OPTIGA™ Trust

Product Authentication Family

SLE95250

OPTIGA™ Trust B Authentication IC

Data Sheet

Revision 1.01, 2017-08-30

Chip Card & Security

Edition 2017-08-30

Published by
Infineon Technologies AG
81726 Munich, Germany

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, 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.

Information

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

Warnings

Due to technical requirements, components may contain dangerous substances. For information on the types in question, please contact the nearest Infineon Technologies Office.

Infineon Technologies components may be used in life-support devices or systems only with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Revision History	
Page or Item	**Subjects (major changes since previous revision)**
Revision 1.01**>,** 2017-08-30	
	Updated Typo errors
<Revision 1.0>, 2016-12-15	
	Updated Electrical Specification
<Revision 0.91>, 2016-06-15	
	Updated Life span counter operation
<Revision 0.9>, 2016-04-15	
	Initial Release

Trademarks of Infineon Technologies AG

AURIX™, C166™, CanPAK™, CIPOS™, CIPURSE™, EconoPACK™, CoolMOS™, CoolSET™, CORECONTROL™, CROSSAVE™, DAVE™, DI-POL™, EasyPIM™, EconoBRIDGE™, EconoDUAL™, EconoPIM™, EconoPACK™, EiceDRIVER™, eupec™, FCOS™, HITFET™, HybridPACK™, I²RF™, ISOFACE™, IsoPACK™, MIPAQ™, ModSTACK™, my-d™, NovalithIC™, OptiMOS™, ORIGA™, POWERCODE™; PRIMARION™, PrimePACK™, PrimeSTACK™, PRO-SIL™, PROFET™, RASIC™, ReverSave™, SatRIC™, SIEGET™, SINDRION™, SIPMOS™, SmartLEWIS™, SOLID FLASH™, TEMPFET™, thinQ!™, TRENCHSTOP™, TriCore™.

Other Trademarks

Advance Design System™ (ADS) of Agilent Technologies, AMBA™, ARM™, MULTI-ICE™, KEIL™, PRIMECELL™, REALVIEW™, THUMB™, µVision™ of ARM Limited, UK. AUTOSAR™ is licensed by AUTOSAR development partnership. Bluetooth™ of Bluetooth SIG Inc. CAT-iq™ of DECT Forum. COLOSSUS™, FirstGPS™ of Trimble Navigation Ltd. EMV™ of EMVCo, LLC (Visa Holdings Inc.). EPCOS™ of Epcos AG. FLEXGO™ of Microsoft Corporation. FlexRay™ is licensed by FlexRay Consortium. HYPERTERMINAL™ of Hilgraeve Incorporated. IEC™ of Commission Electrotechnique Internationale. IrDA™ of Infrared Data Association Corporation. ISO™ of INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. MATLAB™ of MathWorks, Inc. MAXIM™ of Maxim Integrated Products, Inc. MICROTEC™, NUCLEUS™ of Mentor Graphics Corporation. MIPI™ of MIPI Alliance, Inc. MIPS™ of MIPS Technologies, Inc., USA. muRata™ of MURATA MANUFACTURING CO., MICROWAVE OFFICE™ (MWO) of Applied Wave Research Inc., OmniVision™ of OmniVision Technologies, Inc. Openwave™ Openwave Systems Inc. RED HAT™ Red Hat, Inc. RFMD™ RF Micro Devices, Inc. SIRIUS™ of Sirius Satellite Radio Inc. SOLARIS™ of Sun Microsystems, Inc. SPANSION™ of Spansion LLC Ltd. Symbian™ of Symbian Software Limited. TAIYO YUDEN™ of Taiyo Yuden Co. TEAKLITE™ of CEVA, Inc. TEKTRONIX™ of Tektronix Inc. TOKO™ of TOKO KABUSHIKI KAISHA TA. UNIX™ of X/Open Company Limited. VERILOG™, PALLADIUM™ of Cadence Design Systems, Inc. VLYNQ™ of Texas Instruments Incorporated. VXWORKS™, WIND RIVER™ of WIND RIVER SYSTEMS, INC. ZETEX™ of Diodes Zetex Limited.

Last Trademarks Update 2011-11-11

Table of Contents

List of Figures

List of Tables

1 Preface

This document describes on the operation and interface characteristics of the OPTIGA™ Trust B design.

1.1 Abstract

This document is the device specification for OPTIGA™ Trust B design.

1.2 Document definitions

This document describes the architecture and behavior of the OPTIGA™ Trust B design.

1.3 Disclaimer

Infineon is as diligent as possible in compiling and updating the information on this databook. However, Infineon does not guarantee the correctness and completeness of the information provided. Equally, Infineon does not guarantee that this information is up to date. For questions concerning our products, their specifications and their utilization please contact Infineon for the latest specification. Features and spec values may be changed without notice.

1.4 Textual Convention

This document uses the following textual conventions:

- Functional units of subsystems are given in plain UPPER CASE. For example: “The SSC can be used to communicate with shift registers.”.
- Pins using negative logic are indicated by a N postfix. For example: “A reset input pin, RESETN, is provided for the hardware reset.”.
- Bit fields and bits in registers are generally referenced as “Register name.Bit field” or “Register name.Bit”. Most of the register names contain a module name prefix (for example, “SSCCON”, where “SSC” is the module name prefix, and “CON” is the actual register name). In chapters describing peripheral modules, the actual register name is referenced also as the kernel register name.
- Variables used to describe sets of processing units or registers appear in mixed-case type. For example, the register name “CC6xR” refers to multiple “CC6xR” registers with the variable x (x = 0, 1, 2). The bounds of the variables are always given where the register expression is first used (for example, “x = 2 - 0”), and is repeated as needed in the rest of the text.
- The default radix is decimal. Hexadecimal constants have a suffix with the subscript letter “H”, as in 100H. Binary constants have a suffix with the subscript letter “B”, as in: 111B.
- When the extent of register fields, groups of signals, or groups of pins are collectively named in the body of the document, they are given as “NAME[A:B]”, which defines a range for the named group from B to A. Individual bits, signals, or pins are given as “NAME[C]” where the range of the variable C is given in the text. For example: CFG[2:0] and TOS[0].
-

Units are abbreviated as follows:

- kByte = 1024 bytes of memory
- MHz = Megahertz
- Byte = 8-bit quantity
- MByte = 1,048,576 bytes of memory
- kBaud, kBit = 1000 characters/bits per second
- MBaud, MBit = 1,000,000 characters/bits per second
- µs = Microsecond

1.5 Abbreviations and Acronyms

°C	Degree Celsius
mA	milli ampere
mS	milli second
mV	milli volt
µA	micro ampere
µS	micro second
µV	micro volt
IC	Integrated Circuit
PMU	Power Management Unit
TSNP	Thin Small Non Leaded Package
CGU	Clock Generation Unit
OEM	Original Equipment Manufacturer
ODM	Original Design Manufacturer
ECC	Elliptic Curve Cryptography
ODC	OPTIGA™ Digital Certificate
MAC	Message Authentication Code
UID	Unique IDentifier
LSB	Least Significant Bit
MSB	Most Significant Bit
GPIO	General Purpose I/O
MCU	Microcontroller Unit

2 Overview

Infineon Technologies' novel OPTIGA™ Trust B 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 up in security.

2.1 Application Field

The main area of application is authentication leading to increased safety, functionality and reliability of the accessories, replacement parts and disposables with a special focus on batteries.

The OPTIGA™ Trust B Authentication IC lends itself for use in multiple application domains which use its safety and highly reliable authentication features. These protect the systems from unauthorized accessories, replacement parts and disposables. Such unauthorized accessories will be easily and immediately detected, allowing the systems decide the suitable next steps. Also the re-use of the chip as well as unauthorized re-use or re-provisioning of the original part can be avoided using the data authentication feature.

- **Low and high density batteries**
  - Mobile Phones
  - Computing Devices
  - Digital Imaging
  - Power Tools
- **Adaptor**
- **Miscellenous Accessories**
  - Earphones
  - Speakers
  - Docking Stations
  - Game Controller
- **Water Filter Replacement Parts**

2.2 Features

The features of OPTIGA™ Trust B Authentication IC are listed as follows:

- **High level of Security**
  - 131 bits Elliptic Curve Cryptography (ECC) Engine
  - 163 bits OPTIGA™ Trust B Digital Certificate (ODC)
  - Message Authentication Code (MAC) Function
  - Host Challenge by Software(Host → Slave)
  - Security Library Concept for easy host side integration
  - Kill-Feature
- **Customizable Non-Volatile Memories**
  - 64-bits protected NVM read-only space for customer specified information which cannot be modified by end user
  - 512-bits unprotected NVM memories for user mode area
  - Endurance of 100,000 programming cycle (at 25 Deg C ambient temperature)
- **Single Wire Interface**
  - Single-Wire Interfaces (SWI) I/O interface
  - up to 500kbit/s transmission speed
  - Device ID search scheme and address management for multiple device capabilities
  - 96 bits Unique Chip Identification number
  - Communication library concept for easy host side integration
  - Multiple device capabilities in direct powered mode
  - Powered directly or Indirect Power via Single-wire interface
  - Device ID search and management scheme
  - Power-up detection capability
  - Programmable Device Address capability
- **Power Management**
  - Direct powered / Indirect powered application solution
  - Power Up and Down Control Via SWI interface
  - Power Down Control Via Power Down Command
  - Wide Operating Range Single Supply Voltage Support (From 2.0V to 5.5V)
- **Lifespan Indicator**
  - The counter value can only be read by the host, it cannot be reprogrammed
  - Counter value is decrement on command
  - Up to 32 bit Life Span Counter Feature
- **Small Package**
  - PG-TSNP-6-9 Package
  - Package Width of 1.10mm is suitable for slim Printed Circuit Board (PCB) design
  - Package Height of 0.4mm(Max) is suitable for low height form factor profile design
  - Package Size: 1.5mm X 1.1mm
  - Pitch: 0.5mm
  - Comply with RoHS Standard
  - Comply with IPC/J-STD-020 MSL-1 Standard
- **ESD**
  - JESD22-A114 ESD HBM Standard 2kV Standard
  - JESD-C101 ESD CDM 500V Standard

3 Functional Overview

OPTIGA™ Trust B is designed to be used as a companion authentication device. This authentication device reside away from the HOSTsystem such that the host system is able to ensure that it is communicating with an authenticated original product.

The SWI communication link is the basis for the OPTIGA™ Trust B to communicates with the HOST controller. It is designed to conform to the Infineon SWI Bus Interface specification

3.1 Typical Application

OPTIGA™ Trust B can be integrated to any system with very low hardware requirement. In a typical setup, only a pull-up resistor, R_{SWI}, is required for open-drain GPIO.

OPTIGA™ Trust B provides a combination of secure authentication function and user read/write storage space via a single serial 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.

Figure 3-1 shows an example of a Host system connection to an OPTIGA™ Trust B device

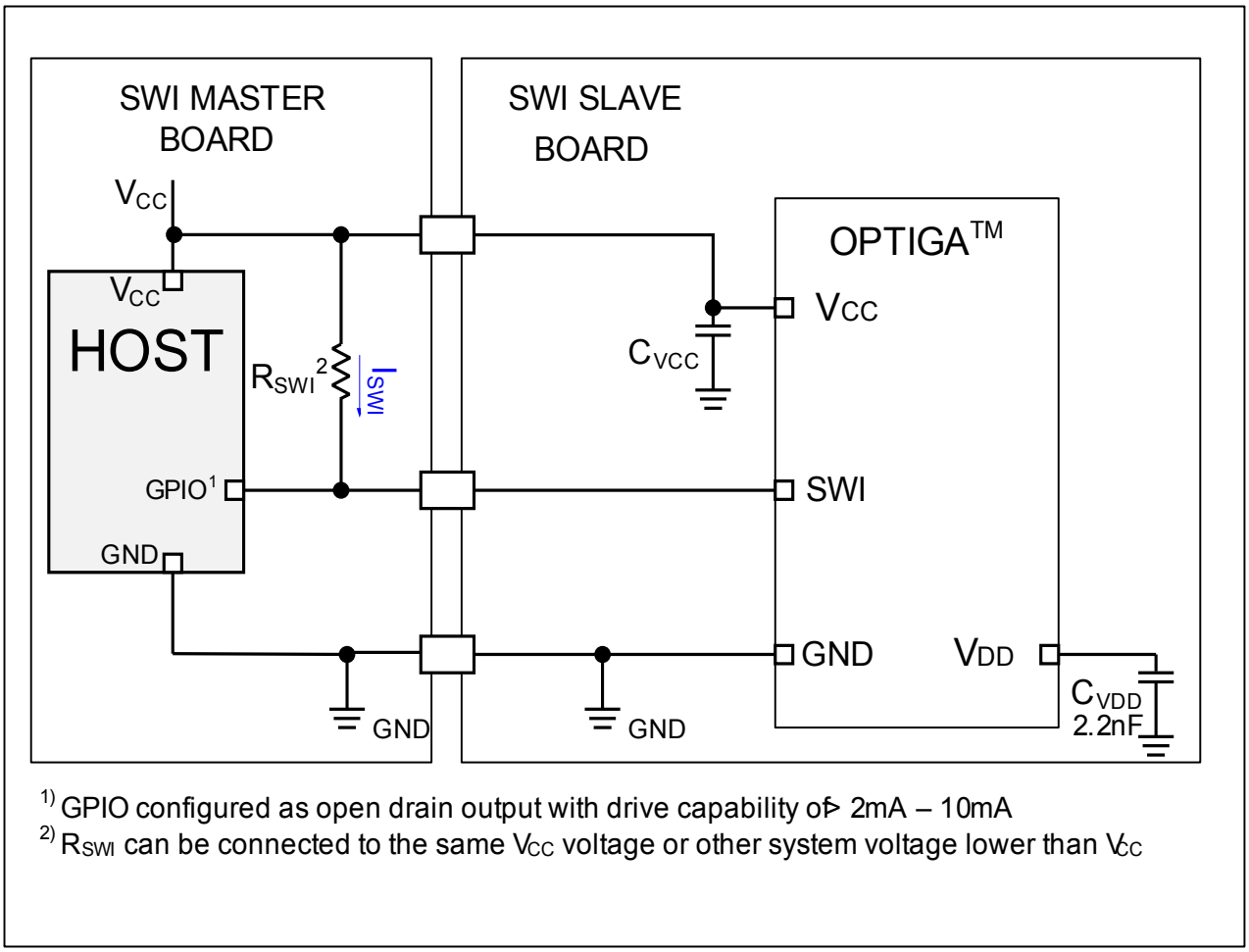

Figure 3-1 Application Diagram of OPTIGA™ Trust B based on Direct Power

In certain scenario where minimum number of wire connection are desired, OPTIGA™ Trust B can be configured with a total of two wires using some external circuit components. **Figure 3-2** shows a setup example of the system where OPTIGA™ Trust B is powered using the communication line. The resistor, R_{SWI}, maintains the power supply with a voltage drop of R_{SWI} multiplied by I_{SWI}. The voltage is fed to the OPTIGA's single wire interface port and its power supply through a diode. Using the following setup, the VCC connection is not required.

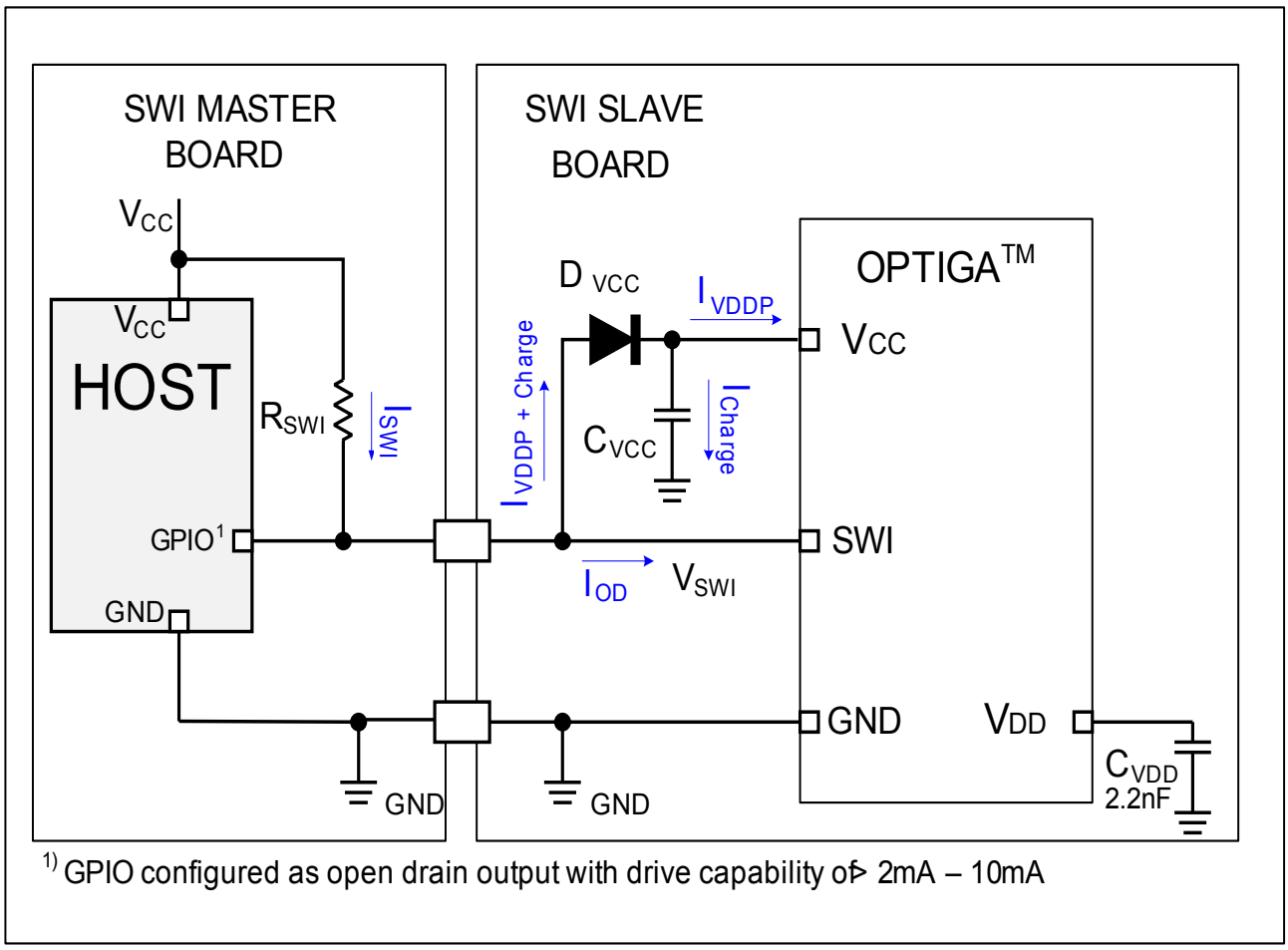

Figure 3-2 Application Diagram of OPTIGA™ Trust B based on Indirect Power

3.2 Support Mode of Operation

Various mode of operations supported in OPTIGA™ Trust B is tabulated in **Table 3-1**.

Table 3-1 Mode of Operation

Mode of Operation	Description
Power Down	• All systems are disabled, lowest current consumption mode
Active - Idle	• Communication Ready • System is not active • NVM is not active • Authentication is not active
Active - Communication	• Communication Ready • System is active • NVM is not active • Authentication is not active
Active - Authentication	• Communication Ready • System is active • NVM is active • Authentication is active
Active - NVM	• Communication Ready • System is active • NVM is active • Authentication is not active

4 Signals Description for PG-TSNP-6-9 Package

This chapter provides:

1. Pin Configuration (PG-TSNP-6-9 Package)
2. Abbreviations for signals description (Pin Type and Buffer Type)
3. Pin Description (PG-TSNP-6-9 Package)

4.1 Pin Configuration (PG-TSNP-6-9 Package)

The Pin configuration diagram for OPTIGA™ Trust B PG-TSNP-6-9 Package

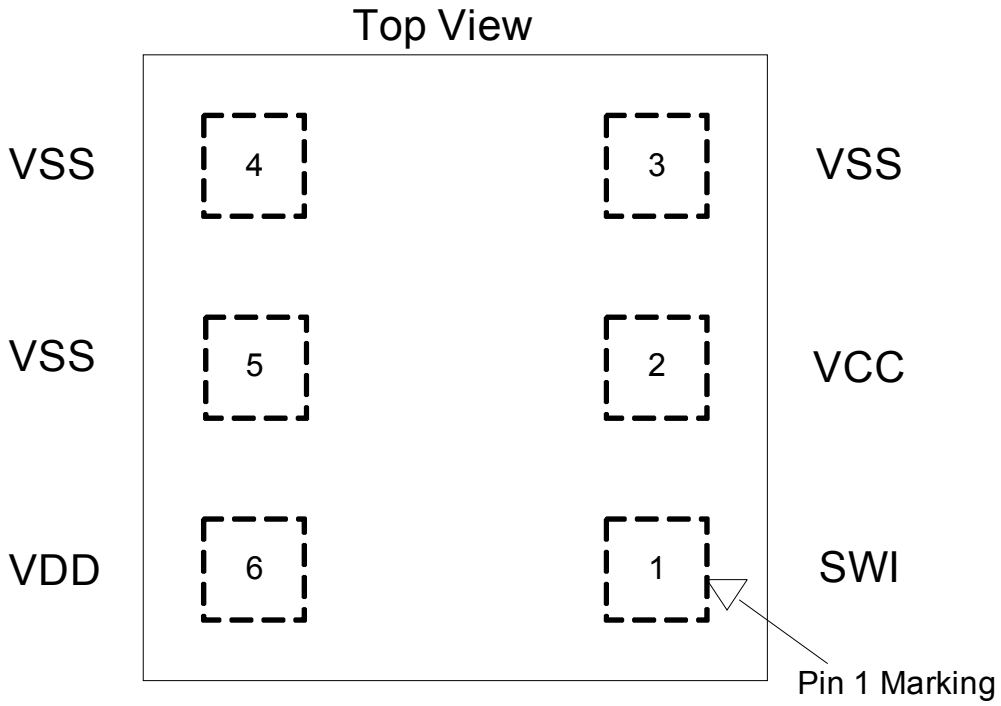

Figure 4-1 Pin Configuration (PG-TSNP-6-9 Package) - Top View

4.2 Abbreviations

The Standard abbreviations for I/O are shown in Table 4-1 and Table 4-2.

Table 4-1 Abbreviations for Pin Type

Abbreviations	Description
I	Standard input-only pin. Digital levels.
O	Output. Digital levels.
I/O	I/O is a bidirectional input/output signal.
AI	Input. Analog levels.
AO	Output. Analog levels.
AI/O	Input or Output. Analog levels.
PWR	Power
GND	Ground
MCL	Must be connected to Low (JEDEC Standard)
MCH	Must be connected to High (JEDEC Standard)
NU	Not Usable (JEDEC Standard)
NC	Not Connected (JEDEC Standard)

Table 4-2 Abbreviations for Buffer Type

Abbreviations	Description
Z	High impedance
PU1	Pull up, 10 kΩ
PD1	Pull down, 10 kΩ
PD2	Pull down, 20 kΩ
TS	Tristate capability: The corresponding pin has 3 operational states: Low, high and high-impedance.
OD	Open Drain. The corresponding pin has 2 operational states, active low and tristate, and allows multiple devices to share as a wire-OR. An external pull-up is required to sustain the inactive state until another agent drives it, and must be provided by the central resource.
OC	Open Collector
PP	Push-Pull. The corresponding pin has 2 operational states: Active-low and active-high (identical to output with no type attribute).
OD/PP	Open-Drain or Push-Pull. The corresponding pin can be configured either as an output with the OD attribute or as an output with the PP attribute.
ST	Schmitt-Trigger characteristics
TTL	TTL characteristics

Note: Any changes and extensions must be negotiated first.

4.3 Pin Description (PG-TSNP-6-9 Package)

Pin description for OPTIGA™ Trust B PG-TSNP-6-9 Package is shown below.

Table 4-3 I/O Signals

Pin No.	Name	Pin Type	Buffer Type	Function
1	SWI	I/O	OD	**Single Wire Interface**

Table 4-4 Power Supply

Pin No.	Name	Pin Type	Buffer Type	Function
2	V_{CC}	PWR	–	**Supply** Positive Power Input for OPTIGA™ Trust B. Connect 0.1µF capacitor.
6	V_{DD}	PWR	–	**Digital Power Supply** Internal Digital Power Supply of OPTIGA™ Trust B. Connect 2.2nF capacitor.

Table 4-5 Ground Pins

Pin No.	Name	Pin Type	Buffer Type	Function
4, 3, 5	V_{SS}	PWR	–	**GND Pin (Pin 4 is the main V_{SS})** This is the common ground of the IC.

4.4 Package

4.4.1 Package Outline: PG-TSNP-6-9

Table 4-6 shows the PG-TSNP-6-9 package dimension for OPTIGA™ Trust.

Table 4-6 PG-TSNP-6-9 Package Dimensions

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
A		1.05	1.1	1.15	mm	Package Width
B		1.45	1.5	1.55	mm	Package Length
C		0.35	0.375	0.40	mm	Package Height
D		0.25	0.30	0.35	mm	Solder Pad Width
E		0.25	0.30	0.35	mm	Solder Pad Length
F			0.50		mm	Solder Pad Pitch

Figure 4-2 shows the PG-TSNP-6-9 package outline for OPTIGA™ Trust.

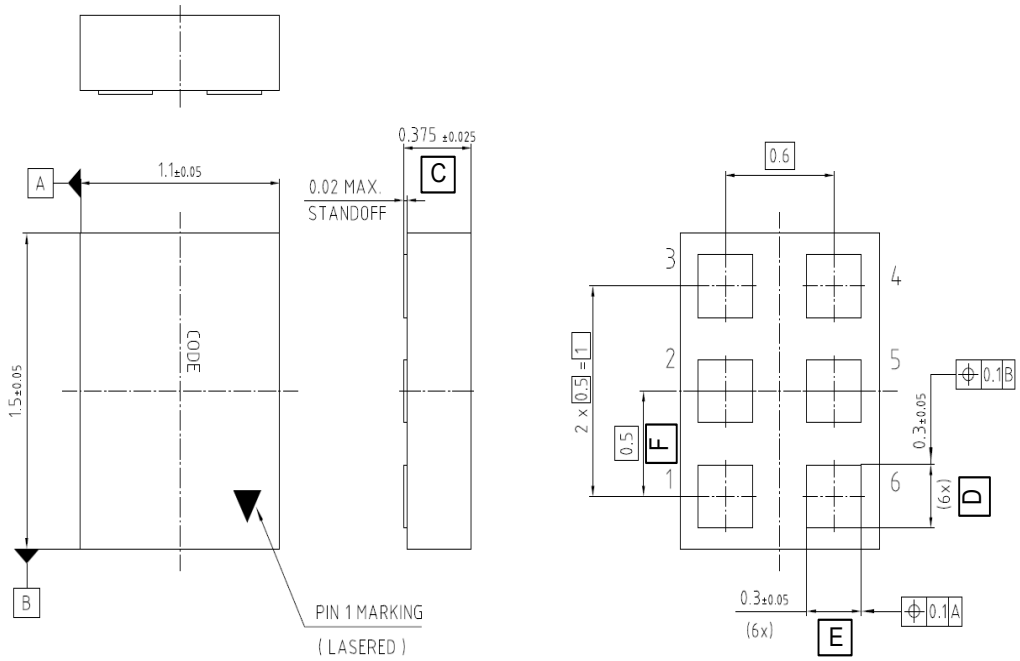

Figure 4-2 PG-TSNP-6-9 Package

5 Electrical Characteristics

5.1 Absolute Maximum Ratings

Stresses above the max. 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 5-1 Absolute Maximum Ratings

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
VCC Supply Voltage	V_{CC}	-0.3	–	6.0	V	
VDD Supply Voltage	V_{DD}	-0.3	–	1.60	V	
I/O	$V_{I/O}$	-0.3	–	6.0	V	
ESD robustness HBM	$V_{ESD,HBM}$			2000.0	V	According to EIA/JESD22-A114
ESD robustness CDM	$V_{ESD,CDM}$			500.0	V	According to EIA/JESD22-C101
Latch up	I_{LU}			100.0	mA	According to EIA/ JESD78
Junction temperature range	T_J	-40.0		85.0	°C	
Storage Temperature	T_{STORE}	-55.0		150.0	°C	

5.2 Operating Conditions

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

Table 5-2 Operating Conditions

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
VCC Supply Voltage Range	V_{CC}	2.0	3.8	5.5	V	Measurement is at the V_{CC} pin.V_{CC}
VDD Supply Voltage Range	V_{DD}	1.35	1.45	1.6	V	Measurement is at the V_{DD} pin. Need to connect 2.2nF Capacitor.Ramp up of VDD shall be slower than 1µSec.
SWI Voltage Range	V_{SWI}	-0.3		5.5	V	

Table 5-2 Operating Conditions (cont'd)

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Current Consumption, Active Idle Mode	$I_{VCC, Active-Idle}$		0.5		mA	Idle Function Mode Ave over Active Idle
Current Consumption, Active Mode, Authentication Operation	$I_{VCC, Active-ECC}$		1.0		mA	Authentication Mode Ave over Authentication
Current Consumption, Power-Down Mode	$I_{VCC,PD}$		1.0	3.0	µA	SWI is set at 0V Maximum Value condition is set at VCC = 4.35V @ 85 Deg C
Ambient Temperature	T_{AMB}	-40	25	85	°C	

5.3 SWI I/O Characteristics

Table 5-3 SWI I/O Characteristics

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
SWI Absolute Maximum Rating	$V_{SWI,ABR}$	-0.3		5.50	V	For Slave Only
SWI Input High Voltage	$V_{SWI,IH}$	1.2		5.5	V	
SWI Input Low Voltage	$V_{SWI,IL}$	-0.30		0.80	V	
SWI Output High Voltage	$V_{SWI,OH}$	1.30		5.5	V	No remote powering, measured at 1.0µA. For Master Only
SWI Output Low Voltage	$V_{SWI,OL}$			0.10	V	Measured at 1mA
SWI Bus Load	$C_{SWI,L}$			250	pF	
SWI Wake up Voltage	$V_{SWI,WK}$	0.8	1.0	1.2	V	
SWI Wake up Filter	$t_{SWI,WK}$	7	20	28	µs	

5.4 SWI Timing Characteristics

Table 5-4 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	kBits/s	
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}	4.75			t_{SWI}	
Receive Timing Parameters						
Duration for 0_B	t_{RO}	0.5		1.5	t_{SWI}	
Duration for 1_B	t_{R1}	2.5		3.5	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}			10.0	t_{SWI}	
Power and Reset Control Timing Parameters						
Power Down Low Time	t_{PDL}	196.0			µs	
Slave Power Up Delay	t_{PUP}	10.0			ms	
Slave Soft Reset Delay	t_{SRD}	1.0			ms	

5.5 EEPROM

Table 5-5 EEPROM

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
EEPROM Endurance	N_{CYC}			10^5	Cycle	25 Deg C
EEPROM Retention	T_{retent}			10	years	25 Deg C
EEPROM Programming Time	t_{PROG}			5.1	ms	

5.6 Authentication Response Computation Time

Table 5-6 Authentication Response Computation Time

Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
Response Computation Time ECCE-131	$T_{ECCE131}$			34.0	ms	

w w w . i n f i n e o n . c o m

Published by Infineon Technologies AG

Общество с ограниченной ответственностью «МосЧип» ИНН 7719860671 / КПП 771901001
Адрес: 105318, г.Москва, ул.Щербаковская д.3, офис 1107

Данный компонент на территории Российской Федерации

Вы можете приобрести в компании MosChip.

Для оперативного оформления запроса Вам необходимо перейти по данной ссылке:

http://moschip.ru/get-element

Вы можете разместить у нас заказ для любого Вашего проекта, будь то серийное производство или разработка единичного прибора.

В нашем ассортименте представлены ведущие мировые производители активных и пассивных электронных компонентов.

Нашей специализацией является поставка электронной компонентной базы двойного назначения, продукции таких производителей как XILINX, Intel (ex.ALTERA), Vicor, Microchip, Texas Instruments, Analog Devices, Mini-Circuits, Amphenol, Glenair.

Сотрудничество с глобальными дистрибьюторами электронных компонентов, предоставляет возможность заказывать и получать с международных складов практически любой перечень компонентов в оптимальные для Вас сроки.

На всех этапах разработки и производства наши партнеры могут получить квалифицированную поддержку опытных инженеров.

Система менеджмента качества компании отвечает требованиям в соответствии с ГОСТ Р ИСО 9001, ГОСТ РВ 0015-002 и ЭС РД 009

Офис по работе с юридическими лицами:

105318, г.Москва, ул.Щербаковская д.3, офис 1107, 1118, ДЦ «Щербаковский»

Телефон: +7 495 668-12-70 (многоканальный)

Факс: +7 495 668-12-70 (доб.304)

E-mail: info@moschip.ru

Skype отдела продаж:
moschip.ru
moschip.ru_4
moschip.ru_6
moschip.ru_9