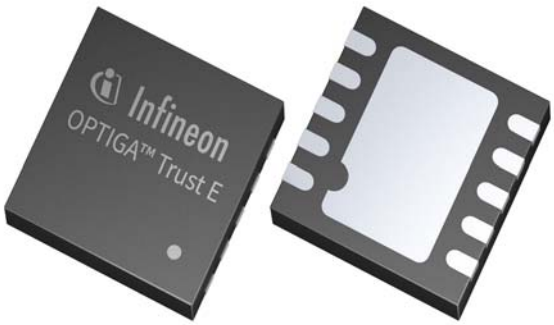
OPTIGA™ Trust E

Datasheet



Key features

- High-end security controller
- Turnkey solution
- I2C interface
- Up to 3 KB user memory
- Cryptographic support: ECC256, SHA-256
- PG-USON-10-2 package (3 x 3 mm)
- Standard & extended temperature ranges
- Full system integration support

Key values

- Protection of IP and data
- Protection of business cases
- Protection of corporate image
- Safeguarding of quality and safety

Applications

- Industrial control and automation
- Consumer electronics
- Smart home
- Medical devices
- Internet of things (IoT)
- PKI networks

About this document

Scope and purpose

This Datasheet provides information to enable integration of a security device, and includes package, connectivity and technical data.

Intended audience

This Datasheet is intended for device integrators and board manufacturers.

Table of contents

1 Introduction

As embedded systems are increasingly gaining the attention of attackers, Infineon Technologies offers the OPTIGA™ Trust E as a turnkey security solution for industrial automation systems, smart homes, consumer devices and medical devices. This advanced security controller comes with full system integration support for easy and cost-effective security deployment for your assets.

The OPTIGA™ Trust E security solution from Infineon is the winner of the internationally acclaimed "SESAMES Award" competition in the category "Best IT solution." It has also been honored with the "Golden SESAMES" – a special category on occasion of the 20 th anniversary of the awards.

Broad range of benefits

Integrated into your specific system architecture, the OPTIGA™ Trust E supports the protection of services, business models and user experience. Based on its one-way authentication mechanism, it uniquely identifies objects and protects PKI networks. Furthermore, the OPTIGA™ Trust E offers protection of quality and safety of your products.

Enhanced security

The OPTIGA™ Trust E comes with an advanced security controller employing Elliptic Curve Cryptography (ECC) with 256-bit keys and SHA-256. This new security technology greatly enhances your overall system security. Furthermore, the OPTIGA™ Trust E features key management, certificate generation and validation, as well as PKI support.

Fast and easy integration

The turnkey setup – with full system integration and all key/certificate material preprogrammed – reduces your efforts for design, integration and deployment to a minimum. As a turnkey solution, the OPTIGA™ Trust E comes with OS, embedded application and complete host-side integration support. The extended temperature range of −40°C to +85°C combined with a standardized I^2C interface and the small PG-USON-10-2 footprint provide an ideal platform for all your embedded projects.

As security in embedded systems is a critical success factor, customers can trust in Infineon Technologies' in-depth security expertise – reflected in over 25 years in a market-leading position – and more than 20 billion security controllers shipped worldwide.

Products

Type	Description	Temperature range	Package
OPTIGA™ Trust E- SLS 32AIA020A4	Enhanced security solution	−25°C to +85°C Standard Temperature Range (STR)	PG-USON-10-2
OPTIGA™ Trust E- SLS 32AIA020A2	Enhanced security solution	−40°C to +85°C Extended Temperature Range (ETR)	PG-USON-10-2
Evaluation kit	Relax kit		Board

OPTIGA™ Trust product family

The OPTIGA™ Trust E is part of Infineon Technologies' OPTIGA™ Trust family, which offers a full range of embedded security products to meet all device authentication needs. Other members of the OPTIGA™ Trust family are:

Introduction

- OPTIGA™ Trust SLS 10ERE, a product for device authentication and brand protection
- OPTIGA™ Trust P SLJ 52ACA, a Java Card-based programmable solution with extensive use case support

Infineon Technologies' OPTIGA™ family is geared towards the protection of embedded systems. All products are based on secured hardware and software. In addition to OPTIGA™ Trust products, the family includes the OPTIGA™ TPM (Trusted Platform Module) lineup for embedded applications that require TCG (Trusted Computing Group) compliance.

2 Connectivity

This chapter provides sample schematics that show how to connect the OPTIGA™ Trust E.

2.1 Power supply schematics

Figure 1 illustrates how the controller is to be supplied.

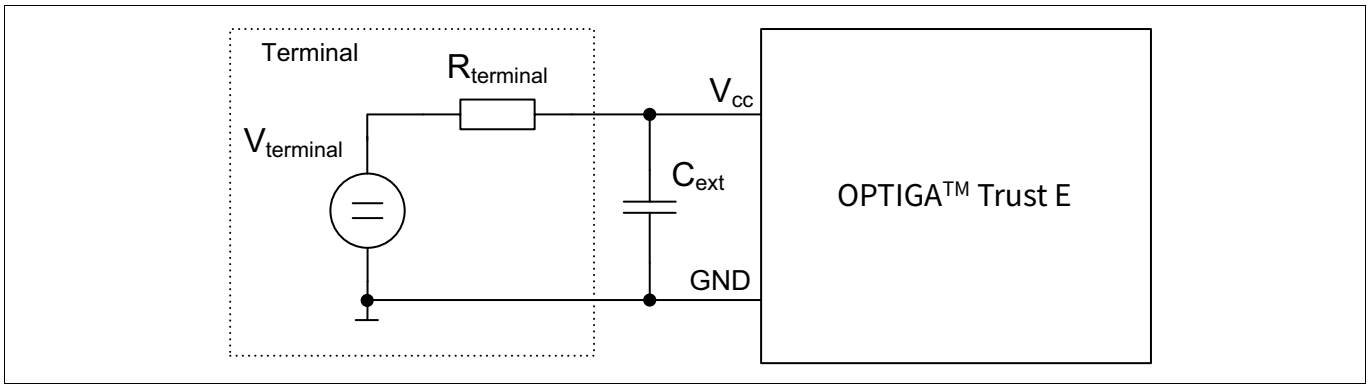


Figure 1 Power supply diagram

Table 1 Minimum required C_{ext} as a function of $R_{terminal}$ and V_{CC}

		V_{CC} [V]			
		1.74 ... 2	**2 ... 2.7**	**2.7 ... 3.3**	**3.3 ... 5.5**
$R_{terminal}$ [Ω]	< 50	n.a.	n.a.	10 nF	10 nF
	< 35	n.a.	n.a.	10 nF	5 nF
	< 20	n.a.	10 nF	10 nF	5 nF
	< 10	47 nF	10 nF	10 nF	5 nF
	< 5	10 nF	5 nF	5 nF	5 nF

2.2 I2C interface

Figure 2 illustrates how the I2C bus is to be connected.

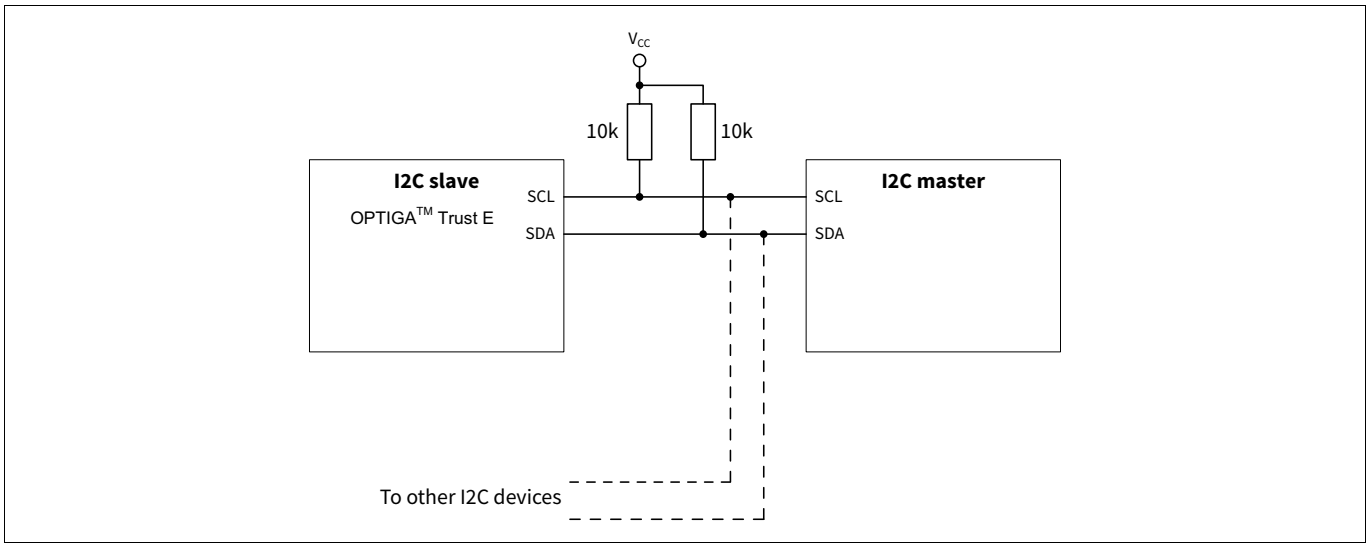


Figure 2 I2C schematic diagram

3 Description of packages

This chapter provides information about available package/module types and how each product's interfaces are assigned to the package pins. For further information on compliance of the packages with European Parliament Directives, see **"RoHS compliance" on Page 16**.

For details and recommendations regarding the assembly of packages on PCBs, please see the following: **http://www.infineon.com/cms/en/product/technology/packages/**

Table 2 Products and their packages

Product	Package types
SLS 32AIA020A2	PG-USON-10-2
SLS 32AIA020A4	PG-USON-10-2

3.1 PG-USON-10-2

The package dimensions of the controller in PG-USON-10-2 packages are given below.

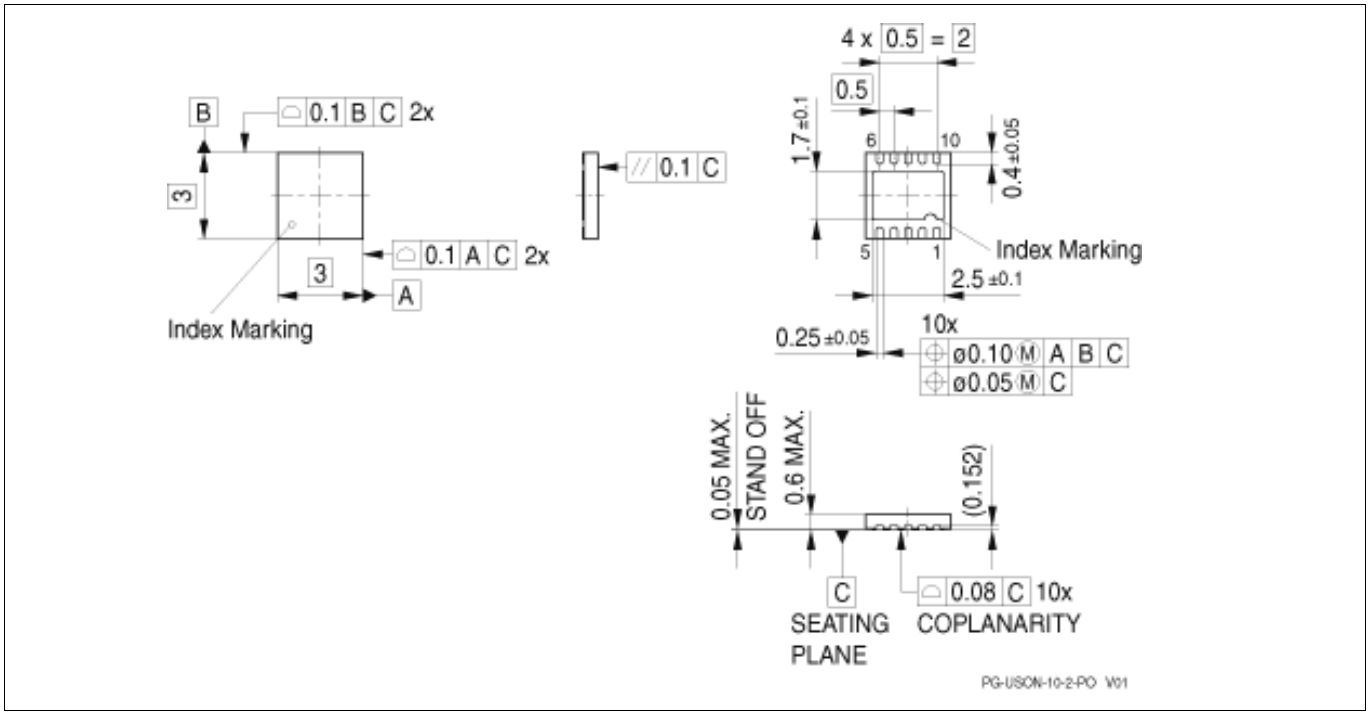


Figure 3 PG-USON-10-2 package

Production sample marking pattern

The following figure describes the productive sample marking pattern on PG-USON-10-2.

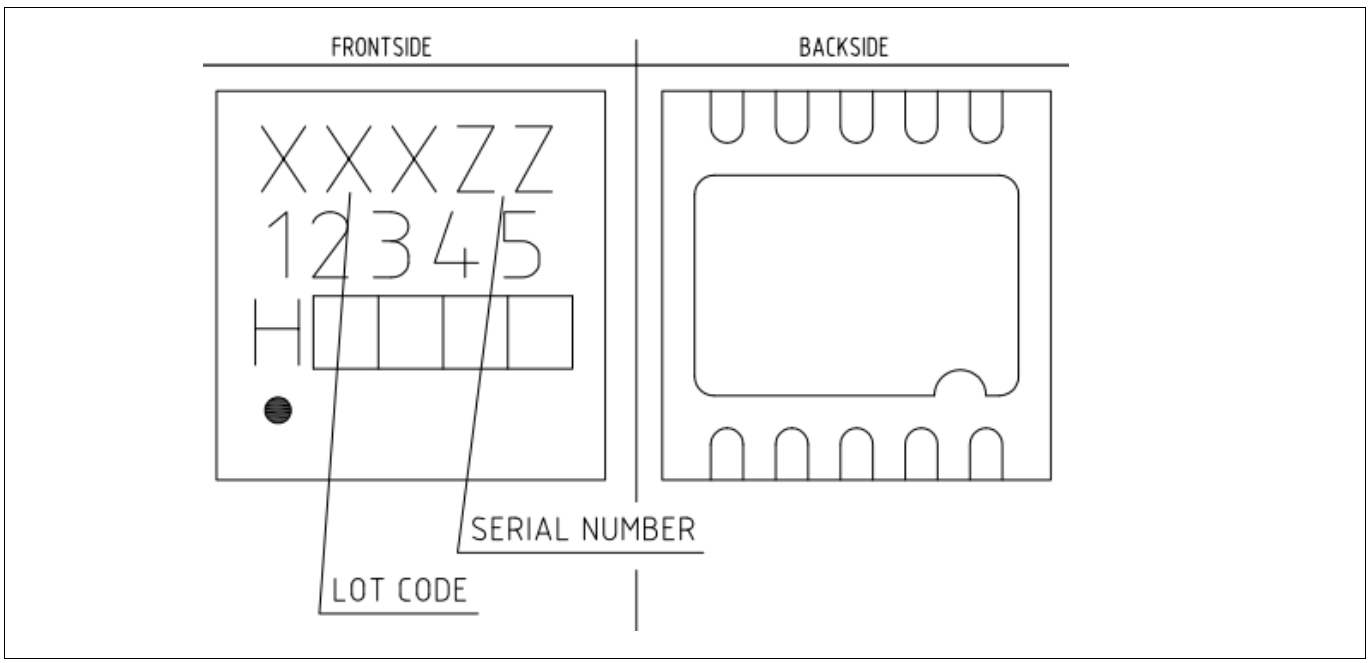


Figure 4 PG-USON-10-2 sample marking pattern

The black dot indicates Pin 01 for the chip. The "LOT CODE" is defined and inserted during fabrication. The "SERIAL NUMBER" is used for internal purposes. The field with "H" is "halogen-free", followed by four digits,

where the first two digits indicate the year and the last two digits indicate the work week. The field marked "12345" is the type code with the last digit indicating the software release version. This is shown in the table below for OPTIGA™ Trust E products for STR and WTR variants.

Table 3 Marking

STR	TRES0
WTR	TREW0

The contacts and their functionality are given in the table below.

Table 4 Contact definitions and functions of PG-USON-10-2 packages

Pin	Type	Function
01	GND	Supply voltage (Ground)
02	I/O	Serial Data Line (SDA)
03	N.C.	Not Connected
04	N.C.	Not Connected
05	N.C.	Not Connected
06	N.C.	Not Connected
07	N.C.	Not Connected
08	I/O	Serial Clock Line (SCL)
09	IN	Reset (RST)
10	V_{CC}	Supply voltage (voltage drain drop)

4 Technical data

This section summarizes the technical data of the products. It provides the operational characteristics as well as the electrical DC and AC characteristics.

4.1 Operational characteristics

All voltages are referenced to the power supply ground in the corresponding package.

Absolute maximum ratings

Table 5 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC}	−0.3	–	7.0	V	–
Input voltage	V_{IN}	−0.3	–	V_{CC} + 0.3	V	–
Operating temperature (ambient)	T_A (STR)	−25	–	85	°C	
	T_A (WTR)	−40	–	85	°C	
Junction temperature	T_J	−40	–	110	°C	–
Pulse voltage for I/O and IN lines (ESD protection)	$V_{ESD, HBM}$ [1)]	4000	–	–	V	
	$V_{ESD, CDM}$ [2)]	500	–	–	V	

1) According to EIA/JESD22-A114-B, Section 4, including ISO/IEC 7816-1 and ISO/IES 10373

2) According to JESD22-C101C – Field-Induced Charged-Device Model Test Method for Electrostatic-Discharge-WithstandThresholds of Microelectronic Components; 2004

Note: Stresses exceeding the values listed under "Absolute maximum ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or at any other conditions whose values exceed those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability, including EEPROM data retention and write/erase endurance.

4.2 Electrical characteristics

Notes

1. *T_A as given for the controller's operating temperature range unless otherwise stated.*
2. *All currents flowing into the controller are considered positive.*

4.2.1 DC electrical characteristics

Current and voltage values assume a terminal that is able to supply the product according to the referenced standards providing a capacitor of C_{ext} as close as possible to the contacting elements.

T_A = −25 °C to 85°C (STR standard temperature range).

T_A = −40 °C to 85°C (WTR wide temperature range).

Table 6 Electrical characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC}	1.62	–	5.5	V	Overall functional voltage range
Supply current[1)], operating (average)	I_{CCAVG}	–	20	–	mA	
Supply current, in *sleep mode*	I_{CCS3}	–	35	100	µA	T_A = 25°C, see Note
RST Input high level	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.3	V	I_{IH} = −20 µA ... +20 µA
RST Input low level	V_{IL}	−0.3	–	0.2 * V_{CC}	V	I_{IL} = −50 µA ... +20 µA

1) Supply current can be limited from 9 mA to 15 mA by software commands.

Note: The typical sleep mode current is the value without any peripheral running in sleep mode.

4.2.2 AC characteristics

Table 7 AC characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
External supply VCC						
Supply ramp-up time	t_{VCCR}	1	–	200	µs	See below

The V_{CC} ramp is depicted in **Figure 5**. 90% of the target supply voltage must be reached within 200 µs after it has exceeded 400 mV. Moreover, its variation must be kept within a ±10% range.

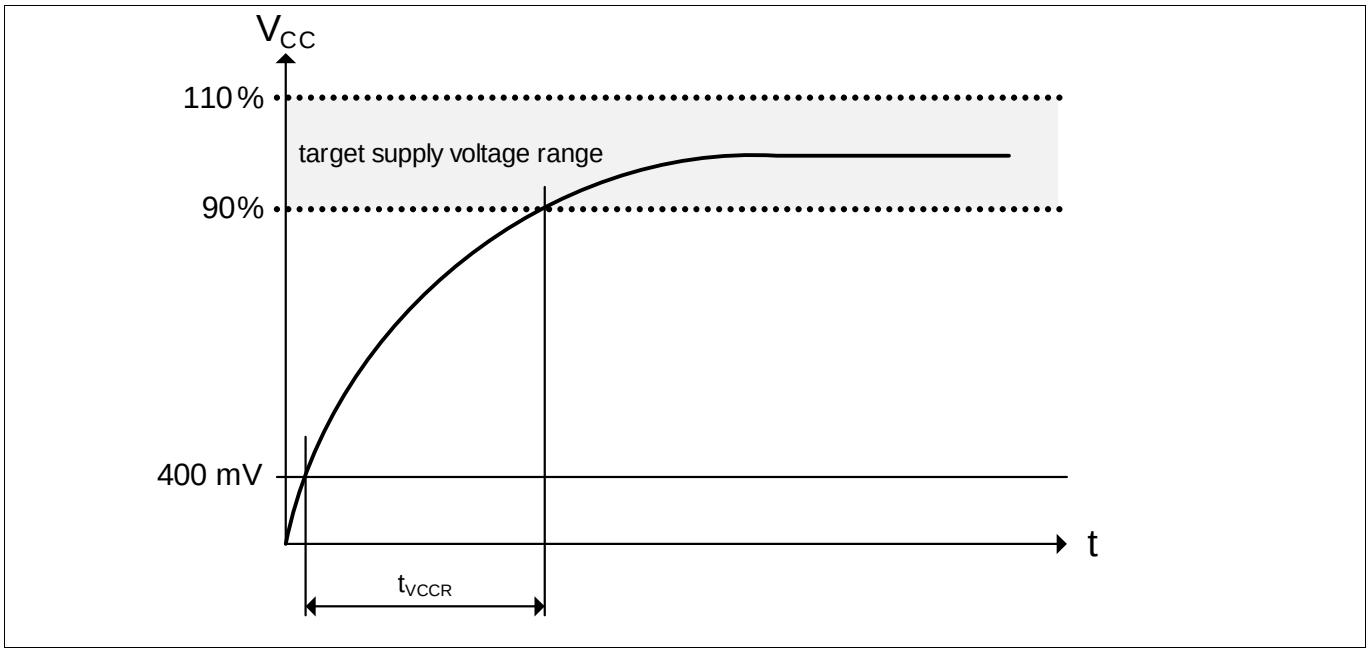


Figure 5 Vcc ramp-up

4.2.3 Startup of I2C interface

There are 2 variants possible for performing the startup procedure:

- Startup after power-on
- Startup in case of warm reset

4.2.3.1 Startup after power-on

The activation of the I2C interface after power-on needs the following reset procedure.

- VCC is powered up and the state of the SDA and SCL line are set to high level during power-up.
- The first transmission may start at the earliest $t_{STARTUP}$ after power-up of the device.

The following figure shows the startup timing of the I2C interface for this case.

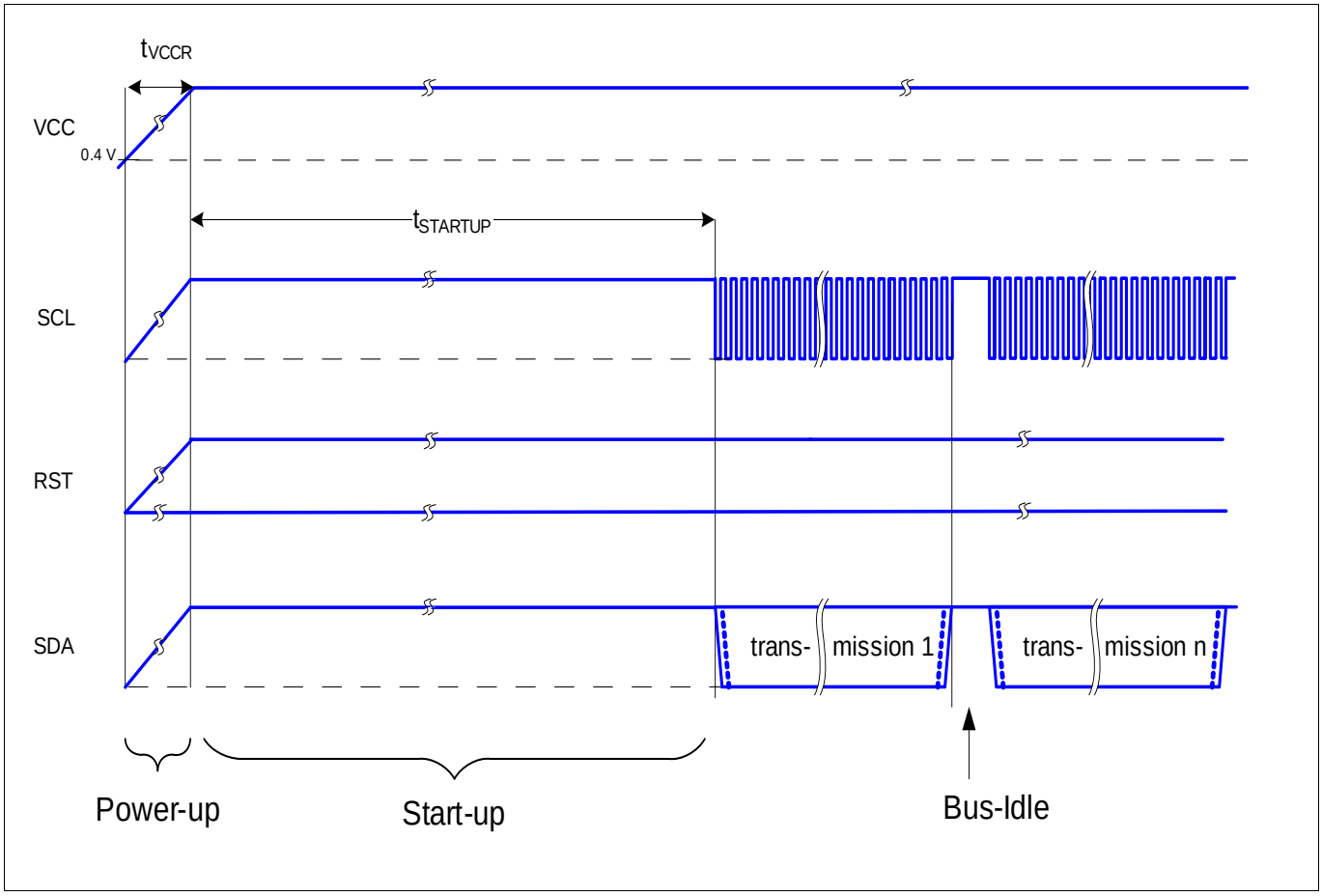


Figure 6 Start-up of I2C interface after power-on

4.2.3.2 Startup for warm resets

When using the reset signal for triggering a warm reset after power-on, the activation of the I2C interface needs the following reset procedure.

- VCC stays powered up.
- The terminal stops I2C communication. SDA and SCL lines are set to high level before RST is set to low-level.
- After its falling edge, RST has to be kept at low-level for at least t1. At the latest, t2, after the falling edge of RST, the terminal must set RST to high level.
- The first transmission may start at the earliest $t_{STARTUP}$ after the rising edge of RST.

The following figure shows the startup timing for this start-up case.

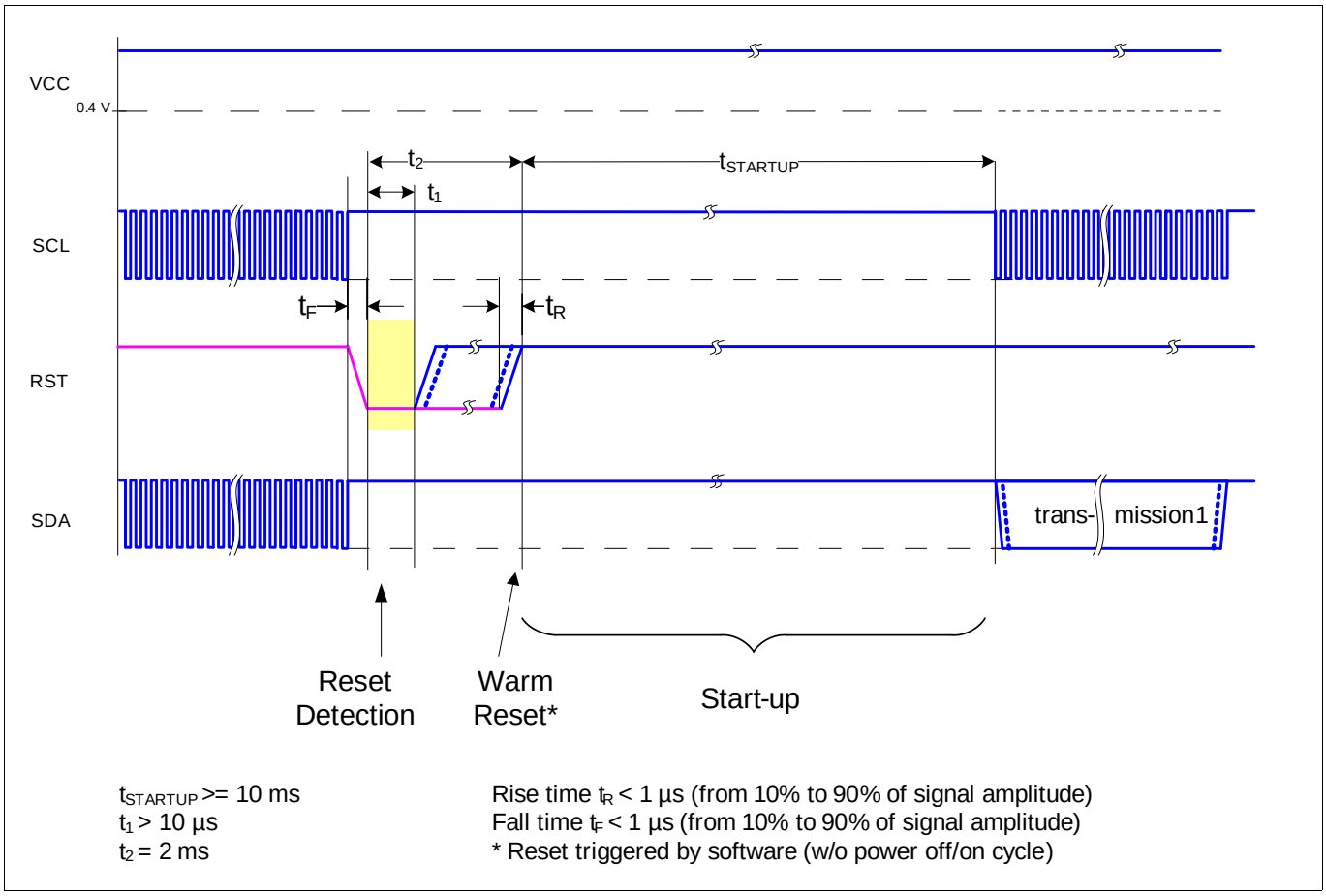


Figure 7 Startup of I2C interface for warm resets

Note: If NVM programming was requested prior to reset, $t_{STARTUP}$ will be prolonged from a typical value of 10 ms to a maximum of 12 ms.

4.2.4 I2C interface characteristics

For operation of the I2C interface, the electrical characteristics are compliant with the I2C bus specification for "Standard-mode" (f_{SCL} = 100 kHz) and "Fast-mode" (f_{SCL} = 400 kHz), with certain deviations as stated in the tables below.

Note: T_A as given for the controller's operating temperature range unless otherwise stated.

Table 8 I2C Standard-mode interface characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	–	100	kHz	
Input low level	V_{IL}	−0.3	–	0.2 * V_{CC}	V	
Input high level	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.3	V	
Output low level	V_{OL1}	0	–	0.3	V	Sink current 1 mA; V_{CC} > 2 V
	V_{OL2}	0	–	0.4	V	Sink current 1 mA; V_{CC} ≤ 2 V
	V_{OL3}	0	–	0.4	V	Sink current 1 mA; V_{CC} ≤ 2 V
Low level output current	I_{OL}	1	–	–	mA	V_{OL} = 0.4 V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	–	–	120	ns	C_b < 100 pF
SCL fall time (bus line, input)	t_{fSCL}	–	–	25	ns	
External pull-up on SDA	R_p	1.2	–	–	kΩ	
Capacitive load for each bus line	C_b	–	–	100	pF	

Table 9 I2C Fast-mode interface characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	–	400	kHz	
Input low level	V_{IL}	−0.3	–	0.2 * V_{CC}	V	
Input high level	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.3	V	
Hysteresis of input stage	V_{HYS}	0.05	–	–	V	
Output low level	V_{OL1}	0	–	0.3	V	Sink current 1 mA; V_{CC} > 2 V
	V_{OL2}	0	–	0.4	V	Sink current 1 mA; V_{CC} ≤ 2 V
	V_{OL3}	0	–	0.4	V	Sink current 1 mA; V_{CC} ≤ 2 V
Low level output current	I_{OL}	1	–	–	mA	V_{OL} = 0.4 V

Table 9 I2C Fast-mode interface characteristics (continued)

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	0.4	–	120	ns	10 pF < C_b < 100 pF
Spikes suppressed by input filter	t_{SP}	–	20	–	ns	Input filter implemented for SCL, not for SDA
SCL fall time (bus line, input)	t_{fSCL}	–	–	25	ns	
Input current (SDA, SCL)	I_I	−10	–	+10	µA	Pull up/down disabled V_{IN} in the range of 10% to 90% of pad supply voltage; see[1)]
External pull-up on SDA	R_p	1.2	–	–	kΩ	
Capacitive load for each bus line	C_b	–	–	100	pF	

1) The condition "If V_{CC} is switched off, I/O pins of fast-mode devices must not obstruct the SDA and SCL lines" is not fulfilled.

5 RoHS compliance

On January 27, 2003 the European Parliament and the council adopted the directives:

- 2002/95/EC on the Restriction of the use of certain Hazardous Substances in electrical and electronic equipment ("RoHS")
- 2002/96/EC on Waste Electrical and Electrical and Electronic Equipment ("WEEE")

Some of these restricted (lead) or recycling-relevant (brominated flame retardants) substances are currently found in the terminations (e.g. lead finish, bumps, balls) and substrate materials or mold compounds.

The European Union has finalized the Directives. It is the member states' task to convert these Directives into national laws. Most national laws are available, some member states have extended timelines for implementation. The laws arising from these Directives have come into force in 2006 or 2007.

The electro and electronic industry has to eliminate lead and other hazardous materials from their products. In addition, discussions are on-going with regard to the separate recycling of ceratin materials, e.g. plastic containing brominated flame retardants.

Infineon Technologies is fully committed to giving its customers maximum support in their efforts to convert to lead-free and halogen-free[1)] products. For this reason, Infineon Technologies' "Green Products" are ROHS-compliant.

Since all hazardous substances have been removed, Infineon Technologies calls its lead-free and halogen-free semiconductor packages "green." Details on Infineon Technologies' definition and upper limits for the restricted materials can be found here.

The assembly process of our high-technology semiconductor chips is an integral part of our quality strategy. Accordingly, we will accurately evaluate and test alternative materials in order to replace lead and halogen so that we end up with the same or higher quality standards for our products.

The use of lead-free solders for board assembly results in higher process temperatures and increased requirements for the heat resistivity of semiconductor packages. This issue is addressed by Infineon Technologies by a new classification of the Moisture Sensitivity Level (MSL). In a first step the existing products have been classified according to the new requirements.

1) Any material used by Infineon Technologies is PBB and PBDE-free. Plastic containing brominated flame retardants, as mentioned in the WEEE directive, will be replaced if technically/economically beneficial.

Revision history

Revision history	
Page or Item	**Subjects (major changes since previous revision)**
Revision 1.0, 2017-08-29	
	Initial version of Datasheet

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

Edition 2017-08-29
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about any aspect of this document?
Email:
security.chipcard.ics@infineon.com

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 technology, delivery terms and conditions and prices, please contact the 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.