OPTIGA™ Authenticate On Short Data Sheet

OPTIGA™ Authenticate Family

Description

This is a basic OPTIGA™ Authenticate On short data sheet that provides basic information for getting started to design of OPTIGA™ Authenticate On.

Features

Authentication

- 163-bit Elliptic Curve Cryptography (ECC) Engine
- 193-bit OPTIGA Digital Certificate (ODC)
- Message Authentication Code (MAC) Function for the User Data Authentication
- MAC based Host Authentication Feature for SLE956681 Only
- Customizable Kill Features
- Unique Chip ID 96-bit
- Ultra low-power operation at max 500uA

Non-Volatile Memory

- 2Kbit NVM size
- Lockable User NVM memory
- 32-bit page granularity
- 2 Lifespan Indicators

Communication Interface

- SWI I/O interface

Package

- Package PG-TSNP-6-16

ESD

- JESD22-A114 ESD HBM 2KV Standard
- JESD22-C101 ESD CDM 500V Standard

Software

- Host Side library

Table of contents

1 Overview

1.1 Product Description

Infineon Technologies' novel OPTIGA™ Authenticate On 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

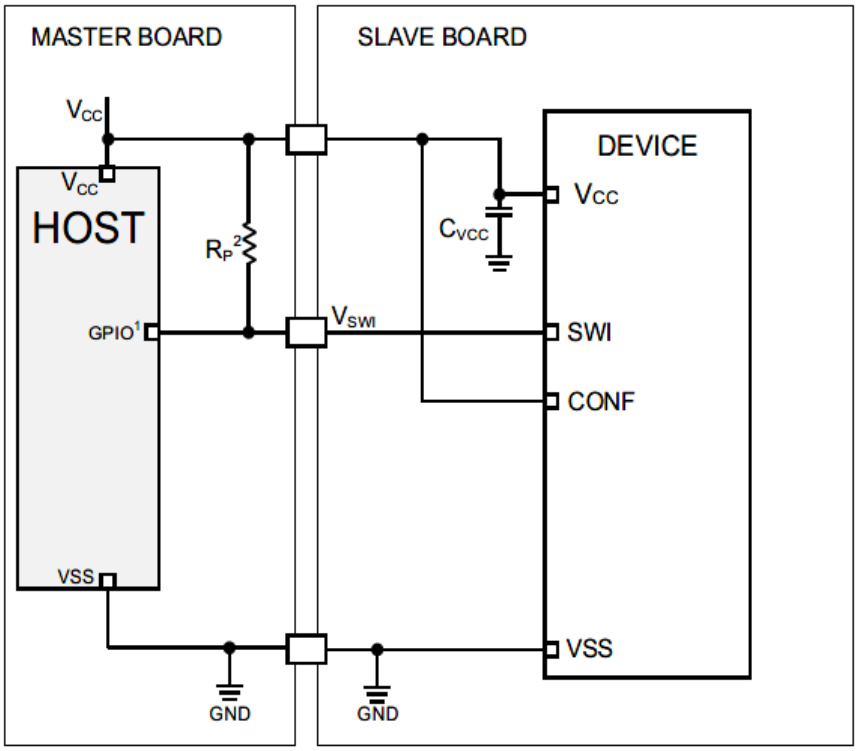
OPTIGA™ Authenticate On is designed to be used as a companion authentication device. This authentication device resides away from the host system such that the host system is able to check if it is communicating with an authenticated original device.

OPTIGA™ Authenticate On supports a configurable SWI interface to communicate with the Host controller. It is designed to be compatible to MIPI BIF dataword. The configuration of the interface link for the OPTIGA™ Authenticate On can be configured in the application board.

1.3 Typical Application

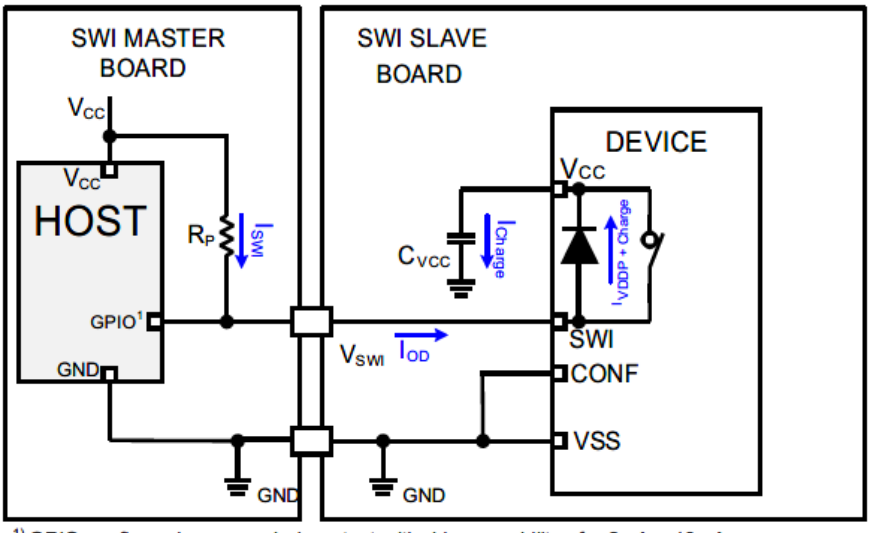
OPTIGA™ Authenticate On can be integrated to any system with very low hardware requirement. In a typical setup, only a pull-up resistor, R_P, is required for an open-drain GPIO. OPTIGA™ Authenticate On provides a combination of secure authentication function and user read/write storage space via a single serial interface (SWI). SWI is able to perform bidirectional communication on multiple devices on the bus without extra hardware. Communication on the SWI is half-duplex transmission in which master and slave can transmit and received commands only one at a time. In SWI architecture, SWI master initiates and controls all the SWI operations. The SWI bus operates in a command and response sequence. An additional feature of SWI interface is the ability of interrupt-based processing which allows for concurrent processing.

Below figures show an example of a Host system connection to an OPTIGA™ Authenticate On device in direct and indirect powered SWI configurations.



1) GPIO configured as open drain output with drive capability of > 2mA – 10mA
2) R_P can be connected to the same V_{CC} voltage or other system voltage lower than V_{CC}

Figure 1 Application Diagram of OPTIGA™ Authenticate On with SWI connectivity (Direct Power)



1) GPIO configured as open drain output with drive capability of > 2mA – 10mA
2) R_P is less than 680 ohm +/-1%

Figure 2 Application Diagram of OPTIGA™ Authenticate On with SWI connectivity (Indirect Power)

2 Signals Description

OPTIGA™ Authenticate On comes with PG-TSNP-6-16 package.

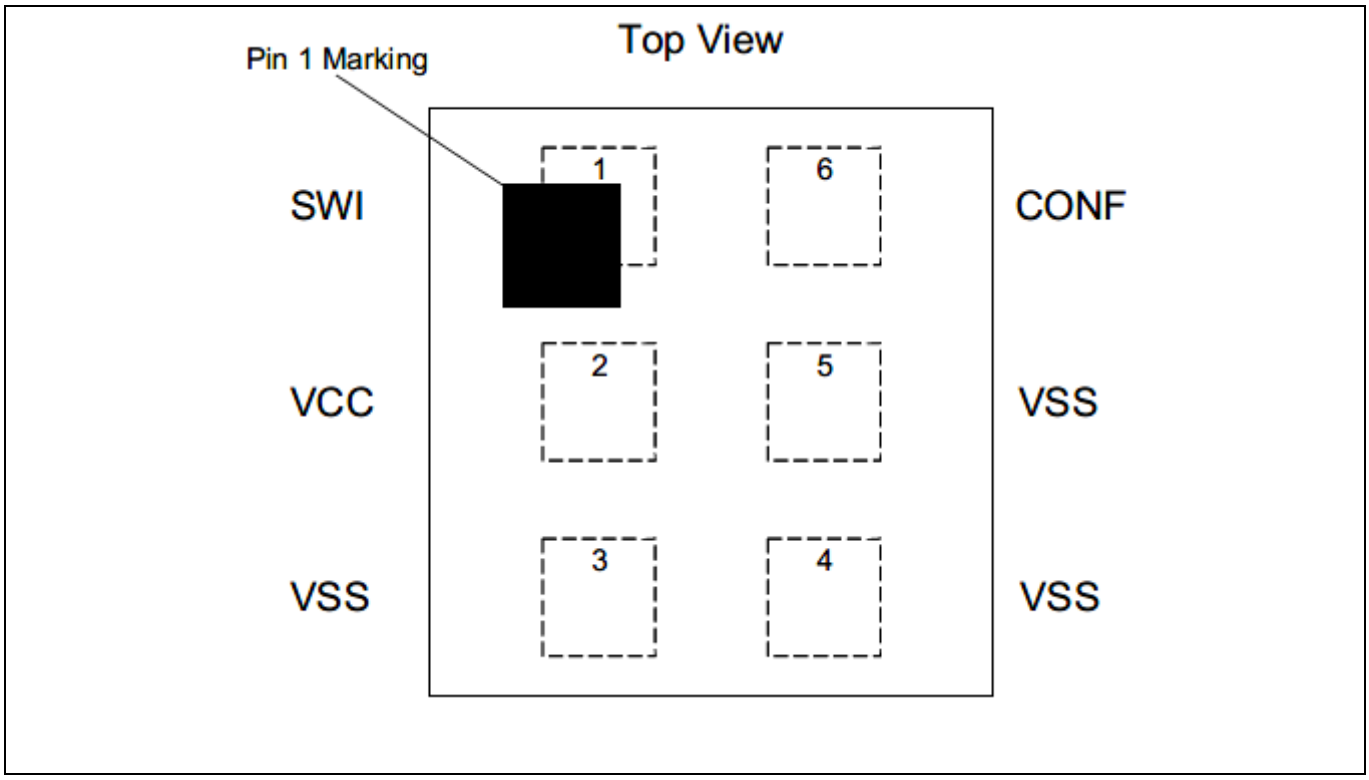


Figure 3 Pin configuration of OPTIGA™ Authenticate On

Table 1 I/O Signals

Pin No.	Name	Pin Type	Buffer Type	Function
1	SWI	I/O	OD	SWI
6	CONF	AI	Z	Must be connected to VSS for indirect power mode Must be connected to VCC for direct power mode

Table 2 Power Supply

Pin No.	Name	Pin Type	Buffer Type	Function
2	VCC	PWR	-	Positive Power Input for device

Table 3 Ground Pins

Pin No.	Name	Pin Type	Buffer Type	Function
3,4,5	VSS	PWR	-	GND Pin This is the common ground of the IC. Pin 4 is

Signals Description

Pin No.	Name	Pin Type	Buffer Type	Function
				the main ground of the package

Table 4 PG-TSNP-6-16 Package Dimensions

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min	Typ	Max		
A		1.45	1.50	1.55	mm	Package Width
B		1.15	1.20	1.25	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

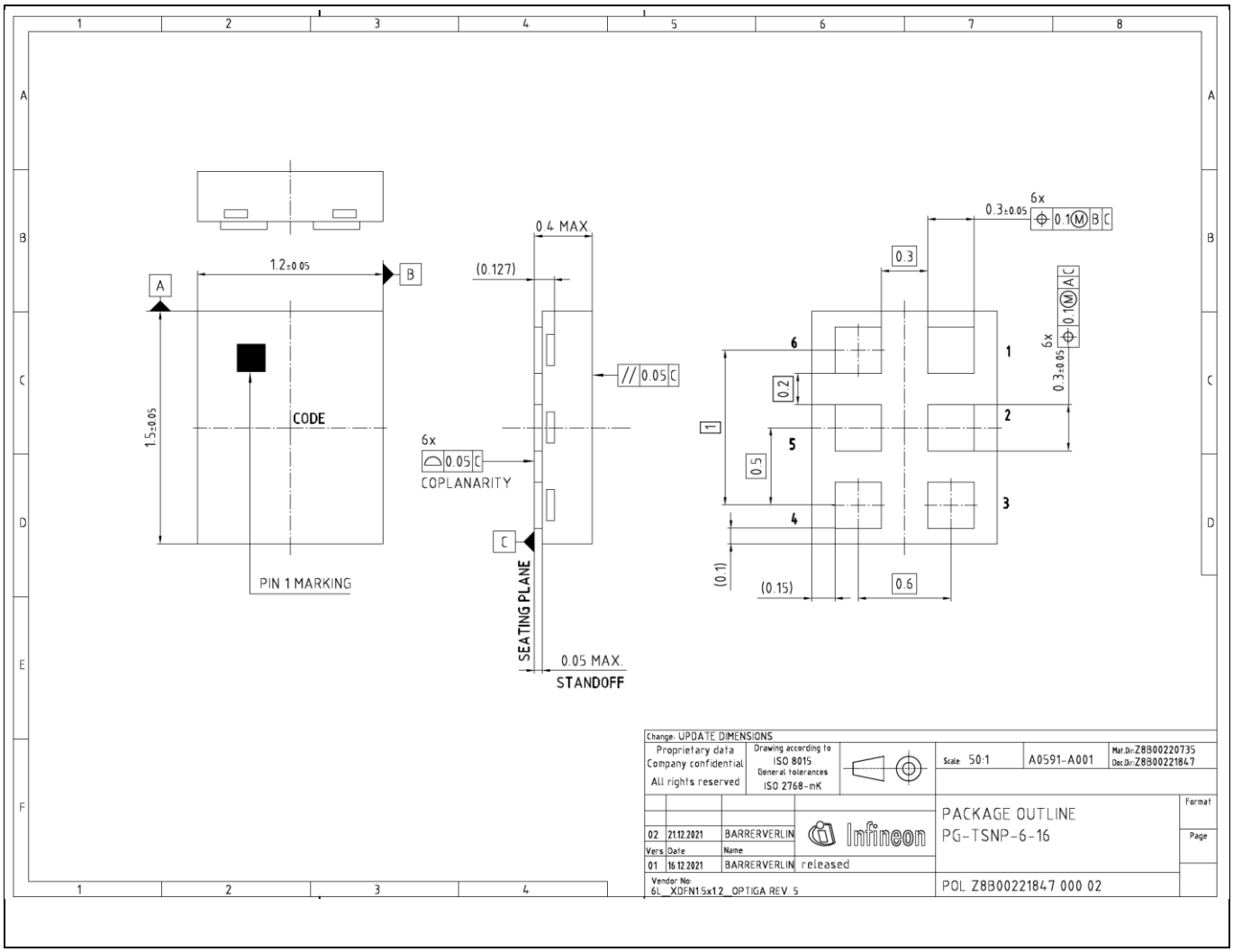


Figure 4 Package Dimension

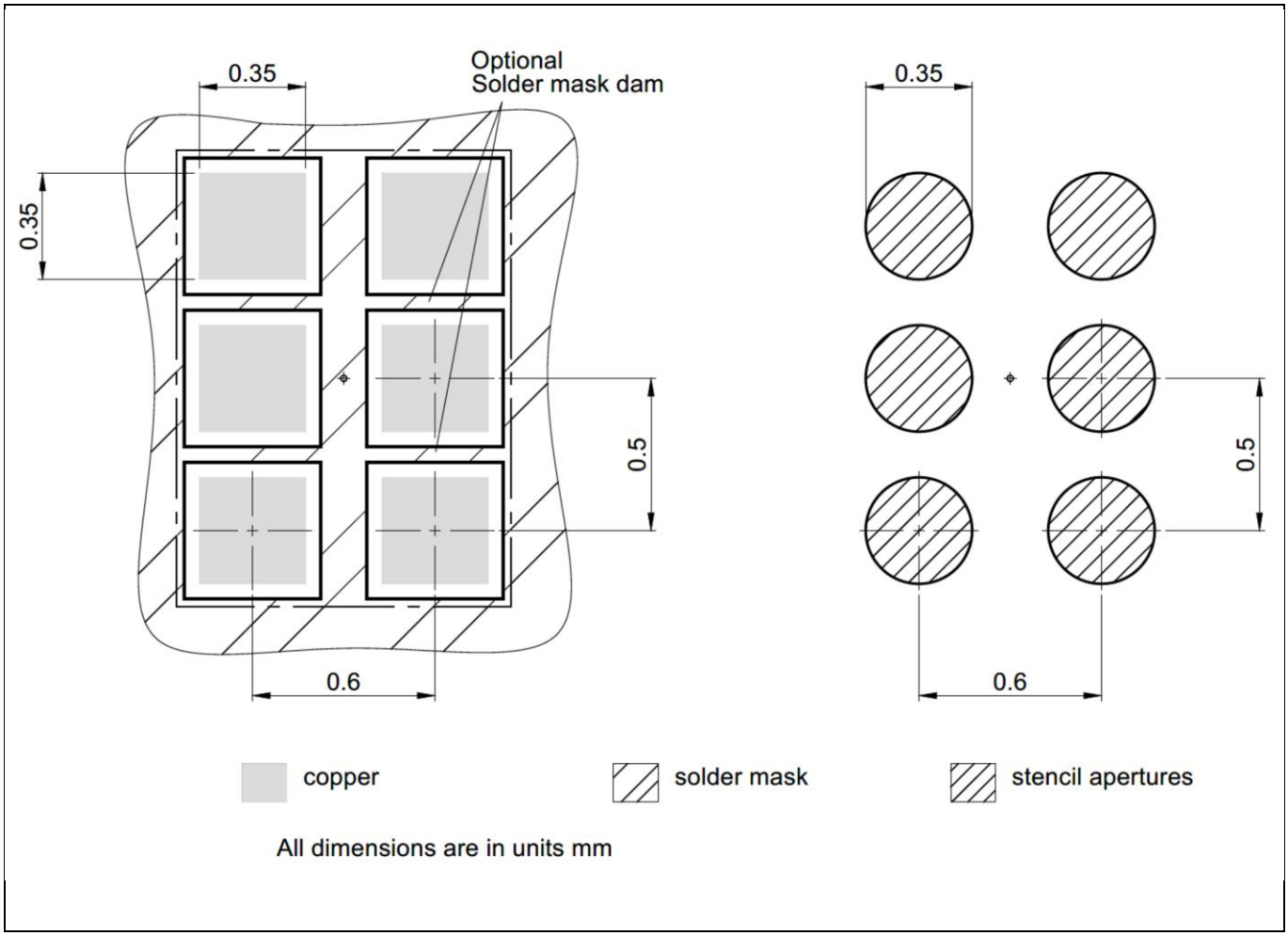


Figure 5 TSNP-6-16 Footprint

3 Packing Specification

3.1 Package Marking

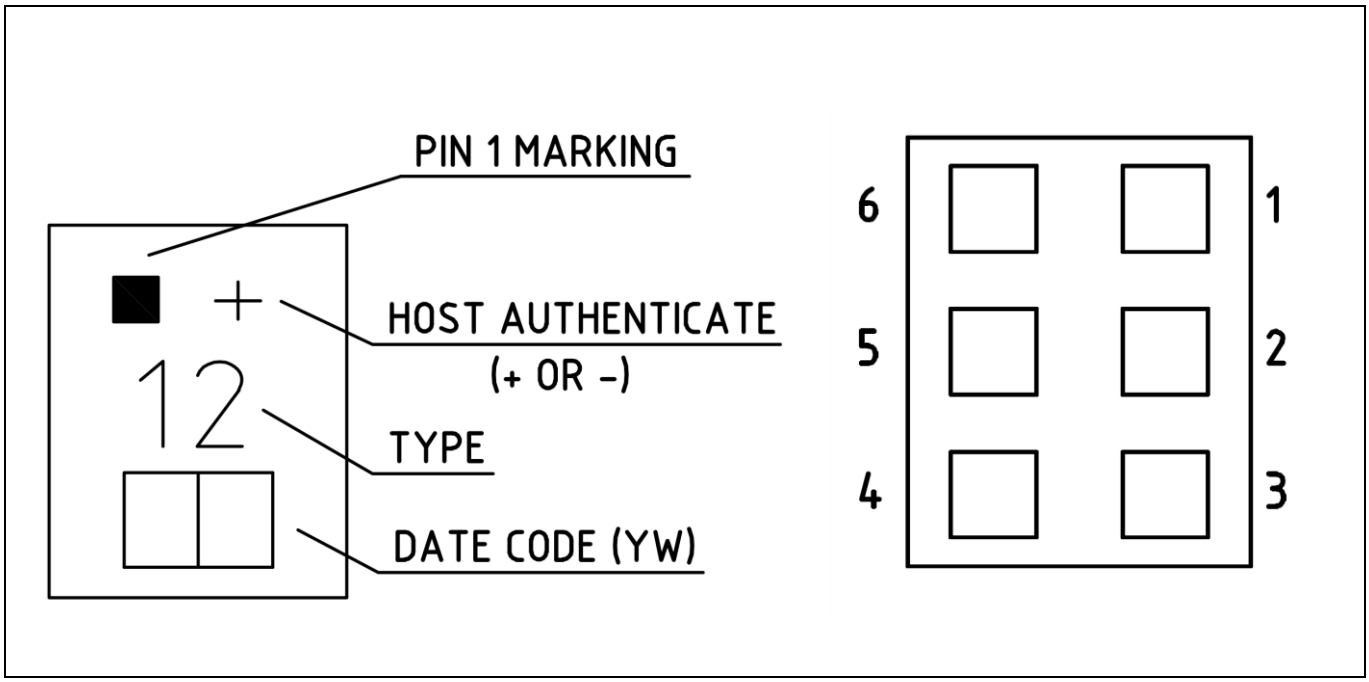


Figure 6 Packaging Laser Marking

3.2 Emboss Carrier Tape

Each box contains a single reel with 5000 pices of device. Reel diameter is 180 mm.

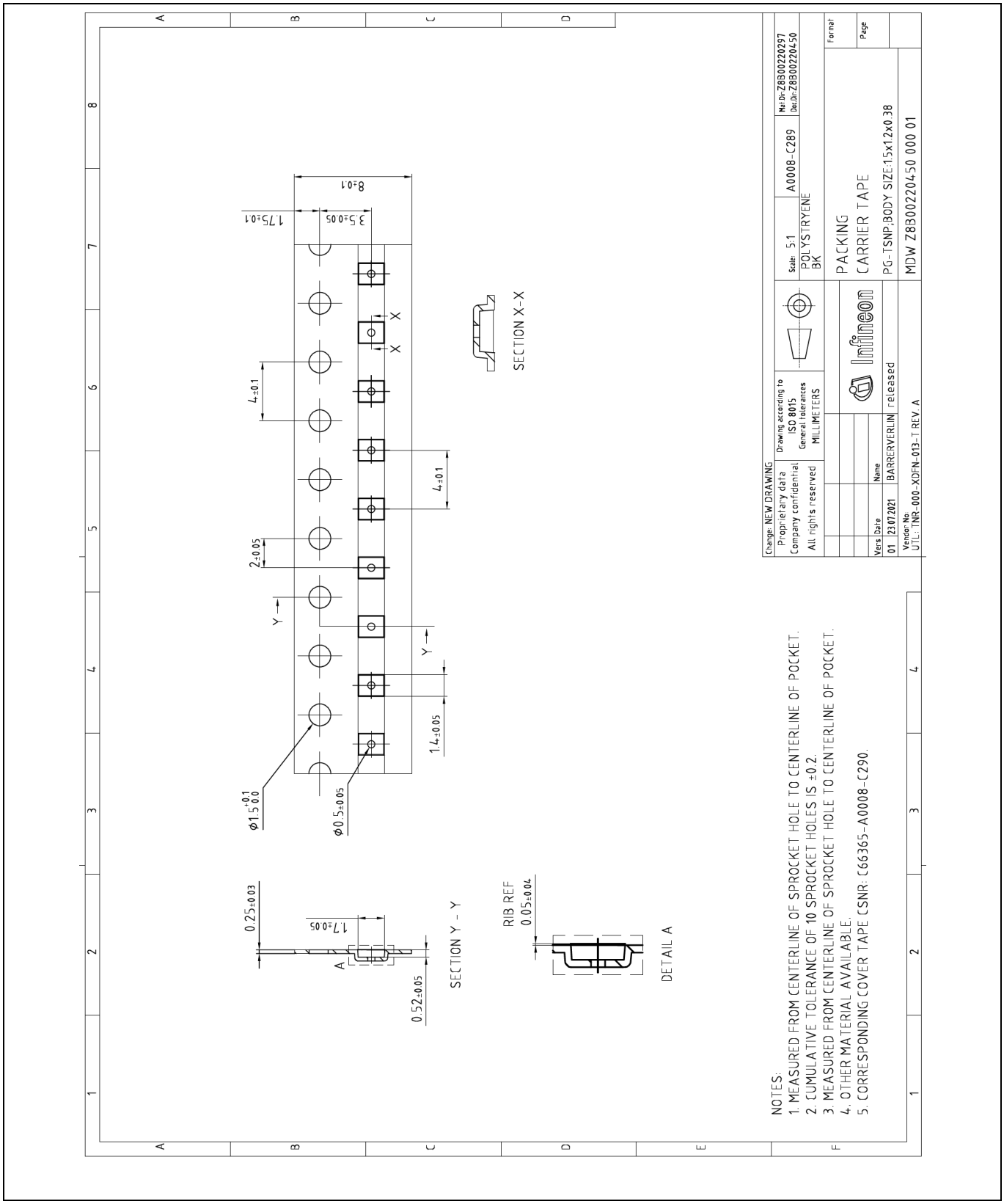


Figure 7 Carrier Tape

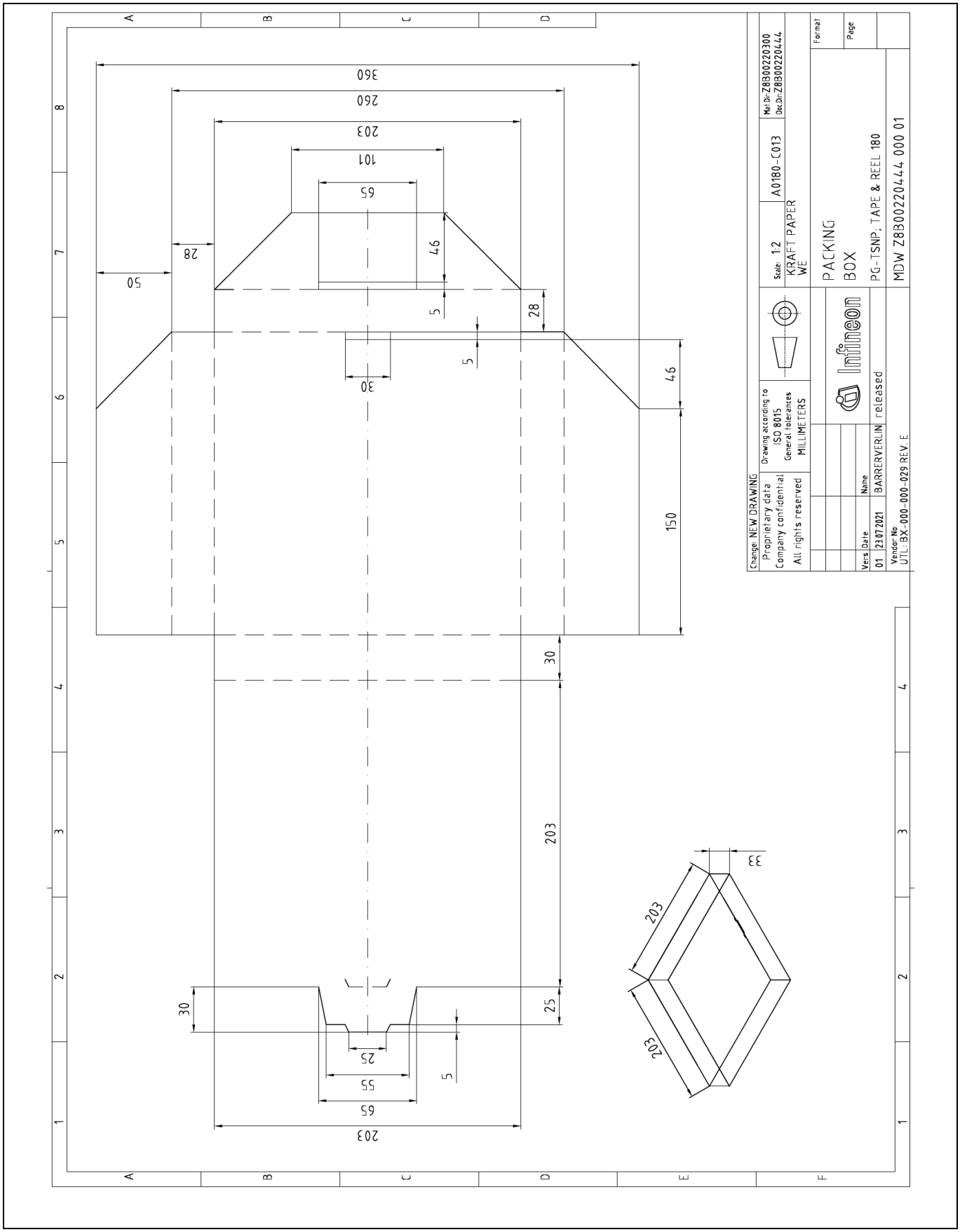


Figure 8 Box specification

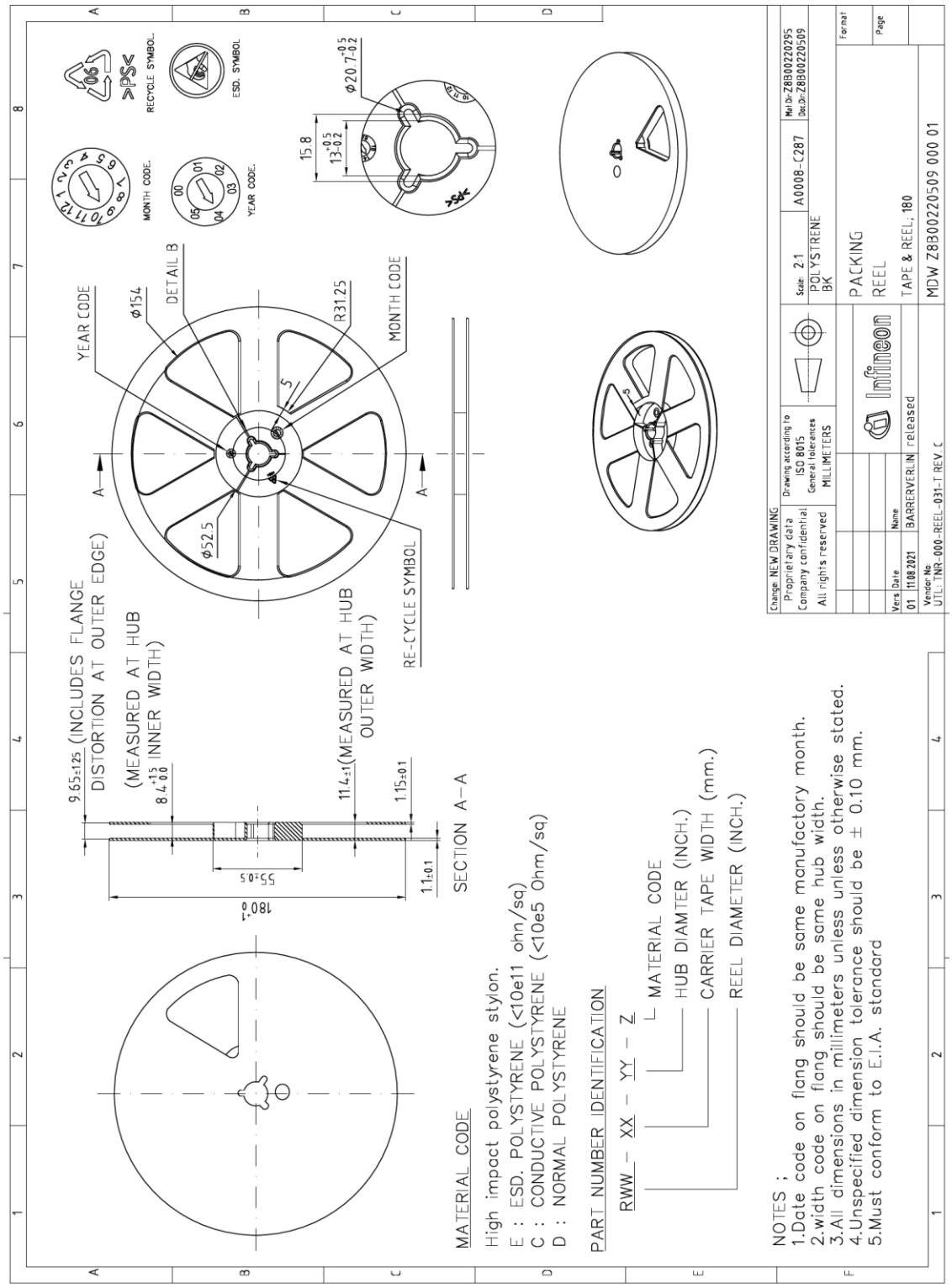


Figure 9 Carrier Tape Specification

4 Electrical Characteristics

4.1 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 (over 24 hours) may affect device reliability. Maximum ratings are absolute ratings; exceeding only one of these values may cause irreversible damage to the integrated circuit.

Table 5 Absolute Maximum Ratings

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
VCC Supply Voltage	V_{CC}	-0.3	–	4.6	V	
SWI Voltage	V_{SWI}	-0.3	-	4.6	V	
ESD robustness HBM	$V_{ESD,HBM}$	2000			V	According to EIA/JESD22-A114
ESD robustness CDM	$V_{ESD,CDM}$	500			V	According to EIA/JESD22-C101
Latch up	I_{LU}	100			mA	According to EIA/ JESD78
Storage Temperature	T_{STORE}	-55.0		150.0	°C	

4.2 Operating Conditions

Within the operational range, the IC operates as explained product description. Typical Values: V_{CC} = 1.8V, T_{AMB}=25 °C

Table 6 Operating Conditions

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
VCC Supply Voltage Range	V_{CC}	1.24		3.63	V	Measurement is at the V_{CC} pin. Ramp up of V_{CC} shall be slower than 1 µSec
SWI Voltage Range	V_{SWI}	-0.3		3.63	V	
Current Consumption, Active Idle Mode	$I_{VCC, Active-Idle}$		150	200	µA	Idle Function Mode Averaged over 1 Sec
Current Consumption, Active Mode, Authentication Operation	$I_{VCC, Active-ECC}$		325	500	µA	Averaged over Authentication
Current Consumption, Power-Down Mode	$I_{VCC,PD}$		1.0		µA	SWI is set at 0V Maximum Value condition is set at V_{CC} = 3.60V @ 85 Deg C
Ambient Temperature	T_{AMB}	-40		85	°C	
Power Down Low Time	t_{PDL}	2000.0			µs	
Power Up Delay	t_{PUD}			8.0	ms	
Soft Reset Delay	t_{SRD}			1.0	ms	

4.3 SWI I/O Characteristics

Table 7 SWI I/O Characterisitics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
SWI Input High Voltage	$V_{SWI,IH}$	1.2			V	
SWI Input Low Voltage	$V_{SWI,IL}$			0.8	V	
SWI Output High Voltage	$V_{SWI,OH}$	1.30			V	No remote powering, measured at 1.0 µA. For Master Only
SWI Output Low Voltage	$V_{SWI,OL}$			0.1	V	Measured at 1 mA
SWI Bus Load	$C_{SWI,L}$			250	pF	

4.4 SWI Timing Characteristics

Table 8 SWI Timing Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Basic Timing Parameters						
Time Base	t_{SWI}	1.0		153	µs	
Bus Frequency	f_{SWI}	3.268		500.0	kHz	50% Zero, 50% One
Peak Data Rate				500	kBits/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		1.4	t_{SWI}	
Duration for 1_B	t_{R1}	2.6		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
Interrupt Trailing Time	t_{TRAIL}			3.25	t_{SWI}	Drive period for all Slaves
Bus Time-Out Parameters						
Bus Time-Out Period	t_{TOUT}			90.0	t_{SWI}	Time Base, t_{SWI} equal or less than 9 µs.
Bus Time-Out Period	t_{TOUT}			10.0	t_{SWI}	Time Base, t_{SWI} above 9 µs.
Power and Reset Control Timing Parameters						
Communication Low Time	t_{PDL}	2000.0			µs	

4.5 Random Number Generation Time

Table 9 Random Number Generation Time

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Random Number Generation Time	T_{RNG}		50.0	60.0	µs	

4.6 Authentication Response Computation Time

Table 10 Authentication Response Computation Time

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Response Computation Time ECCS-163	$T^{1)}_{ECCS163}$		83	100	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 (theorically, 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.

4.7 NVM Characteristics

Table 11 NVM Characterisitics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
NVM Endurance	N_{CYC}			500,000	Cycle	25 °C
NVM Retention	T_{retent}			10	years	25 °C
NVM Programming Time	t_{PROG}		4.59	5.1	ms	25 °C

Revision history

Document version	Date of release	Description of changes
0.1	2021-01-27	Initial Version.
0.2	2021-10-01	Fixed minor typo.
0.3	2022-05-06	Added Char data and diagrams
0.4	2022-05-12	Editorial changes
0.5	2022-12-20	Added TSNP Solder mask
0.6	2023-10-18	Rename Product Brief to Short datasheet and remove restricted marking

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

Edition 2023-10-18

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@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.