OPTIGA™ Authenticate S Short Data Sheet

OPTIGA™ Authenticate Family

Description

This short data sheet describes the OPTIGA™ Authenticate S authentication device together with its features and functionality.

Features

Authentication

- 163-bit Elliptic Curve Cryptography (ECC) Engine
- 193-bit OPTIGA Digital Certificate (ODC)
- Message Authentication Code (MAC) function for user data authentication
- MAC based Host Authentication (selected sales codes)
- Customizable kill (end-of-life) features
- Unique Chip ID 96-bit

Non-Volatile Memory

- Lockable User NVM memory
- 32-bit page granularity
- Lifespan indicator

Communication Interface

- I2C I/O interface
- SWI I/O interface
- GPO as output interface

Package

- Package PG-TSNP-6-12

ESD

- JESD22-A114 ESD HBM 2KV standard
- JESC-C101 ESD CDM 500V standard
- IEC-61000-4-2 contact discharge 8KV for I/O pins
- IEC-61000-4-2 air discharge 15KV for I/O pins

Software

- Host-side library

Table of contents

1 Overview

1.1 Product Description

Infineon Technologies' novel OPTIGA™ Authenticate S Authentication chip offers a robust cryptographic solution that assists OEMs and system manufacturers to ensure the authenticity and safety of their original products, and protection of their investments against unauthorized after-market replacements.
It leverages Infineon's market leading security know-how into the battery and accessory authentication markets. With its innovative asymmetric cryptography approach, it significantly reduces system cost whilst making a leap in security.

1.2 Functional Overview

OPTIGA™ Authenticate S is designed to be used as a companion authentication device. This authentication device resides away from the host system such that the host system is able to check if it is communicating with an authenticated original device.

OPTIGA™ Authenticate S supports a configurable I2C interface and SWI interface to communicate with the Host controller. It is designed to conform to the I2C- bus specification and the Infineon SWI Bus Interface specification. The configuration of the interface link for the OPTIGA™ Authenticate S can be configured in the application board.

1.3 Typical Application

OPTIGA™ Authenticate S can be integrated into a host system supporting I2C interface as shown in Figure 1. It operates as an I2C slave device supporting 100 kHz and 400 kHz operating frequency. Depending on the selected frequency, the appropriate pull-up resistors need to be applied. I2C uses two wires to transmit data synchronously. One of the wires (SCL) carries the clock signal that is controlled by the I2C master and the other wire (SDA) is used to send and receive data. I2C is a widely used protocol and the transmission protocol is well-defined and well supported by many hardware architectures [1].

Apart from I2C communication support, OPTIGA™ Authenticate S also supports the Infineon SWI protocol. It requires only a single GPIO for input and output. A pull-up resistor, R_p, is required for the open-drain configuration. OPTIGA™ Authenticate S provides a combination of secured authentication function and user read/write storage space via a single serial interface (SWI). SWI is able to perform bidirectional communication on multiple devices on the bus without extra hardware. Communication on the SWI is using half-duplex transmission in which master and slave cannot transmit and receive commands concurrently. In the SWI architecture, an SWI master initiates and controls all the SWI operations. The SWI bus operates in command and response sequences. An additional feature of the SWI interface is the ability of interrupt-based processing which allows for concurrent processing.

Below figures show examples of a host system connection to an OPTIGA™ Authenticate S device in I2C and SWI configurations.

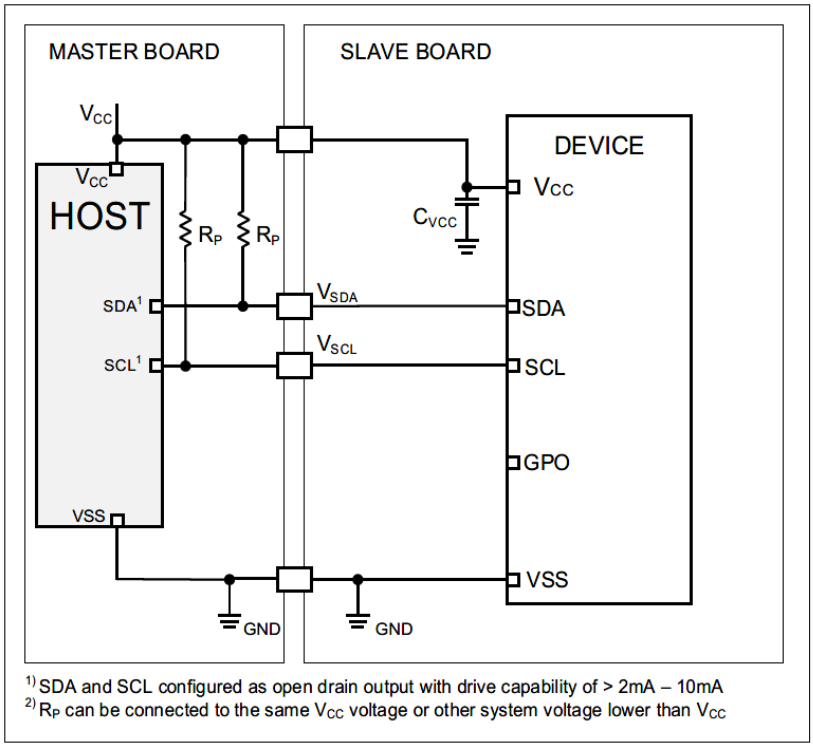


Figure 1 Application diagram of OPTIGA™ Authenticate S with I2C connectivity

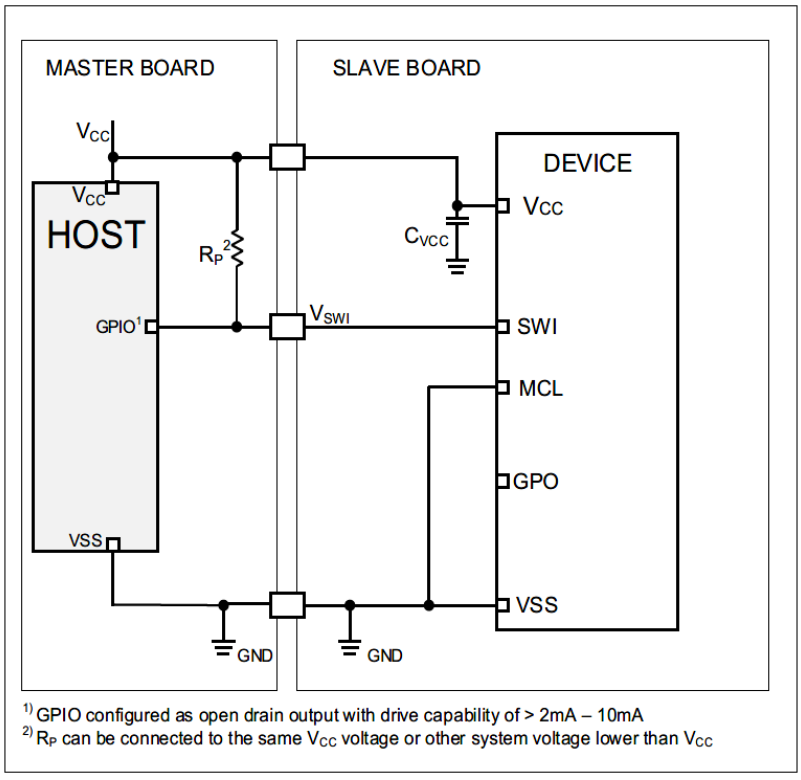


Figure 2 Application diagram of OPTIGA™ Authenticate S with SWI connectivity (direct powered)

Overview

In another typical application, OPTIGA™ Authenticate S can operate in indirect power mode where it is powered up by the communication line and is maintained powered during the communication transaction through the SWI communication. The resistor, R_P, maintains the power supply with a voltage drop of R_P multiplied by I_P. The voltage is fed to the OPTIGA™ Authenticate S's single wire interface port and its power supply through a diode.

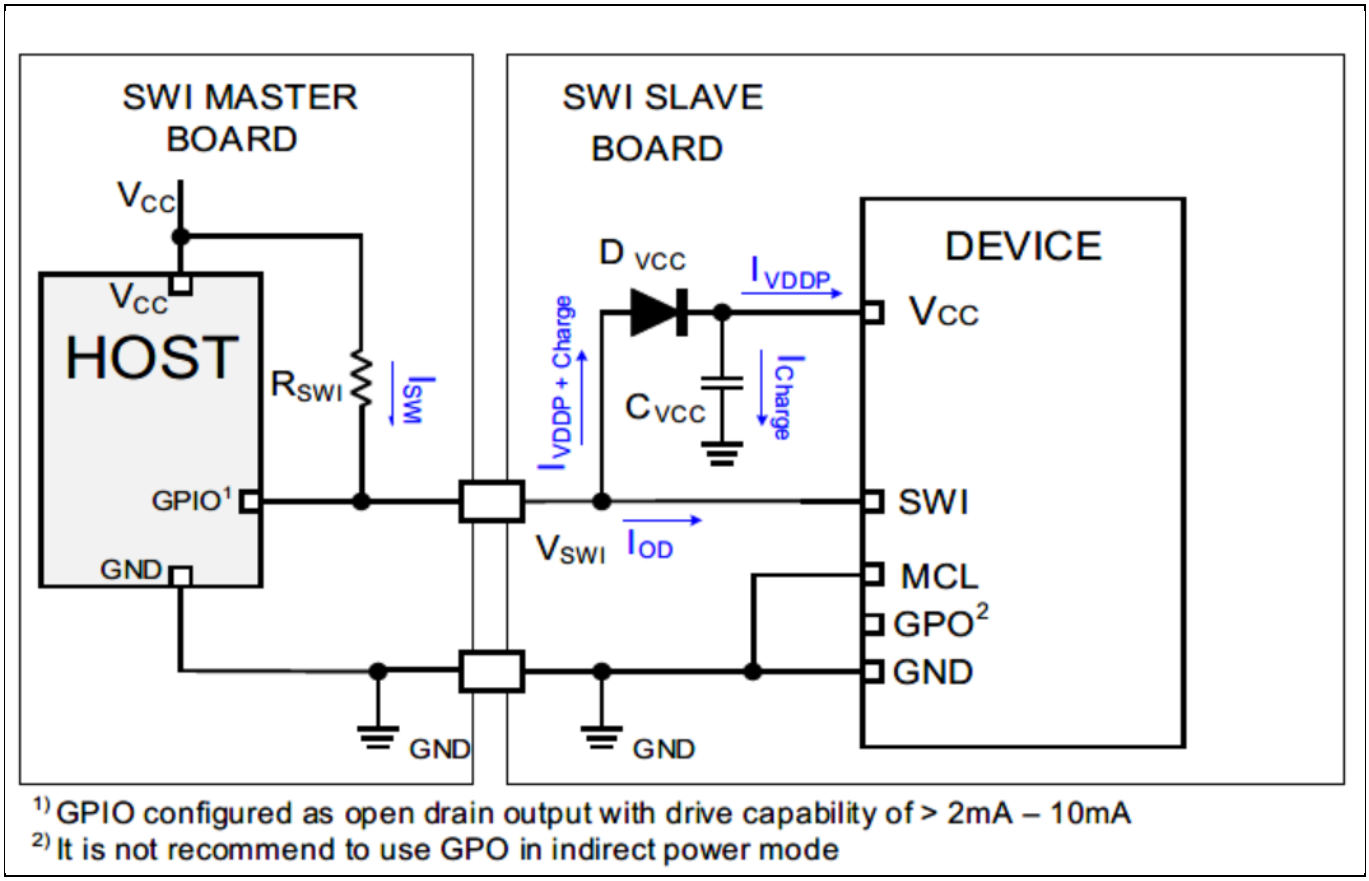


Figure 3 Application diagram of OPTIGA™ Authenticate S with SWI connectivity (Indirect powered)

2 Device Types/Order Information

The OPTIGA™ Authenticate S is available in the following standard temperature range shown in Table 1 and extended temperature range shown in Table 2.

Table 1 Device Configuration for standard temperature

Device Name	Package	Remarks
SLE95401	PG-TSNP-6-12	1Kbit User NVM
SLE95402	PG-TSNP-6-12	2Kbit User NVM
SLE95405	PG-TSNP-6-12	5Kbit User NVM
SLE95411	PG-TSNP-6-12	Host Authentication with 1Kbit User NVM
SLE95412	PG-TSNP-6-12	Host Authentication with 2Kbit User NVM
SLE95415	PG-TSNP-6-12	Host Authentication with 5Kbit User NVM

Table 2 Device Configuration for extended temperature

Device Name	Package	Remarks
SLE95401	PG-TSNP-6-12	1Kbit User NVM
SLE95402	PG-TSNP-6-12	2Kbit User NVM
SLE95405	PG-TSNP-6-12	5Kbit User NVM
SLE95411	PG-TSNP-6-12	Host Authentication with 1Kbit User NVM
SLE95412	PG-TSNP-6-12	Host Authentication with 2Kbit User NVM
SLE95415	PG-TSNP-6-12	Host Authentication with 5Kbit User NVM

3 Signals Description

OPTIGA™ Authenticate S is delivered in a PG-TSNP-6-12 package.

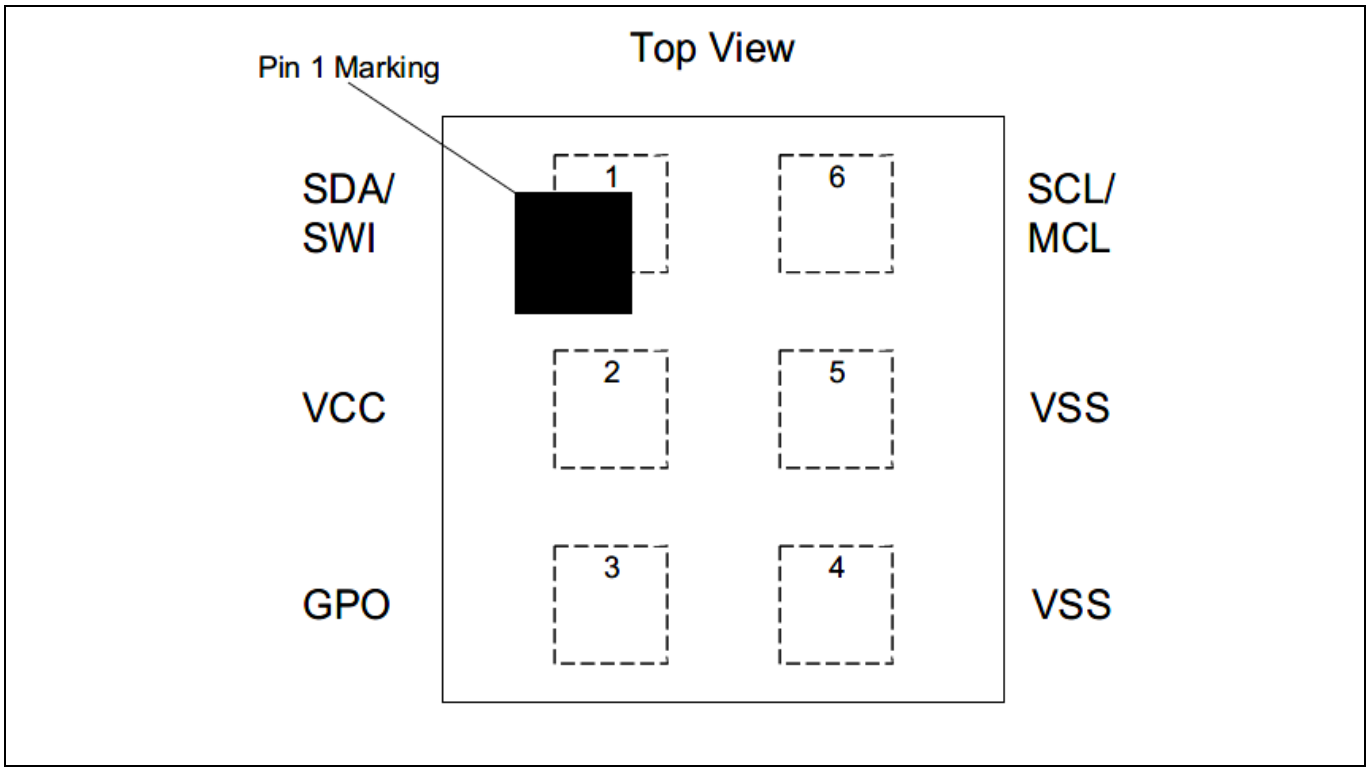


Figure 4 Pin configuration of OPTIGA™ Authenticate S

Table 3 I/O Signals

Pin No.	Name	Pin Type	Buffer Type	Function
1	SDA/SWI	I/O	OD	Serial Data (I2C Configuration) SWI
6	SCL/MCL	I	OD	Serial Clock (I2C Configuration) Must be connected to LOW (SWI Configuration)
3	GPO	O	PP	GPO

Table 4 Power Supply

Pin No.	Name	Pin Type	Buffer Type	Function
2	V_{CC}	PWR	-	Positive Power Input for device

Table 5 Ground Pins

Pin No.	Name	Pin Type	Buffer Type	Function
4,5	VSS	PWR	-	GND Pin This is the common ground of the IC. Pin 4 is the main ground of the package

Table 6 PG-TSNP-6-12 Package Dimensions

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min	Typ	Max		
A		1.45	1.50	1.55	mm	Package Width
B		1.45	1.50	1.55	mm	Package Length
		0.35	0.38	0.40	mm	Package Height
AC		0.25	0.30	0.35	mm	Solder Pad Width
BC		0.25	0.30	0.35	mm	Solder Pad Length
			0.60		mm	Solder Pad Pitch - X
			0.50		mm	Solder Pad Pitch - Y

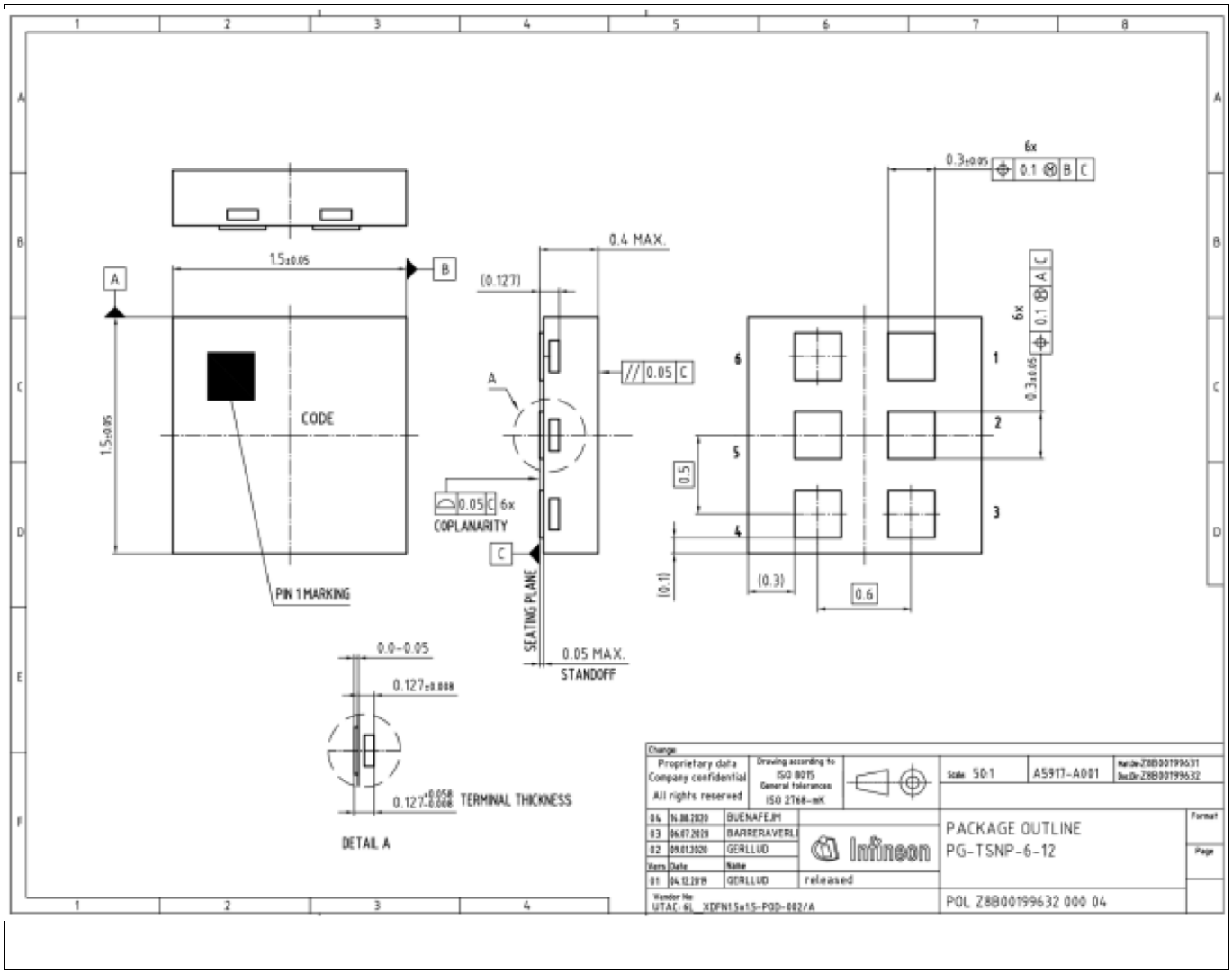


Figure 5 Package Dimensions

4 Packing Specification

4.1 Package Marking

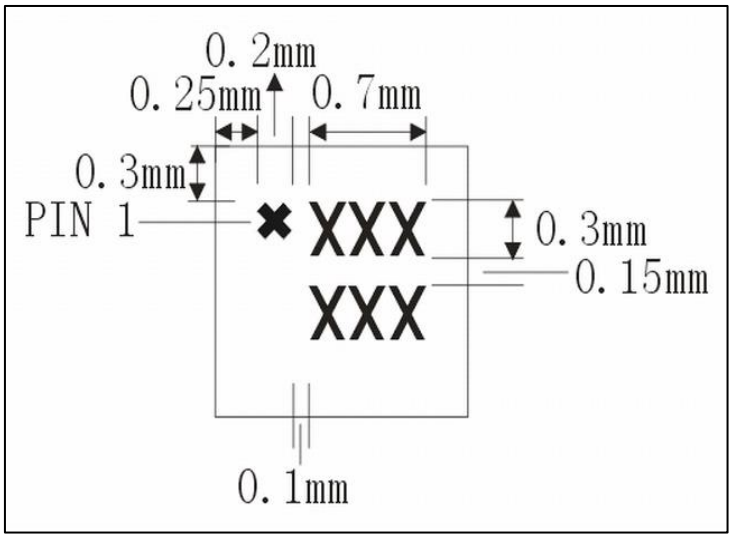
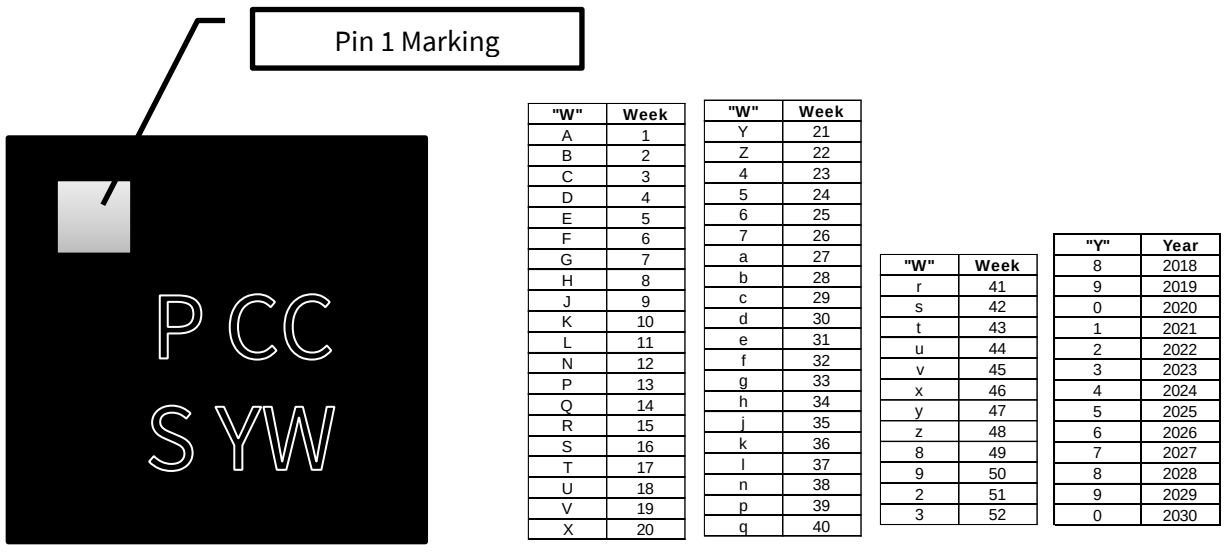


Figure 6 PG-TSNP-6-12 package marking and dimensions



"W"	Week
A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
J	9
K	10
L	11
N	12
P	13
Q	14
R	15
S	16
T	17
U	18
V	19
X	20

"W"	Week
Y	21
Z	22
4	23
5	24
6	25
7	26
a	27
b	28
c	29
d	30
e	31
f	32
g	33
h	34
j	35
k	36
l	37
n	38
p	39
q	40

"W"	Week
r	41
s	42
t	43
u	44
v	45
x	46
y	47
z	48
8	49
9	50
2	51
3	52

"Y"	Year
8	2018
9	2019
0	2020
1	2021
2	2022
3	2023
4	2024
5	2025
6	2026
7	2027
8	2028
9	2029
0	2030

Figure 7 Package laser marking

P refers to product number and CC refers to delivered customer code. S refers to sample code. YW refers to date code. The date code can be decoded using the supplied table.

4.2 Emboss Carrier Tape

Each box contains a single reel with 5000 pieces. Reel diameter is 180 mm.

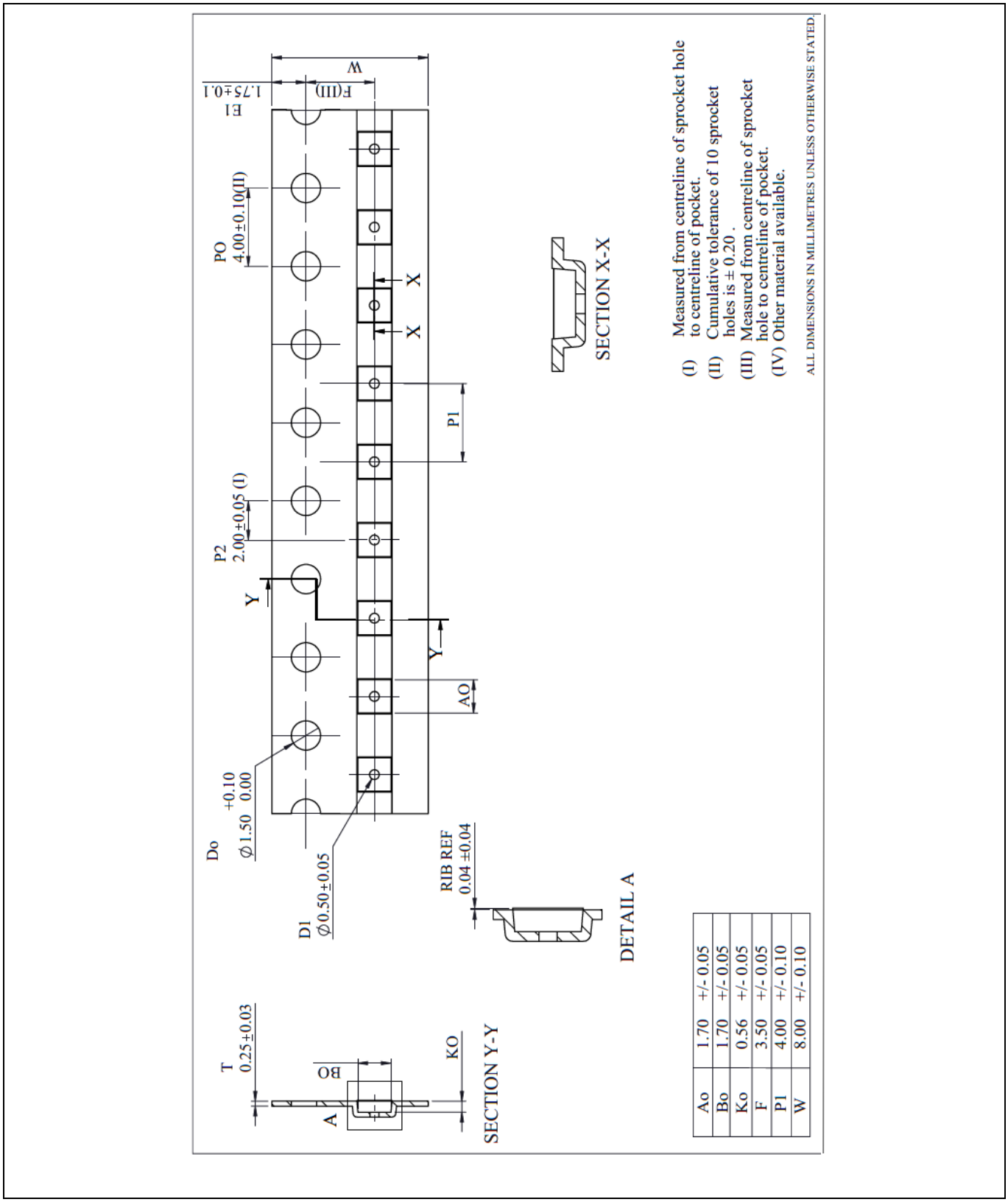


Figure 8 7-inch carrier tape specification

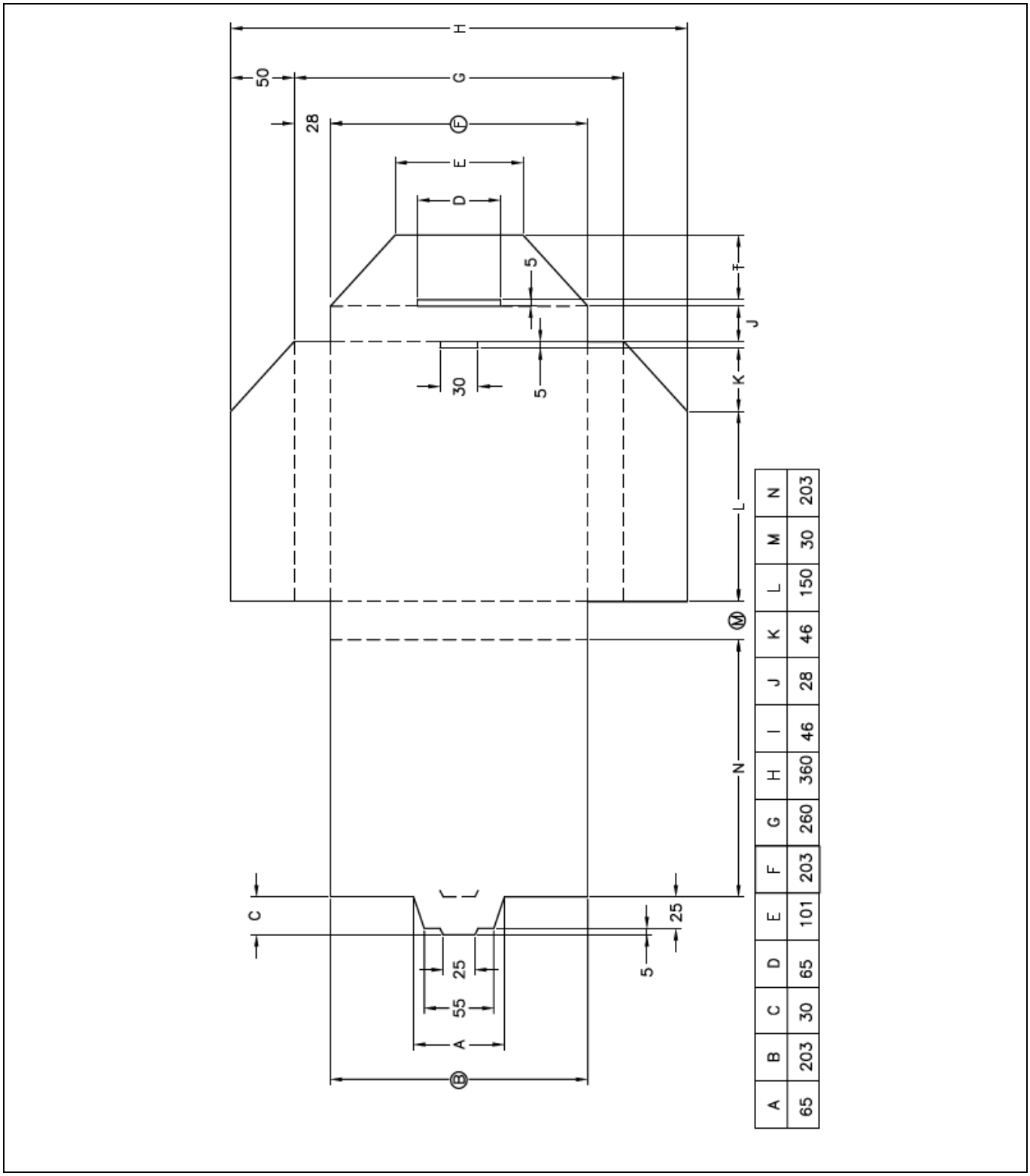
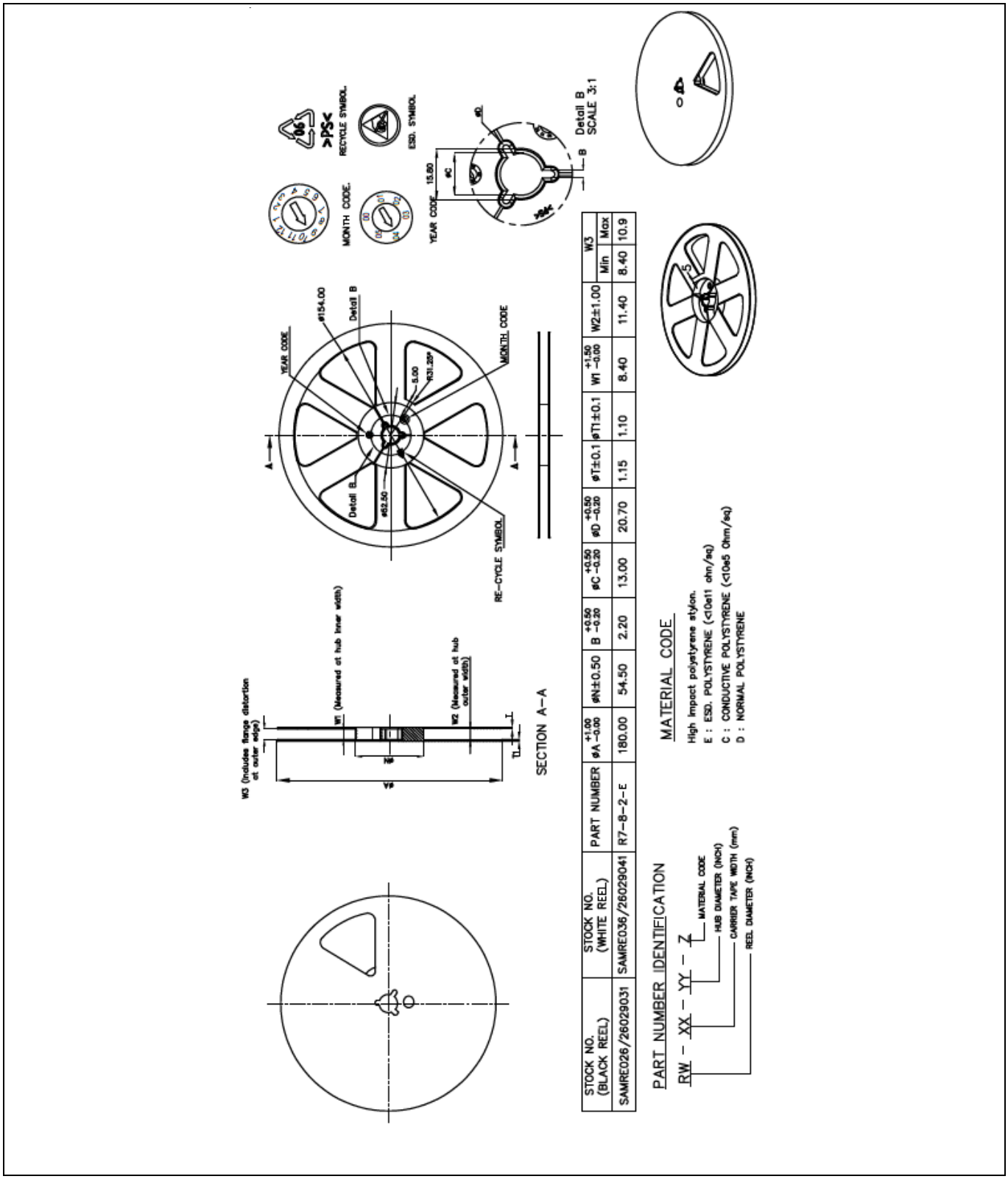


Figure 9 Box specification



STOCK NO. (BLACK REEL)	STOCK NO. (WHITE REEL)	PART NUMBER	øA +1.00 −0.00	øN±0.50	B +0.50 −0.20	øC +0.50 −0.20	øD +0.50 −0.20	øT±0.1	øT1±0.1	W1 +1.50 −0.00	W2±1.00	W3 Min	W3 Max
SAMRE026/26029031	SAMRE036/26029041	R7–8–2–E	180.00	54.50	2.20	13.00	20.70	1.15	1.10	8.40	11.40	8.40	10.9

Figure 10 7-inch reel specification

5 Electrical Characteristics

5.1 Absolute Maximum Ratings

Stresses above the maximum values listed here may cause permanent damage to the device. Exposure to absolute maximum rating conditions for extended periods may affect device reliability. Maximum ratings are absolute ratings; exceeding only one of these values may cause irreversible damage to the integrated circuit.

Table 7 Absolute Maximum Ratings

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
VCC Supply Voltage	V_{CC}	-0.3	–	6.0	V	
SCL Voltage	V_{SCL}	-0.3	–	6.0	V	
SDA Voltage	V_{SDA}	-0.3	-	6.0	V	
ESD robustness HBM	$V_{ESD,HBM}$	2000			V	According to JS-001-2012
ESD robustness CDM	$V_{ESD,CDM}$	500			V	According to JS-002-2018
Latch up	I_{LU}	100			mA	According to EIA/ JESD78
Storage Temperature	T_{STORE}	-55		150	°C	

5.2 Operating Conditions

Within the operational range, the IC operates as explained in the product description.
Typical Values: V_{CC}=3.8V, T_{AMB}=25 °C

Table 8 Operating Conditions

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
VCC supply voltage range	V_{CC}	1.8	3.8	5.5	V	Measurement is at the V_{CC} pin. Ramp up of V_{CC} shall be slower than 1µs
SCL voltage range	V_{SCL}	-0.3		5.5	V	For I2C interface only
SDA voltage range	V_{SDA}	-0.3		5.5	V	For I2C interface only
Current consumption, active idle mode	$I_{VCC, Active-Idle}$		0.38		mA	Idle Function Mode Averaged over 1s
Current consumption, active mode, authentication operation	$I_{VCC, Active-ECC}$		1.2		mA	Averaged over Authentication
Current consumption, active mode, host authentication operation	$I_{VCC, Active-HA}$		1.2		mA	Averaged over Authentication
Current consumption, power-down mode	$I_{VCC,PD}$		1.0		µA	SDA is set at 0V Maximum value condition is set at V_{CC} = 4.35V @ 85 °C
Ambient temperature	T_{AMB}	-40	25	85	°C	
Ambient temperature	$T_{AMB,110}$	-40	25	110	°C	
Ambient temperature	$T_{AMB,120}$	-40	25	120	°C	NVM Write Operation is prohibited above 110°C
Power-down low time	t_{PDL}	225.0			µs	
Power-up delay	t_{PUD}			10.0	ms	
Power-up delay	t_{PUD}			5.0	ms	From 0 °C to 40 °C
Soft reset delay	t_{SRD}			1.0	ms	

5.3 I2C Interface Characteristics (Standard Mode)

The table below defines the Standard Mode operation of the I2C interface. The I2C interface characteristics have been extracted from the I2C-bus specification.

Table 9 I2C Interface Characteristics (Standard Mode)

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Low-Level input voltage	V_{IL}	-0.3		0.3*V_{CC}	V	
High-Level input voltage	V_{IH}	0.7*V_{CC}		[1]	V	
Low-Level output voltage 1	$V_{OL,1}$			0.4	V	Open Drain or Open Collector at 3mA sink current; $V_{cc} > V_{cc(min)}$

Electrical Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Low-Level output current	I_{OL}	3.0			mA	V_{OL} = 0.4V
Output fall time from $V_{IH(MIN)}$ to $V_{IL(MAX)}$	t_{OF}			250[2)]	ns	
Input current for SDA/SCL pin	I_I	-10.0		10	µA	$0.1V_{CC} < V_I < 0.9V_{CC(MAX)}$
Capacitance for SDA/SCL pin	C_I[3)]			10	pF	

1) Maximum $V_{IH}=V_{CC(MAX)}$ + 0.5V or 5.5V whichever is lower
2) The maximum t_F for the SDA and SCL bus lines quoted in the below table (300ns) is longer than the specified maximum t_{OF} for the output stages (250ns). This allows a series protection resistor to be connected between SDA/SCL pins and the SDA/SCL bus lines without exceeding the maximum specified t_F.
3) Special purpose devices such as multiplexers and switches may exceed this capacitance because they connect multiple paths together

5.4 I2C Interface Timing Characteristics (Standard Mode)

The table below defines the interface timing characteristics for Standard Mode operation of the I2C interface. These have been extracted from the I2C-bus specification.

Table 10 I2C Interface Timing Characteristics (Standard Mode)

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
SCL Clock Frequency	f_{SCL}	0.0		100.00	kHz	
Hold time (repeated) START condition	$t_{HD,STA}$	4.0			µs	After this period, the first clock pulse is generated
Low Period for SCL	t_{LOW}	4.7			µs	
High Period for SCL	t_{HIGH}	4.0			µs	
Setup Time for a repeated START Condition	$t_{SU,STA}$	4.7			µs	
Data Hold Time	$t_{HD,DAT}$	0.0			µs	
Data Setup Time	$t_{SU,DAT}$	250.0			ns	
Rise time for SCL or SDA	t_R			1000	ns	Applicable to Master
Fall time for SCL or SDA	t_F			300	ns	
Setup time for STOP Condition	$t_{SU,STO}$	4.0			µs	
Bus Free Time between STOP and START Condition	t_{BUF}	4.7			µs	
Capacitance load for each bus line	C_b			400.0	pF	
Data valid time	$t_{VD;DAT}$			3.45[2)]	µs	
Data valid acknowledge time	$t_{VD;ACK}$			3.45[2)]	µs	
Noise margin at the LOW level	V_{nL}	$0.1*V_{CC}$			V	For each connected device (including hysteresis)

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Noise margin at the HIGH level	V_{nH}	0.2*V_{CC}			V	For each connected device (including hysteresis)

1) A device must internally provide a hold time of at least 300 ns for the SDA signal (with respect to the $V_{IH(MIN)}$ of the SCL signal) to bridge the undefined region of the falling edge of SCL.
2) The maximum $t_{HD;DAT}$ could be 3.45 us for Standard-mode, but must be less than the maximum of $t_{VD;DAT}$ or $t_{VD;ACK}$ by a transition time. This maximum must only be met if the device does not stretch the LOW period (t_{LOW}) of the SCL signal. If the clock stretches the SCL, the data must be valid before it releases the clock.

5.5 I2C Interface Characteristics (Fast Mode)

The table below defines the Fast Mode operation of the I2C interface. The I2C interface characteristics have been extracted from the I2C-bus specification.

Table 11 I2C Interface Characteristics (Fast Mode)

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Low-Level input voltage	V_{IL}	-0.3		0.3*V_{CC}	V	
High-Level input voltage	V_{IH}	0.7*V_{CC}		[1]	V	
Hysteresis of Schmitt trigger inputs	V_{HYS}	0.05*V_{CC}			V	
Low-Level output voltage 1	$V_{OL,1}$	0.0		0.4	V	Open Drain or Open Collector at 3mA sink current; $V_{cc} > V_{cc(min)}$
Low-Level output voltage 2	$V_{OL,2}$	0.0		0.2*V_{CC}	V	Open Drain or Open Collector at 2mA sink current[2]; $V_{CC}<=V_{CC(MIN)}$
Low-Level output current	I_{OL}	3.0			mA	V_{OL} = 0.4V
		6.0			mA	V_{OL} = 0.6V [3]
Output fall time from $V_{IH(MIN)}$ to $V_{IL(MAX)}$	t_{OF}	20*(V_{CC}/ 5.5V)[4]		250[5]	ns	
Pulse width of spikes that must be suppressed by the input filter	t_{SP}			50[6]	ns	
Input current for SDA/SCL pin	I_I	-10.0		10	µA	0.1*V_{CC} < V_I < 0.9*$V_{CC(MAX)}$. If V_{CC} is switched off, I/O pins must not obstruct the SDA and SCL lines.
Capacitance for SDA/SCL pin	C_I			10	pF	

1) Maximum V_{IH}=$V_{CC(MAX)}$ + 0.5V or 5.5V whichever is lower
2) The same resistor value to drive 3mA at 3.0V V_{CC} provides the same RC time constant when using < 2V VCC with a smaller current draw.

3) In order to drive full bus load at 400kHz, 6mA I_{OL} is required at 0.6V V_{OL}. Parts not meeting this specification can still function, but not at 400kHz and 400pF.
4) Necessary to be backwards compatible with Fast-Mode. For Fast-Mode Only.
5) The maximum t_f for the SDA and SCL bus lines quoted in the below table (300ns) is longer than the specified maximum t_{OF} for the output stages (250ns). This allows a series protection resistor to be connected between SDA/SCL pins and the SDA/SCL bus lines without exceeding the maximum specified t_F.
6) Special purpose devices such as multiplexers and switches may exceed this capacitance because they connect multiple paths together

5.6 I2C Interface Timing Characteristics (Fast Mode)

The table below defines the interface timing characteristics for Fast Mode operation of the I2C interface. These have been extracted from the I2C-bus specification.

Table 12 I2C Interface Timing Characteristics (Fast Mode)

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0.0		400.00	kHz	
Hold time (repeated) START condition	$t_{HD,STA}$	0.6			µs	After this period, the first clock pulse is generated
Low period for SCL	t_{LOW}	1.3			µs	
High period for SCL	t_{HIGH}	0.6			µs	
Setup time for a repeated START Condition	$t_{SU,STA}$	0.6			µs	
Data hold time	$t_{HD,DAT}$	0.0[1)]			µs	
Data setup time	$t_{SU,DAT}$	100.0[3)]			ns	
Rise time for SCL or SDA	t_R	20.0		330.00	ns	Applicable to Master
Fall time for SCL or SDA	t_F	20*(V_{CC}/ 5.5V)		300.00	ns	
Setup time for STOP Condition	$t_{SU,STO}$	0.6			µs	
Bus free time between STOP and START conditions	t_{BUF}	1.3			µs	
Capacitance load for each bus line	C_b			400.0	pF	
Data valid time	$t_{VD;DAT}$			0.9[2)]	µs	
Data valid acknowledge time	$t_{VD;ACK}$			0.9[2)]	µs	
Noise margin at the LOW level	V_{nL}	0.1*V_{CC}			V	For each connected device (including hysteresis)
Noise margin at the HIGH level	V_{nH}	0.2*V_{CC}			V	For each connected device (including hysteresis)

1) A device must internally provide a hold time of at least 300 ns for the SDA signal (with respect to the $V_{IH(MIN)}$ of the SCL signal) to bridge the undefined region of the falling edge of SCL.
2) The maximum $t_{HD;DAT}$ could be 0.9us for Fast-mode, but must be less than the maximum of $t_{VD;DAT}$ or $t_{VD;ACK}$ by a transition time. This maximum must only be met if the device does not stretch the LOW period (t_{LOW}) of the SCL signal. If the clock stretches the SCL, the data must be valid before it releases the clock.

3) A Fast-mode I2C-bus device can be used in a Standard-mode I2C-bus system, but the requirement $t_{SU;DAT}$ 250ns must then be met. This will automatically be the case if the device does not stretch the LOW period of the SCL signal. If such a device does stretch the LOW period of the SCL signal, it must output the next data bit to the SDA line $t_{r(MAX)} + t_{SU;DAT} = 1000$ acknowledge timing.

5.7 SWI I/O Characteristics

Table 13 SWI I/O Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
SWI input high voltage	$V_{SWI,IH}$	1.2			V	V_{SWI} should be lower than V_{CC}
SWI input low voltage	$V_{SWI,IL}$			0.8	V	
SWI output high voltage	$V_{SWI,OH}$	1.30			V	No indirect powering, measured at 1.0µA. For Master Only
SWI output low voltage	$V_{SWI,OL}$			0.1	V	Measured at 1mA
SWI bus load	$C_{SWI,L}$			250	pF	

5.8 SWI Timing Characteristics

Table 14 SWI Timing Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Basic Timing Parameters						
Time base	t_{SWI}	1.0		50	µs	
Bus frequency	f_{SWI}	10.0		500.0	kHz	50% Zero, 50% One
Peak data rate				500	kBit/s	
Bus rise time	t_r			200	ns	
Bus fall time	t_f			200	ns	
Transmit Timing Parameters						
Duration for 0_B	t_{TO}	0.75		1.25	t_{SWI}	
Duration for 1_B	t_{T1}	2.75		3.25	t_{SWI}	
Duration for STOP	t_{TS}	6.00			t_{SWI}	
Receive Timing Parameters						
Duration for 0_B	t_{RO}	0.6	1.0	1.4	t_{SWI}	
Duration for 1_B	t_{R1}	2.6	3.0	3.4	t_{SWI}	
Duration for STOP	t_{RS}	4.5			t_{SWI}	
Interrupt Timing Parameters						
Interrupt arming time	t_{ARM}	4.75			t_{SWI}	
Interrupt active time	t_{INT}	0.75	1	1.25	t_{SWI}	Drive period for all Slaves

Electrical Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Interrupt trailing time	t_{TRAIL}			3.25	t_{SWI}	Drive period for all Slaves
Bus Time-Out Parameters						
Bus Time-Out Period	t_{TOUT}			44.0	t_{SWI}	Please take note for Time Base, t_{SWI} equal to 1µs.
Bus Time-Out Period	t_{TOUT}			22.0	t_{SWI}	Please take note for Time Base, t_{SWI} equal to 2µs.
Bus Time-Out Period	t_{TOUT}			14.0	t_{SWI}	Please take note for Time Base, t_{SWI} equal to 3µs.
Bus Time-Out Period	t_{TOUT}			12.0	t_{SWI}	Please take note for Time Base, t_{SWI} equal to above 3µs.
Bus Time-Out Period	t_{TOUT}			10.0	t_{SWI}	Please take note for Time Base, t_{SWI} equal to above 5µs.
Power and Reset Control Timing Parameters						
Communication Low Time	t_{PDL}	225.0			µs	

Table 15 GPO

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
GPO output high Voltage	$V_{GPO,OH}$	V_{GPO}-0.7			V	Measured at 1mA
GPO output low Voltage	$V_{GPO,OL}$			0.1	V	Measured at 1mA
GPO internal pull-up resistance	$R_{PU(INT)}$	50	100	150	kΩ	
GPO internal pull-down resistance	$R_{pd(INT)}$	50	100	150	kΩ	
GPO frequency	f_{GPO}			1	MHz	10%/90% V_{CC}, C_{LOAD}=25pF
GPO rise time	$t_{GPO,r}$			15	ns	V_{CC}=3.8V, C_{LOAD} = 25pF, 10%/90% of V_{CC}
GPO fall time	$t_{GPO.f}$			15	ns	V_{CC}=3.8V, C_{LOAD} = 25pF, 10%/90% of V_{CC}
GPO load capacitance	C_{LOAD}			25	pF	

5.9 Random Number Generation Time

Table 16 Random Number Generation Time

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Random number generation time	T_{RNG}		55.0	60.0	µs	

5.10 Host Authentication Response Computation Time

Table 17 Host Authentication Response Computation Time

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Host Authentication Computation Time	$T^{1)}_{HA}$			3.30	ms	

1) Min. value here refers to the host needing to wait at least max (T_{HA}) before accessing the device for the response value. Max value here is optional (theoretically, the host can wait as long as it requires before reading back the response value) but this is provided for the host opting to time-out the readback process as a sign for abnormal activity.

5.11 ECC Authentication Response Computation Time

Table 18 ECC Authentication Response Computation Time

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Response Computation Time ECCE-163	$T^{1)}_{ECCE163}$			60.0	ms	

1) Min. value here refers to the host needing to wait at least max ($T_{ECCS163}$) before accessing the device for the response value. Max value here is optional (theoretically, the host can wait as long as it requires before reading back the response value) but this is provided for the host opting to time-out the readback process as a sign for abnormal activity.

5.12 NVM Characteristics

Table 19 NVM Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
NVM endurance	N_{CYC}			500,000	Cycles	25°C
NVM retention	T_{retent}			10	years	25°C
NVM programming time	t_{PROG}		4.59	5.1	ms	25°C
NVM programming time for MACCRx command	$t_{PROG, MACCRx}$			12.5	ms	

6 Appendix

[1] UM10204, I2C-Bus Specification and User Manual, NXP Semiconductors, Rev 6.00, 04 April 2014

Revision history

Document version	Date of release	Description of changes
1.0	2021-02-24	Initial Public Version (preliminary).
1.1	2021-12-12	Product name renamed from Authenticate IDoT to Authenticate S Updated Electrical Characteristics and minor typos

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2021-12-12

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email:
DSSCustomerService@infineon.com

Document reference

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.