OPTIGA™ Trust X

Datasheet

Key features

- High-end security controller
- Turnkey solution
- One-way authentication using ECDSA
- Mutual authentication using DTLS client (IETF standard RFC 6347)
- Secure communication using DTLS
- Compliant with the USB Type-C™ Authentication standard
- I2C interface
- Up to 10 KB user memory
- Cryptographic support: ECC256, AES128, SHA-256, TRNG, DRNG
- PG-USON-10-2 package (3 x 3 mm)
- Standard & extended temperature ranges
- Full system integration support
- Common Criteria Certified EAL6+ (high) hardware
- Cryptographic Tool Box based on ECC NIST P256, P384 and SHA256 (sign, verify, key generation, ECDH, session key derivation)

Key values

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

Applications

- Industrial control and automation
- Consumer electronics
- Smart home
- Medical devices

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 offers the OPTIGA™ Trust X as a turnkey security solution for industrial automation systems, smart homes, consumer devices and medical devices. This high-end security controller comes with full system integration support for easy and cost-effective deployment of high-end security for your assets.

Broad range of benefits

Integrated into your device, the OPTIGA™ Trust X supports protection of your brand and business case, differentiates your product from your competitors, and adds value to your product, making it stronger against cyberattacks.

Enhanced security

The OPTIGA™ Trust X comes with an advanced security controller employing Elliptic Curve Cryptography (ECC) with 256-bit keys, AES128 and SHA-256. This new security technology greatly enhances your overall system security. Furthermore, the OPTIGA™ Trust X covers a broad range of use cases necessary to protect the authenticity, integrity and confidentiality of your device: mutual authentication, secure communication, data store protection, lifecycle management, secure updates and also – from version X2 on – platform integrity protection.

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 X comes with OS, embedded application and complete host-side integration support. The extended temperature range of −40°C to +105°C combined with a standardized I^2C interface and the small PG-USON-10-2 footprint will enable all your embedded projects.

Almost 30 years in a market-leading position with nearly 20 billion security controllers shipped worldwide are the result of Infineon's strong expertise and its commitment to make security a success factor for you.

Products

Type	Description	Temperature range	Package
OPTIGA™ Trust X - SLS 32AIA020X4	Embedded security solution for connected devices	−25°C to +85°C Standard Temperature Range (STR)	PG-USON-10-2
OPTIGA™ Trust X - SLS 32AIA020X2	Embedded security solution for connected devices	−40°C to +105°C Extended Temperature Range (ETR)	PG-USON-10-2
Evaluation Kit	Provides all the components required to set up the environment to demonstrate the features of the OPTIGA™ Trust X		Board

2 Connectivity

This chapter explains the schematics of the products and gives some recommendations as to how the controller should be externally connected.

2.1 Power Supply Schematics

Figure 1 illustrates how the controller is to be supplied.

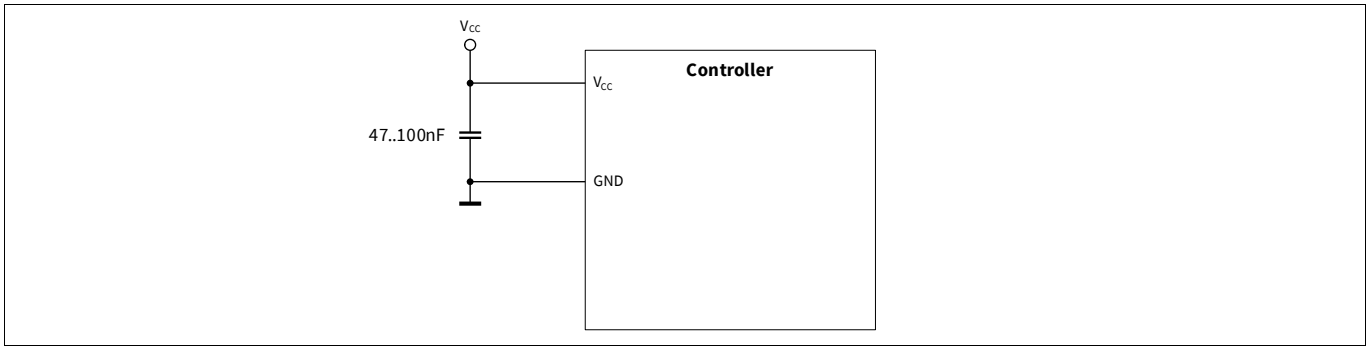

Figure 1 Power Supply Diagram

Contrary to other areas of application in which different types of capacitors are switched in parallel to stabilize the power supply, normally only one capacitor is required here. This is due to the wide variation limits of the supply voltage and the additional internal measures to handle sudden changes in load. For this decoupling capacitor, use a ceramic type with a low equivalent series resistance.

2.2 Pinout, Signal and Interface Characteristics Defined by OS

The following sections provide a more generic guidance on how power pins and interface signals are to be connected in the system.

2.2.1 Interfaces

This section shows how the interfaces are to be connected.

2.2.1.1 I2C

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

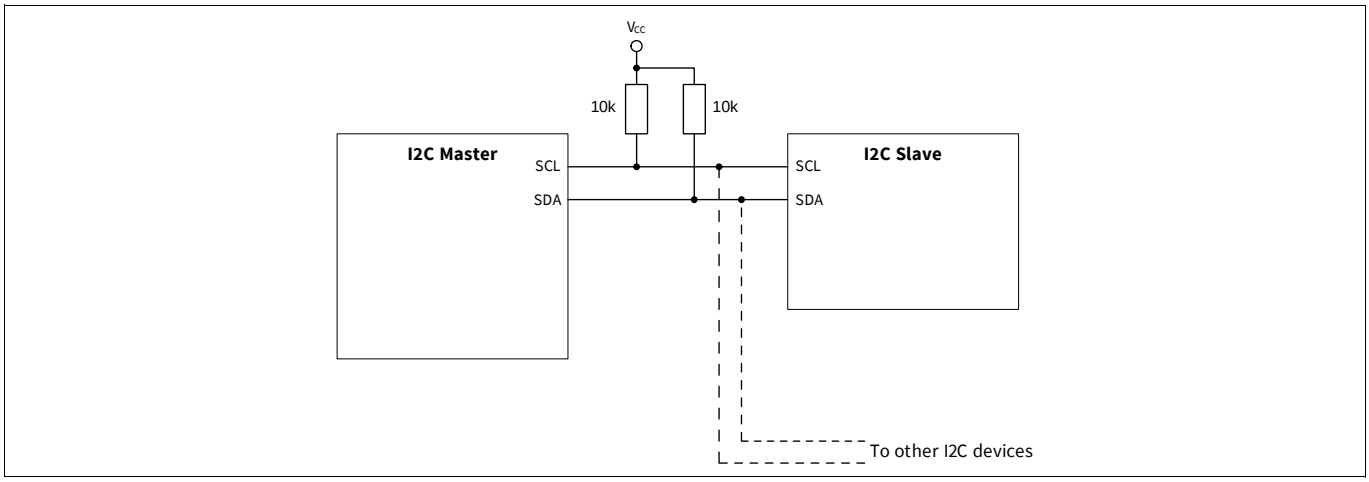

Figure 2 I2C Schematic Diagram

3 Description of Packages

This chapter provides information on the package types and how the interfaces of each product are assigned to the package pins. For further information on compliance of the packages with European Parliament Directives, see **“RoHS Compliance” on Page 15**.

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

3.1 PG-USON-10-2

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

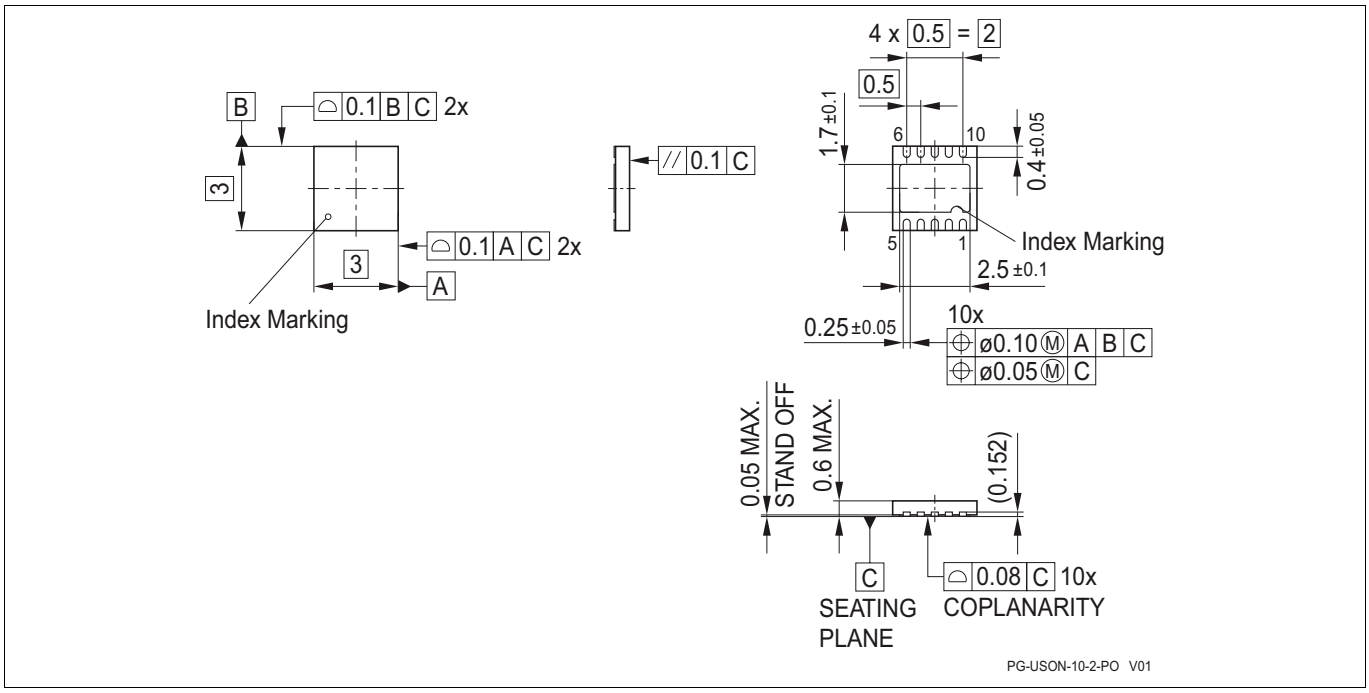

Figure 3 PG-USON-10-2 Package Outline

The following figure shows the footprint of the PG-USON-10-2 package:

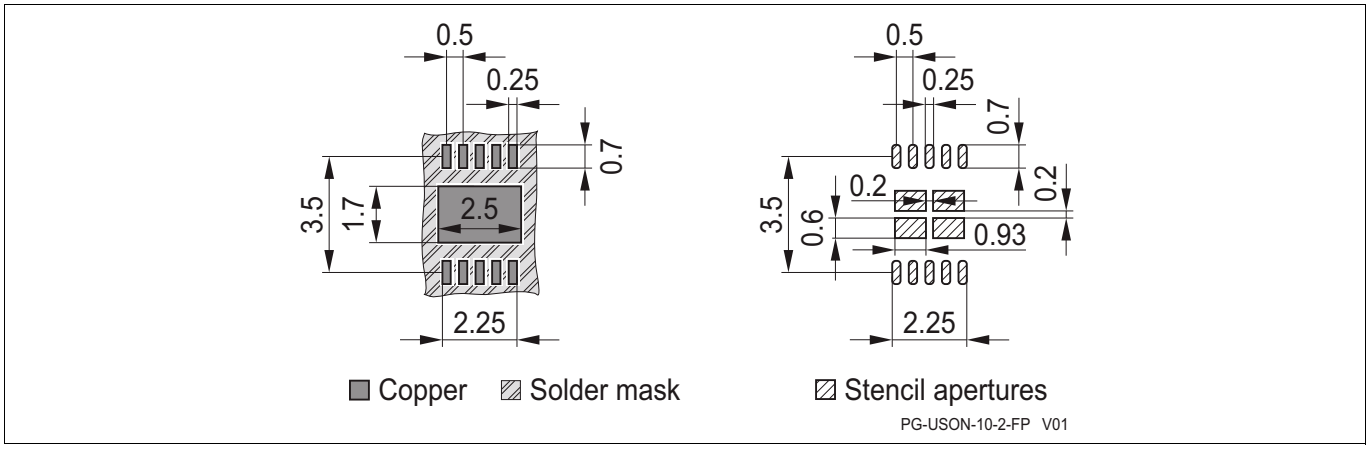

Figure 4 PG-USON-10-2 Package Footprint

Description of Packages

The figure below shows the PG-USON-10-2 in top view:

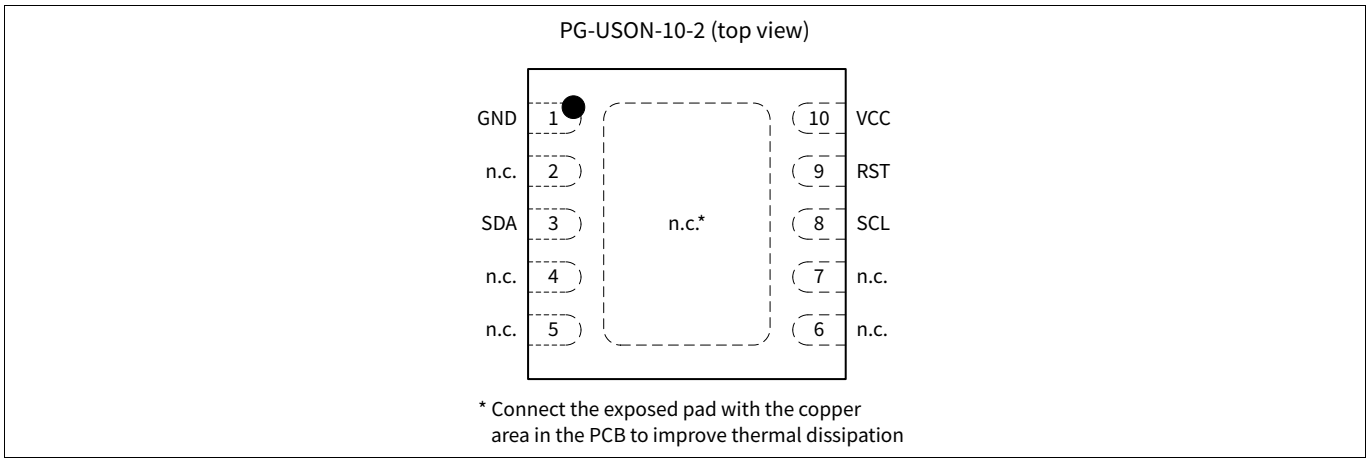

Figure 5 PG-USON-10-2 Top View

Production Sample Marking Pattern

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

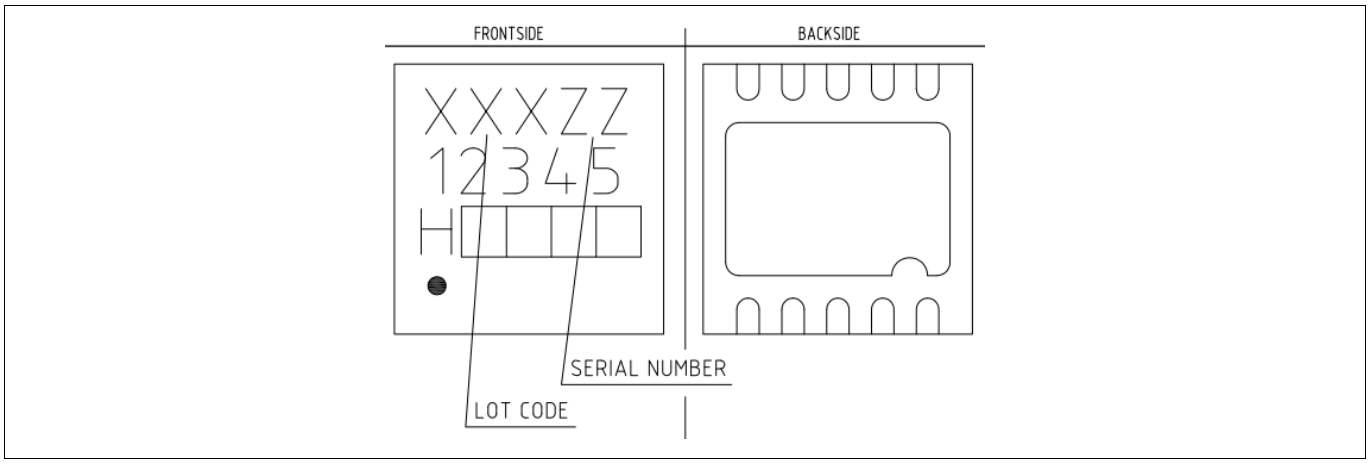

Figure 6 PG-USON-10-2 Sample Marking Pattern

The black dot indicates pin 01 for the chip. The following table describes the sample marking pattern:

Table 1 Marking Table for PG-USON-10-2 Packages

Indicator	Description
LOT CODE	Defined and inserted during fabrication
ZZ	Indicates the Certifying Authority Serial Number / SKU#, e.g. "00" would mean "SKU#0"
H/E	H = "Halogen-free", E = "Engineering samples" This indicator is followed by "YYWW", where YY is the "Year" and WW is the "Work Week" of the production. This is inserted during fabrication. Engineering samples have "E YYWW" and productive samples have "H YYWW"

Table 1 Marking Table for PG-USON-10-2 Packages (continued)

Indicator	Description
12345	Convention: T&#$@ where: • The letter "T" is constant throughout to indicate the OPTIGA™ Trust family • & indicates whether the product is a Trust X or Trust E controller • # indicates whether the controller is an ETR (E) or STR (S) variant • $ specifies the OPTIGA™ Trust X/E release version number • @ specifies the software version Example: "TXE10" means 'OPTIGA™ Trust X', 'ETR variant', 'release version 1', 'software version 0'

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

Table 2 Contact Definitions and Functions of PG-USON-10-2 Packages

Pin	Type	Function
01	GND	Supply voltage (Ground)
02	NC	Not connected
03	I/O	Serial Data Line (SDA)
04	NC	Not connected
05	NC	Not connected
06	NC	Not connected
07	NC	Not connected
08	I/O	Serial Clock Line (SCL)
09	IN	Active Low Reset (RST)
10	PWR	Supply voltage (V_{CC})

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.

4.1.1 Absolute Maximum Ratings

Table 3 Absolute Maximum Ratings

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Operating temperature (ambient)	T_A	−40	–	105	°C	ETR variant, T_J must be kept
		−25	–	85	°C	STR variant, T_J must be kept
Junction temperature	T_J	–	–	110	°C	–
Supply voltage	V_{CC}	−0.3	–	7.0	V	–
Input voltage	V_{IN}	−0.3	–	7.0	V	All pins with ISA feature (Indirect Supply Avoidance)[1)]
Operational lifetime[2)]	$TrustX_{life}$	–	–	–	Year	

1) The pins used for operating the I2C interface are provided with an "indirect supply avoidance" feature (ISA) which allows switching off of the supply voltage of the security controller regardless of the input voltage V_{IN_I2C} at these pins and without drawing a significant pad input current.

2) The operational lifetime is calculated on the basis of a defined application profile. The underlying application profile is described in the corresponding Qualification Report.

Notes

1. *The values stated in the table above may be further restricted for particular products (i.e., sales codes).*
2. *All voltages are referenced to common ground (GND) reference, unless otherwise specified.*
3. *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 NVM data retention and write/erase endurance.*

4.2 Electrical Characteristics

Notes

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

4.2.1 DC Electrical Characteristics

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

All currents flowing into the controller are considered positive.

Table 4 Electrical Characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC}	1.62	–	5.5	V	Overall functional range
	V_{CC_I2C}	1.62	–	5.5	V	Supply voltage range for operation of I2C
Supply current[1)]	I_{CCAVG}	–	14.0	–	mA	While running a typical authentication profile T_A = 25°C; V_{CC} = 5.0 V
Supply current, in *sleep mode*	I_{CCS3}	–	–	100	µA	T_A = 25°C; V_{CC_I2C} = 3.3 V; I2C ready for operation (no bus activity), all other inputs at V_{CC}, no other interface activity
RST input low voltage	V_{IL}	−0.3	–	0.3 * V_{CC}	V	
RST input high voltage	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.3	V	

1) Supply current can be limited from 6 mA to 15 mA by software commands.

4.2.2 AC Electrical Characteristics

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

All currents flowing into the controller are considered positive.

Table 5 AC Characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
V_{CC} rampup time	t_{VCCR}	1	–	1000	µs	400 mV to 90% of V_{CC} target voltage ramp

The V_{CC} ramp is depicted in **Figure 7**. 90% of the target supply voltage must be reached within t_{VCCR} after it has exceeded 400 mV. Moreover, its variation must be kept within a ±10% range.

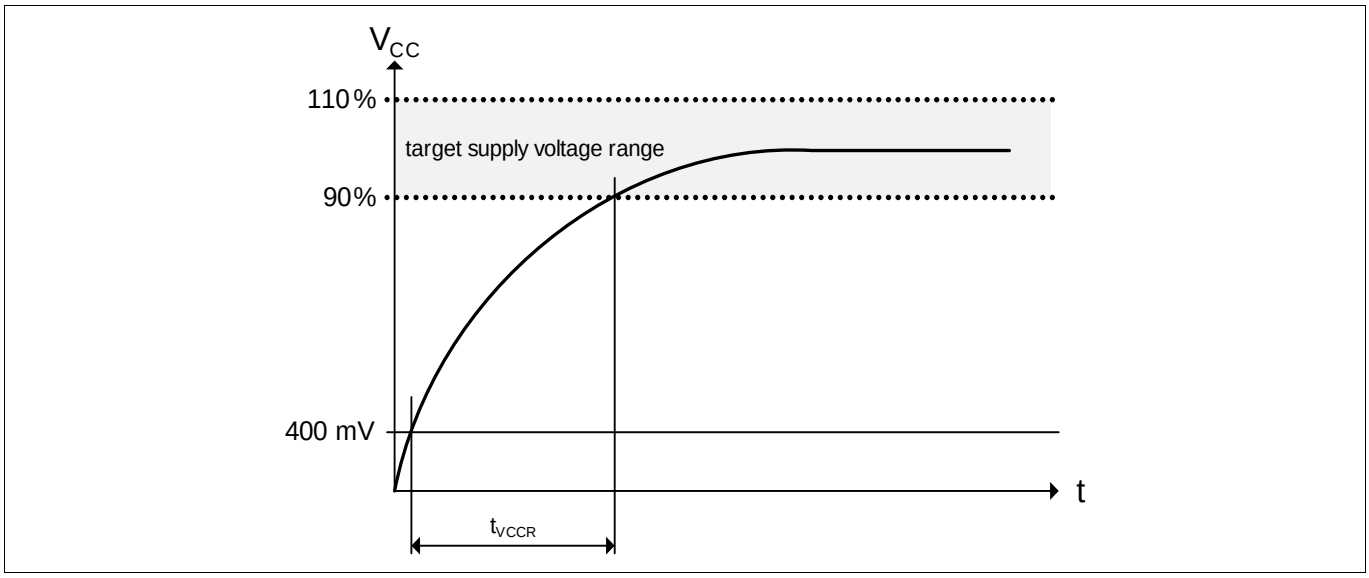

Figure 7 Vcc Rampup

4.2.3 I2C Interface Characteristics

4.2.3.1 General I2C Characteristics

Table 6 I2C Operation Supply and Input Voltages

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC_I2C}	1.62	–	5.5	V	
SDA, SCL input voltage	V_{IN_I2C}	−0.3	–	V_{CC_I2C} + 0.5 or 5.5[1)]	V	V_{CC_I2C} is in the operational supply range.
		−0.3	–	5.5	V	V_{CC_I2C} is switched off.

1) Whichever is lower

4.2.3.2 I2C Standard/Fast Mode Interface Characteristics

For operation of the I2C interface, the electrical characteristics are compliant with the I²C bus specification Rev. 4 for "standard-mode" (f_{SCL} up to 100 kHz) and "fast-mode" (f_{SCL} up to 400 kHz), with certain deviations as stated in the table below.

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

Table 7 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	–	0.3 * V_{CC_I2C}	V	
Low-level output voltage	V_{OL1}	0	–	0.4	V	Sink current 3 mA; $V_{CC\_I2C} \geq 2.7$ V Sink current 2 mA; $V_{CC\_I2C} < 2.7$ V
Low-level output current	I_{OL}	3 2	–	–	mA	$V_{OL} = 0.4$ V; $V_{CC\_I2C} \geq 2.7$ V $V_{OL} = 0.4$ V; $V_{CC\_I2C} < 2.7$ V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	–	–	250	ns	$C_b \leq 400$ pF; $V_{CC\_I2C} \geq 2.7$ V $C_b \leq 200$ pF; $V_{CC\_I2C} < 2.7$ V
Capacitive load for each bus line	C_b	–	–	400 200	pF	$V_{CC\_I2C} \geq 2.7$ V $V_{CC\_I2C} < 2.7$ V

Table 8 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	–	0.3 * V_{CC_I2C}	V	

Table 8 I2C Fast Mode Interface Characteristics (continued)

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Low-level output voltage	V_{OL1}	0	–	0.4	V	Sink current 3 mA; $V_{CC\_I2C} \geq 2.7$ V Sink current 2 mA; $V_{CC\_I2C} < 2.7$ V
Low-level output current	$I_{OL\ (0.4)}$	3 2	–	–	mA	$V_{OL} = 0.4$ V; $V_{CC\_I2C} \geq 2.7$ V $V_{OL} = 0.4$ V; $V_{CC\_I2C} < 2.7$ V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	20 * V_{CC_I2C} / 5.5 V[1)]	–	250	ns	$C_b \leq 400$ pF; $V_{CC\_I2C} \geq 2.7$ V $C_b \leq 200$ pF; $V_{CC\_I2C} < 2.7$ V
Capacitive load for each bus line	C_b	15[2)]	–	400 200	pF	$V_{CC\_I2C} \geq 2.7$ V $V_{CC\_I2C} < 2.7$ V

1) A min. capacitive load is necessary to reach t_{OF}.

2) A min. capacitive load is necessary to reach t_{fmin}.

4.2.3.3 I2C Fast Mode Plus Interface Characteristics

For operation of the I2C interface, the electrical characteristics are compliant with the I^2C bus specification Rev. 4 for "fast mode plus" (f_{SCL} up to 1 MHz), with certain deviations as stated in the table below.

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

Table 9 I2C Fast Mode Plus Interface Characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	–	1000	kHz	
Input low-level	V_{IL}	−0.3	–	0.3 * V_{CC_I2C}	V	
Low-level output voltage	V_{OL1}	0	–	0.4	V	Sink current 3 mA; $V_{CC\_I2C} \geq 2.7$ V Sink current 2 mA; $V_{CC\_I2C} < 2.7$ V
Low-level output current	I_{OL}	3 2	–	–	mA	$V_{OL} = 0.4$ V; $V_{CC\_I2C} \geq 2.7$ V $V_{OL} = 0.4$ V; $V_{CC\_I2C} < 2.7$ V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	20 * V_{CC_I2C} / 5.5 V[1)]	–	120	ns	$C_b \leq 150$ pF
Capacitive load for each bus line	C_b	15[1)]	–	150	pF	

1) A min. capacitive load is necessary to reach t_{OF}.

4.2.3.4 Start-Up of I2C Interface

There are 2 variants possible for performing the startup procedure:

- Startup after power-on
- Startup for warm resets

4.2.3.4.1 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.

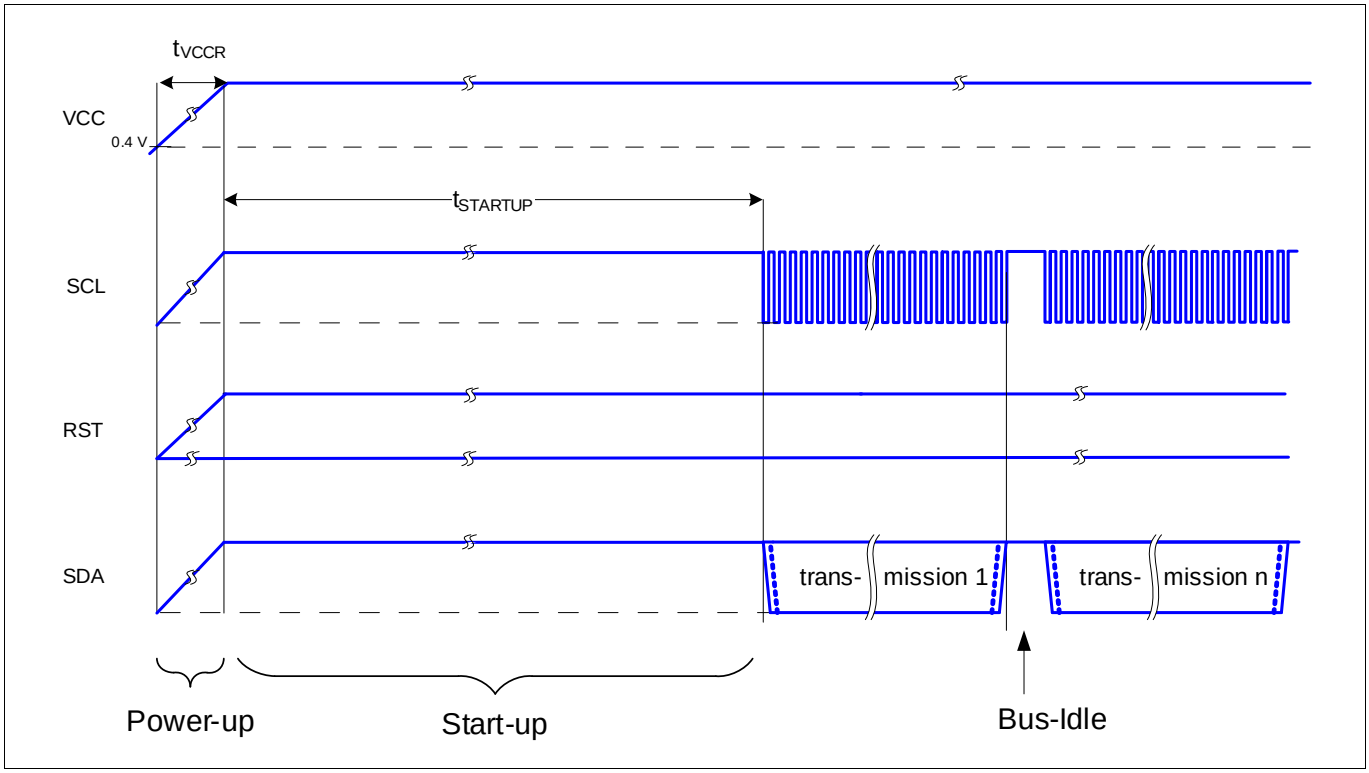

Figure 8 Startup of I2C Interface After Power-On

Table 10 Startup of I2C Interface After Power-On

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Startup time	$t_{STARTUP}$	10			ms	

4.2.3.4.2 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 remains 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 timing for this startup case.

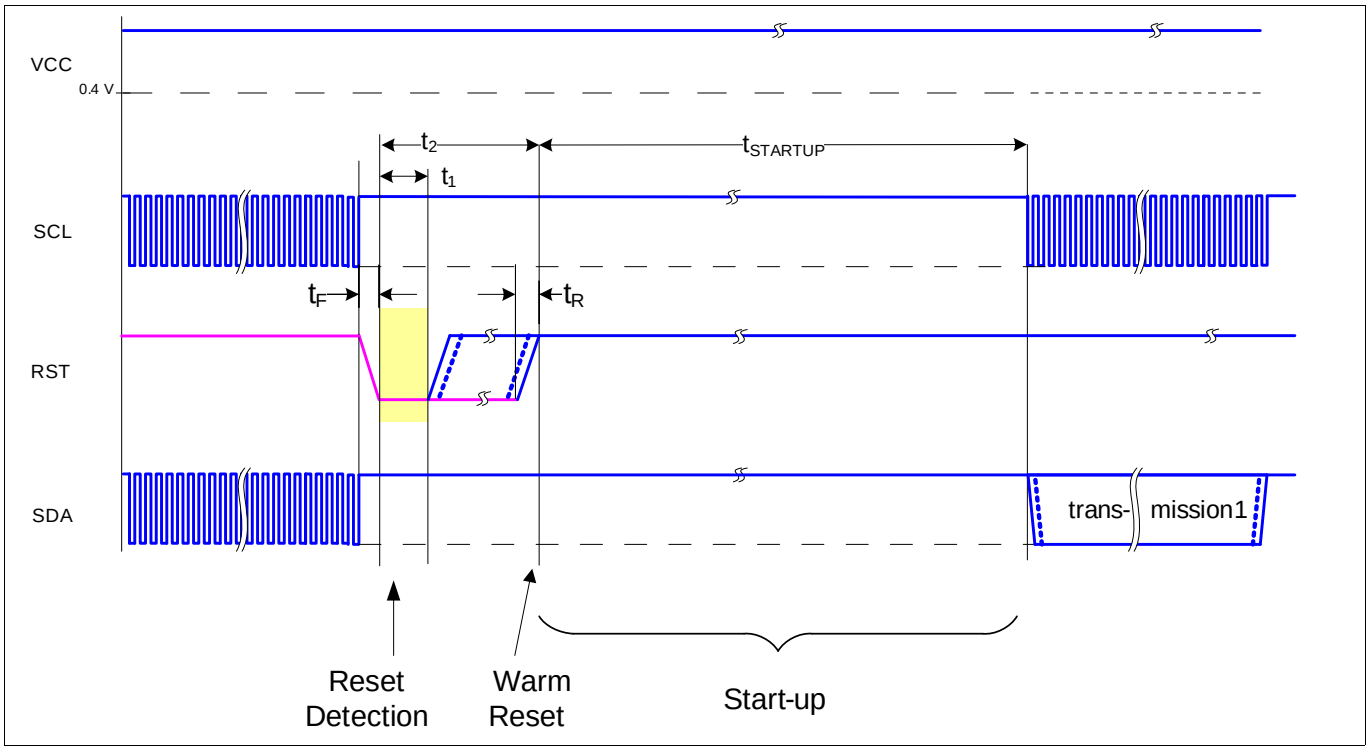

Figure 9 Startup of I2C Interface for Warm Resets

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

Table 11 Startup of I2C Interface for Warm Resets[1)]

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Startup time	$t_{STARTUP}$	10			ms	
Rise time	t_R			1	µs	From 10% to 90% of signal amplitude
Fall time	t_F			1	µs	From 10% to 90% of signal amplitude
Reset detection	t_1	10			µs	
Reset low	t_2	10		2500	µs	

1) Reset triggered by software (without power off/on cycle)

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 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's "Green Products" are ROHS-compliant.

Since all hazardous substances have been removed, Infineon calls its lead-free and halogen-free semiconductor packages "green." Details on Infineon's 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 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 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 2.1, 2017-06-23	
Key features, **Enhanced security**	Modified text
Revision 2.0, 2017-06-08	
Key features	Added TRNG and DRNG to cryptographic support features
Key features, **Enhanced security**	Added cryptographic toolbox
Key features, **Enhanced security**	Added footnote indicating current limitation configuration by software commands
CoverBack	Removed trademarks from back cover
Revision 1.4, 2017-02-22	
	First version for release
Revision 1.3 (Internal review)	
Revision 1.2 (Internal review)	
Revision 1.1 (Internal review)	
Revision 1.0 (Internal review)	
	Initial version

Revision History

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

Edition 2017-06-23
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.