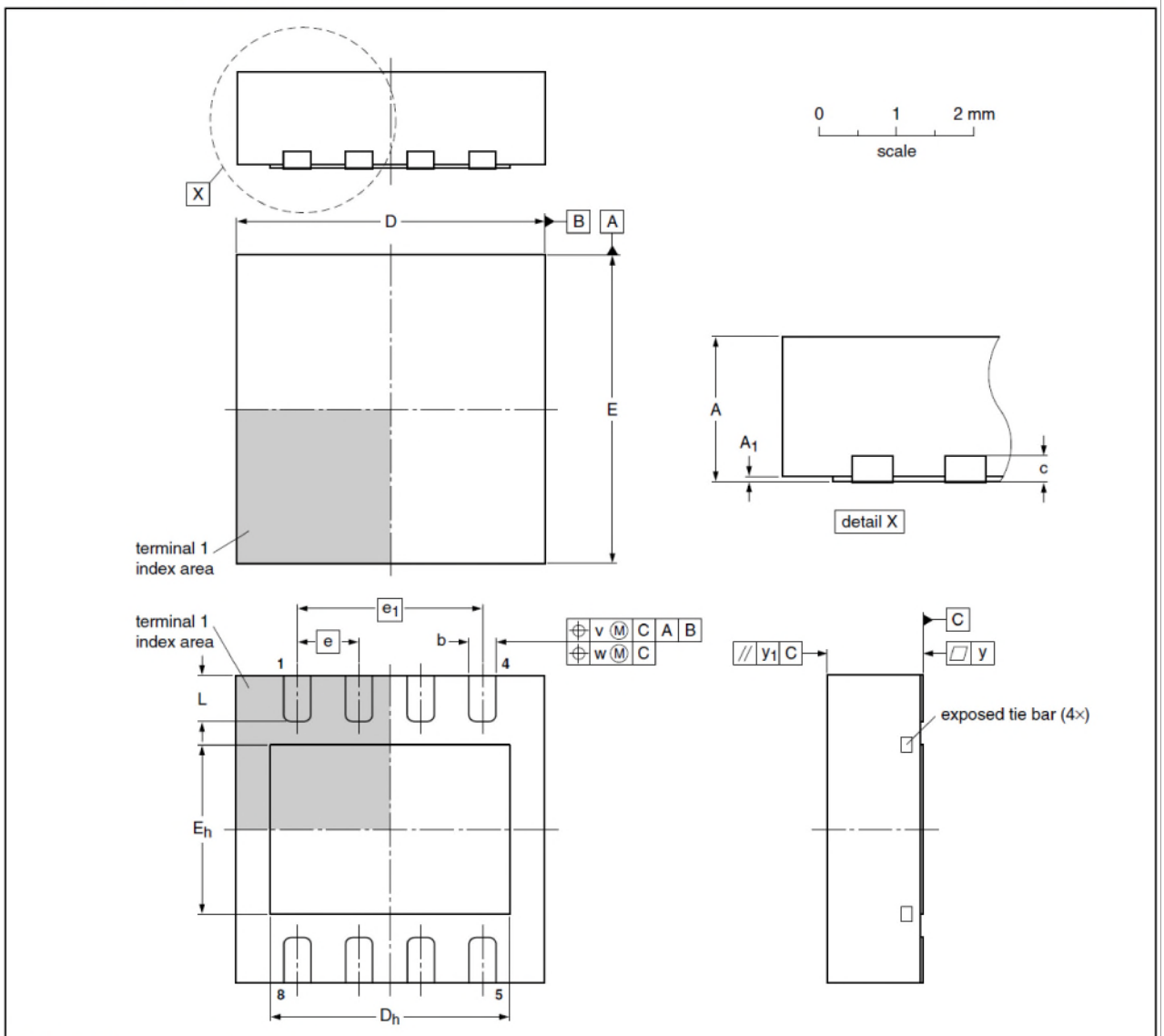
Fig 1. Pin configuration for HVSON-8 (SOT909-1)

Table 6. Pin description HVSON8

Symbol	Pin	Description
I2C_SCL	1	I^2C clock
VSS	2	ground
IF0	3	interface activation, apply high on startup
n.c.	4	not connected
IF1	5	I^2C address selection
RST_N	6	reset input, active LOW
VCC	7	power supply voltage input
I2C_SDA	8	I^2C data

8. Package outline

HVSON8: plastic thermal enhanced very thin small outline package; no leads;
8 terminals; body 4 x 4 x 0.85 mm SOT909-1



DIMENSIONS (mm are the original dimensions)

UNIT	A(1) max.	A1	b	c	D(1)	Dh	E(1)	Eh	e	e1	L	v	w	y	y1
mm	1	0.05 0.00	0.4 0.3	0.2	4.1 3.9	3.25 2.95	4.1 3.9	2.35 2.05	0.8	2.4	0.65 0.40	0.1	0.05	0.05	0.1

Note

1. Plastic or metal protrusions of 0.075 mm maximum per side are not included.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT909-1		MO-229				~~05-09-26~~ 05-09-28

Fig 2. Package outline SOT909-1

9. Packing information

9.1 Reel packing

The A71CL product is available on 7” tape on reel and 13” tape on reel. Details are provided in Table 7.

Table 7. Reel packing options

Package type	Reel type	Minimum packing quantity
HVSON8	7” tape on reel	1500
HVSON8	13” tape on reel[1]	6000

[1] For details about packing method, product orientation, tape dimensions and labeling for A71 parts in HVSON8 package having an ordering code (12NC) ending 118 refer to Ref. 2.

10. 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 Ref. 1).

11. Limiting values

Table 8. Limiting values

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

Symbol	Parameter	Conditions		Min	Max	Unit
V_{DD}	supply voltage			-0.3	+4.6	V
V_I	input voltage	any signal pad		-0.3	+4.6	V
I_I	input current	pad I2C_SDA, I2C_SCL		-	10	mA
I_O	output current	pad I2C_SDA, I2C_SCL		-	10	mA
I_{lu}	latch-up current	$V_I < 0$ V or $V_I > V_{DD}$		-	100	mA
V_{esd_hbm}	electrostatic discharge voltage (Human Body Model)	pads VCC, VSS, RST_N, I2C_SDA, I2C_SCL	[1]		± 2.0	kV
V_{esd_cdm}	electrostatic discharge voltage (Charge Device Model)	pads VCC, VSS, RST_N, I2C_SDA, I2C_SCL	[3]		± 500	V
P_{tot}	Total power dissipation		[2]	-	1	W
T_{stg}	Storage temperature			-55	+125	°C

[1] MIL Standard 883-D method 3015; human body model; C = 100 pF, R = 1.5 kΩ; T_{amb} = −25 °C to +85 °C.

[2] Depending on appropriate thermal resistance of the package.

[3] JESD22-C101, JEDEC Standard Field induced charge device model test method.

12. Recommended operating conditions

The A71CL offers two operation modes, the so-called 1V8 mode and the 3V3 mode targeted for battery supplied applications.

Table 9. Recommended operating conditions

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{DD}	supply voltage range	3V3 mode range CPU in free runing mode		2.50	3.3	3.6	V
		1V8 mode		1.62	1.8	1.98	V
V_I	DC input voltage on digital I/O pads I2C_SCL, I2C_SDA	3V3 mode		0		3.6	V
		1V8 mode		0		3.6	V
V_I	DC input voltage on digital input pad RST_N	3V3 mode		0		3.6	V
		1V8 mode		0		3.6	V
T_{amb}	Operating ambient temperature	A7101		-25		+85	°C
		A7102		-40		+90	°C

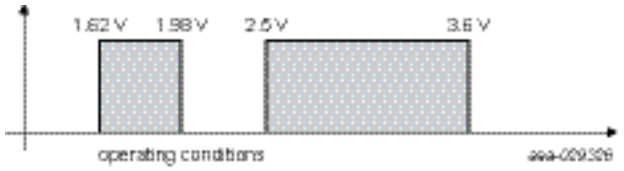


Fig 3. Recommended operating conditions over voltage range

13. Characteristics

13.1 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.

13.1.1 General and I²C I/O interface

Table 10. Electrical DC characteristics of I2C_SCL, I2C_SDA and RST_N

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
Input/Output: I2C_SCL, I2C_SDA in push-pull mode							
V_{IH}	HIGH level input voltage			0.7 V_{DD}		V_{Imax}[1]	V
V_{IL}	LOW level input voltage			-0.5		0.3 V_{DD}	V
I_{IH}	HIGH level input current in input mode	$V_{IHmin} < V_I < V_{IHmax}$				± 10	µA
I_{IL}	LOW level input current	$V_{ILmin} < V_I < V_{ILmax}$				± 10	µA
V_{OH}	HIGH level output voltage	I_{OH} = −3.0 mA; 3V3 mode	[2]	0.7 V_{DD}			V
		I_{OH} = −3.0 mA; 1V8 mode	[2]	0.7 V_{DD}			V
V_{OL}	LOW level output voltage	I_{OL} = 3.0 mA 3V3 mode				0.4	V
		I_{OL} = 2.0 mA 1V8 mode				0.2 V_{DD}	V
Input/Output: I2C_SCL, I2C_SDA in open-drain mode							
V_{IH}	HIGH level input voltage			0.7 V_{DD}		V_{Imax}[1]	V
V_{IL}	LOW level input voltage			-0.5		0.3 V_{DD}	V
I_{IH}	HIGH level input current in input mode	$V_{IHmin} < V_I < V_{IHmax}$				± 10	µA
I_{IL}	LOW level input current	$V_{ILmin} < V_I < V_{ILmax}$				± 10	µA
V_{OL}	LOW level output voltage	I_{OL} = 3.0 mA 3V3 mode				0.4	V
		I_{OL} = 2.0 mA 1V8 mode				0.2 V_{DD}	V
Input: RST_N							
V_{IH1}	HIGH level input voltage			0.7 V_{DD}		V_{Imax}[1]	V
V_{IL1}	LOW level input voltage			-0.3		0.3 V_{DD}	V
I_{IH1}	HIGH level RST_N input current	$V_{IH1min} \leq V_I \leq V_{DD}$	[3]			± 20	µA
I_{IL1}	LOW level RST_N input current	0 V ≤ V_I ≤ V_{IL1max};	[3]			± 20	µA

[1] Maximum value according to Table 9 “Recommended operating conditions”

[2] : External pull-up resistor 20 kΩ to VDD. 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_{OHmin} = 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} (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_{OHmin} is specified as “the larger value of 0.7 V_{DD} and 3.8 V, respectively”.

[3] The active low RST_N input internally has a resistive pull-down device to VSS. Accordingly a current is flowing into the pad voltages above 0 V. Figure 4 shows the RST_N input characteristic.

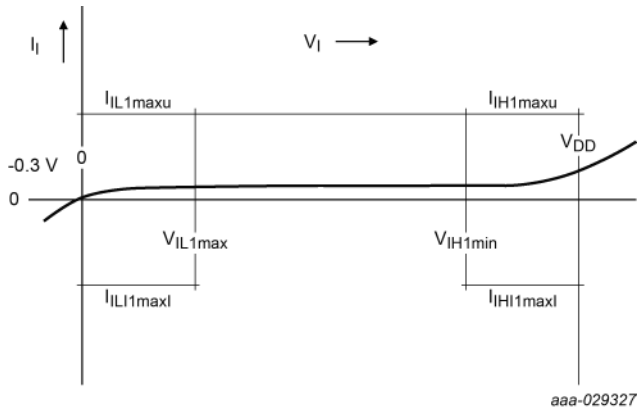


Fig 4. Input characteristic of RST_N

13.1.2 I²C interface at 3V3 mode operation[1]

Table 11. Electrical characteristics of IC supply voltage V_{DD}; V_{SS} = 0 V; T_{amb} = -40 to +90 °C

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
Supply							
V_{DD}	supply voltage range	3V3 mode range CPU in free running mode		2.50	3.3	3.6	V
I_{DD}	no coprocessor active	CPU in free running mode			6.3	7.0	mA
	EPROM programming in progress	CPU in free running mode			7.3	8.0	mA
	AES coprocessor active	CPU in free running mode			9.3	10.3	mA
	ECC coprocessor active	CPU in free running mode			13.7	15.1	mA
$I_{DD(SLP)}$	supply current SLEEP mode	T_{amb} = 25 °C			45	150	µA
$I_{DD(DSLP)}$	supply current deep sleep mode	RST_N at 0V, T_{amb} = 25 °C				10	µA
		RST_N at 0V, T_{amb} = 90 °C				10	µA

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

13.1.3 I²C interface at 1V8 mode operation[1]

Table 12. Electrical characteristics of IC supply voltage V_{DD}; V_{SS} = 0 V; T_{amb} = -40 to +90 °C

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
Supply							
V_{DD}	supply voltage range	1V8 mode range		1.62	1.8	1.98	V
I_{DD}	no coprocessor active	CPU in free running mode			2.45		mA
	AES coprocessor active	CPU in free running mode			2.7		mA
	ECC coprocessor active	CPU in free running mode			7.5		mA
$I_{DD(SLP)}$	supply current SLEEP mode	T_{amb} = 25 °C			40	80	µA
$I_{DD(DSLP)}$	supply current deep sleep mode	RST_N at 0V, T_{amb} = 25 °C				10	µA
		RST_N at 0V, T_{amb} = 90 °C				10	µA

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

13.2 AC characteristics

Table 13. Non-volatile memory timing characteristics; V_{DD} = 1.8 V ± 10% or 3 V ± 10% V; V_{SS} = 0 V; T_{amb} = -40 to 90 °C

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
t_{EEP}	EEPROM erase + program time				2.7		ms
t_{EEE}	EEPROM erase time				1.7		ms
t_{EEW}	EEPROM program time				1.0		ms
t_{EER}	EEPROM data retention time	T_{amb} = +55 °C		25			years
N_{EEC}	EEPROM endurance (number of programming cycles)			5×10^5			cycles

Table 14. Electrical AC characteristics of I2C_SDA, I2C_SCL, and RST_N[1]; V_{DD} = 1.8 V ± 10% or 3 V ± 10% V; V_{SS} = 0 V; T_{amb} = -40 to 90 °C

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
Input/Output: I2C_SDA, I2C_SCL in open-drain mode							
tr_{IO}	I/O Input rise time	Input/reception mode	[4]			1	µs
tf_{IO}	I/O Input fall time	Input/reception mode	[4]			1	µs
tf_{OIO}	I/O Output fall time	Output/transmission mode; C_L = 30 pF	[4]			0.3	µs
f_{CLK}	External clock frequency in I²C applications	t_{CLKW}, T_{amb} and V_{DD} in their spec'd limits		-		400	kHz
t_{CLKW}	Clock pulse width i.r.t. clock period (positive pulse duty cycle of CLK)		[3]	40		60	%
Inputs: RST_N							
t_{RW}	Reset pulse width (RST_N low) without entering deep sleep mode			40		400	µs
t_{RDSLP}	Reset pulse width (RST_N low) to enter deep sleep mode			500			µs
t_{WKP}	Wake-up time from SLEEP mode	$f_{CLKmin} < f_{CLK} < f_{CLKmax}$		-	8	10	µs

Table 14. Electrical AC characteristics of I2C_SDA, I2C_SCL, and RST_N[1]; V_{DD} = 1.8 V ± 10% or 3 V ± 10% V; V_{SS} = 0 V; T_{amb} = -40 to 90 °C

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
t_{WKPIO}	Pad LOW time for wake-up from SLEEP 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 SLEEP mode			40		-	µs
t_{WKWT}	Time from SLEEP mode wake/up event to I2C_SDA valid				50	100	ns
C_{PIN}	Pin capacitances RST_N, I2C_SDA, /I2C_SCL	Test frequency = 1 MHz; T_{amb} = 25 °C		-		10	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 20% and 80% of the signal amplitude.
t_f is defined as fall time between 80% and 20% of the signal amplitude.

[3] During AC testing the inputs RST_N, I2C_SDA, I2C_SCL 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}.

[4] 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.

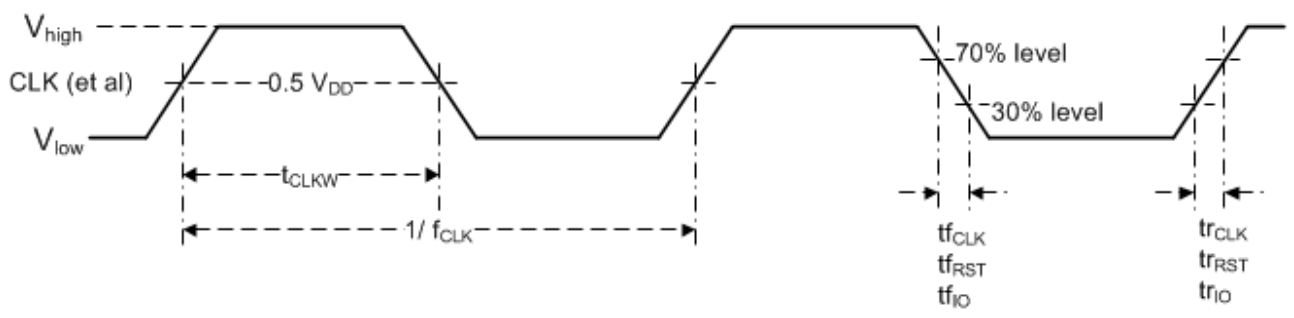


Fig 5. External clock drive and AC test timing reference points of I2C_SDA, I2C_SCL, and RST_N (see Table note [3] and Table note [4]) in open drain mode

13.3 EMC/EMI

EMC and EMI resistance according to IEC 61967-4.

14. Abbreviations

Table 15. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
CRC	Cyclic Redundancy Check
DES	Digital Encryption Standard
DPA	Differential Power Analysis
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read-Only Memory
I/O	Input/Output
MAC	Message Authentication Code
OS	Operating System
PKI	Public Key Infrastructure
SFI	Single Fault Injection
SHA	Secure Hash Algorithm

15. References

[1] I^2C-bus specification and user manual, Rev. 3.0 — June-19-2007, NXP Semiconductors

[2] SOT909-1; HVSON8; Reel pack; Ordering code (12NC) ending 118; Packing Information; Rev. 2 — 19 April 2013

[3] Application note SCIIC Protocol Specification, Application note, Rev 1.5, an195015 — 31 January 2017

[4] Application note A71CL Secure Module - APDU Specification, Application note, A71CL Secure Module - APDU Specification an515411

16. Revision history

Table 16. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
512331	2020-09-10	Short data sheet		512330
Modifications	Added footnote to table 4			
512330	2018-11-27	Short data sheet		-
Modifications:	• Initial version			

17. Legal information

17.1 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.

17.2 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.

17.3 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 here. **— 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. **— 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 **— 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 is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions. **— Security** — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products. **— 17.4Licenses**

ICs with DPA Countermeasures functionality

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.

17.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

FabKey — is a trademark of NXP B.V.

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

18. Contact information

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

For sales office addresses, please send an email to: **salesaddresses@nxp.com**

19. Tables

20. Figures

21. Contents

continued >>

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

Date of release: 10 September 2020
512331