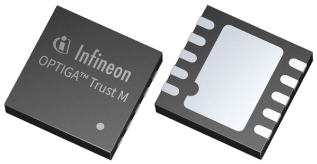
OPTIGA™ Trust M

Datasheet

Document release reference: Z8F80311641-D

Features



- High-end security controller
- Based on Common Criteria EAL 6+ (high) certified hardware
- PSA Level 3 certified
- Turnkey solution
- Up to 10 kB user memory
- PG-USON-10-2,-4 package (3 mm x 3 mm)
- Standard & extended temperature ranges
- I2C interface with Shielded Connection (encrypted communication)
- Cryptographic support:
  - ECC: NIST curves up to P-521, Brainpool r1 curve up to 512,
  - RSA® up to 2048,
  - AES key up to 256,
  - Hashing support up to SHA-256, HMAC up to SHA-512,
  - TLS v1.2 PRF and HKDF up to SHA-512
- OPTIGA™ Trust M Software Framework on Github - https://github.com/Infineon/optiga-trust-m
- Crypto ToolBox commands for SHA-256, ECC and RSA® Feature, AES, HMAC and Key derivation
- Configurable device security monitor, 4 Monotonic up counters
- Protected (integrity and confidentiality) update of data, key and metadata objects
- Hibernate for zero power consumption (Leakage current < 2.5µA only)
- Lifetime for Industrial Automation and Infrastructure is 20 years and 15 years for other Application Profiles

Potential applications

- Industrial control and building automation
- Consumer electronics and Smart Home
- Cloud connectivity
- Multicopters and drones

Benefits

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

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

Table of contents

List of tables

List of figures

1 Introduction

As embedded systems (for example, IoT devices) are increasingly gaining the attention of attackers, Infineon offers the OPTIGA™ Trust M as a turnkey security solution for industrial automation systems, smart homes, consumer devices and healthcare 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.

1.1 Broad range of benefits

Integrated into your device, the OPTIGA™ Trust M 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.

1.2 Enhanced security

The OPTIGA™ Trust M is based on an advanced security controller with built-in tamper-resistant NVM for secured storage and Symmetric/Asymmetric crypto engines to support ECC NIST curves up to P-521, ECC Brainpool curve up to P-512, RSA® up to 2048, AES key up to 256, HMAC up to SHA-512, HKDF up to SHA-512 and SHA-256. This new security technology greatly enhances your overall system security.

1.3 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 M comes with preprogrammed OS/Application code locked and with host-side modules to integrate with host micro controller software. The temperature range of −40°C to +105°C combined with a standardized I2C interface and the small PG-USON-10-2,-4 footprints will facilitate onboarding in your existing ecosystem. Almost 30 years in a market-leading position with nearly 20 billion security controllers shipped worldwide are the results of Infineon's strong expertise and its commitment to make security a success factor for you.

1.4 Applications

The OPTIGA™ Trust M covers a broad range of use cases necessary for many types of applications that include the following:

1. Network node protection using Mutual Authentication such as TLS or DTLS
2. Protect the Authenticity, Integrity and Confidentiality of your product, data and IP
3. Secured Communication
4. Datastore Protection
5. Lifecycle Management
6. Platform Integrity Protection
7. Secured Updates

1.5 Device features

The OPTIGA™ Trust M comes with up to 10 kB of user memory that can be used to store X.509 certificates and data. OPTIGA™ Trust M is based on Common Criteria (CC) EAL6+ (high) certified hardware enabling it to prevent physical attacks on the device itself and providing a high level of protection for stored keys or arbitrary data stored against access by an unauthorized entity. OPTIGA™ Trust M (SLS 32AIA010MK) is certified to PSA Level 3. The PSA certificate can be found at http://www.psacertified.org. The CC certificate can be found at www.bsi.bund.de by searching for BSI-DSZ-CC-0961 (Hardware Identifier IFX_CCI_00000Bh) and referring to the latest CC certificate. OPTIGA™ Trust M supports a high-speed I2C communication interface of up to 1 MHz (FM+).

Table 1 Products for V1

Sales Code	Temperature range	Package	Description	Evaluation Kit
OPTIGA™ Trust M SLS 32AIA010MH	−40°C to +105°C Extended Temperature Range (ETR)	PG-USON-10-2,-4	Embedded security solution for connected devices	PSoC™ 62S2 Wi-Fi BT Pioneer Kit connected to the OPTIGA™ Trust M shield
OPTIGA™ Trust M SLS 32AIA010MS	−25°C to +85°C Standard Temperature Range (STR)	PG-USON-10-2,-4		

Table 2 Products for V3

Sales Code	Temperature range	Package	Description	Evaluation Kit
OPTIGA™ Trust M SLS 32AIA010ML	−40°C to +105°C Extended Temperature Range (ETR)	PG-USON-10-2,-4	Embedded security solution for connected devices	PSoC™ 62S2 Wi-Fi BT Pioneer Kit connected to the OPTIGA™ Trust M shield
OPTIGA™ Trust M SLS 32AIA010MK	−25°C to +85°C Standard Temperature Range (STR)	PG-USON-10-2,-4		

Table 3 Default configurations based on the features of OPTIGA™ Trust M V3

Sales Code	Temperature range	Package	Description	Evaluation Kit
OPTIGA™ Trust M Express SLS 32AIA010MLUSON10 XTMA9	-40 ˚C to +105 ˚C Extended Temperature Range (ETR)	PG-USON-10-2,-4	Embedded security solution for quick and easy cloud onboarding	PSoC™ 62S2 Wi-Fi BT Pioneer Kit connected to the OPTIGA™ Trust M Express shield
OPTIGA™ Trust M MTR SLS 32AIA010MM	-25 ˚C to +85 ˚C Standard Temperature Range (STR)	PG-USON-10-2,-4	Embedded security solution for Matter enabled devices	PSoC™ 62S2 Wi-Fi BT Pioneer Kit connected to the OPTIGA™ Trust M MTR shield

Infineon and its distribution partners offer a wide range of customization options (for example, X.509 certificate generation and key provisioning) for the security chip. For details on offered solutions (like OPTIGA™ Trust M Express), selection guide and orders, please see the following page:

https://www.infineon.com/optiga-trust-m

Table 4 Features

Features	Supported Curve/Algorithm	ToolBox commands	V1	V3
ECC	ECC NIST P256/384	Sign, Verify, Key generation, and ECDH(E)	x	x
	ECC NIST P521, ECC Brainpool P256/384/512 r1	Sign, Verify, Key generation, and ECDH(E)		x

(table continues...)

Table 4 (continued) Features

Features	Supported Curve/Algorithm	ToolBox commands	V1	V3
RSA®	RSA® 1024/2048	Sign, Verify, Key generation, Encrypt and Decrypt	x	x
Key Derivation	TLS v1.2 PRF SHA-256	TLS PRF using SHA-256	x	x
	TLS v1.2 PRF SHA-384/512	TLS PRF using SHA-384/512		x
	HKDF SHA-256/384/512	HKDF using SHA-256/384/512		x
AES	Key size - 128/192/256 (ECB, CBC, CBC-MAC, CMAC)	Key generation, Encrypt and Decrypt		x
Random generation	TRNG, DRNG, Pre-Master secret for RSA® Key exchange	Generate random	x	x
HMAC	HMAC with SHA-256/384/512	HMAC generation and Verification		x
Hash	SHA-256	Hash generation	x	x
Protected data (object) update (Integrity)	ECC NIST P256/384 RSA® 1024/2048 Signature scheme as ECDSA FIPS 186-3/RSA® SSA PKCS#1 v1.5 without hashing	Secured data object update	x	x
	ECC NIST P521, ECC Brainpool P256/384/512 r1 Signature scheme as ECDSA FIPS 186-3/RSA® SSA PKCS#1 v1.5 without hashing	Secured data object update		x
Protected Data/key/ metadata update (Integrity and/or confidentiality)	ECC NIST P256/384/521 ECC Brainpool P256/384/512 r1 RSA® 1024/2048 Signature scheme as ECDSA FIPS 186-3/RSA® SSA PKCS#1 v1.5 without hashing	Secured data/key object update and metadata update for Data/key object		x

2 System block diagram

The following figure depicts the system block diagram for OPTIGA™ Trust M.

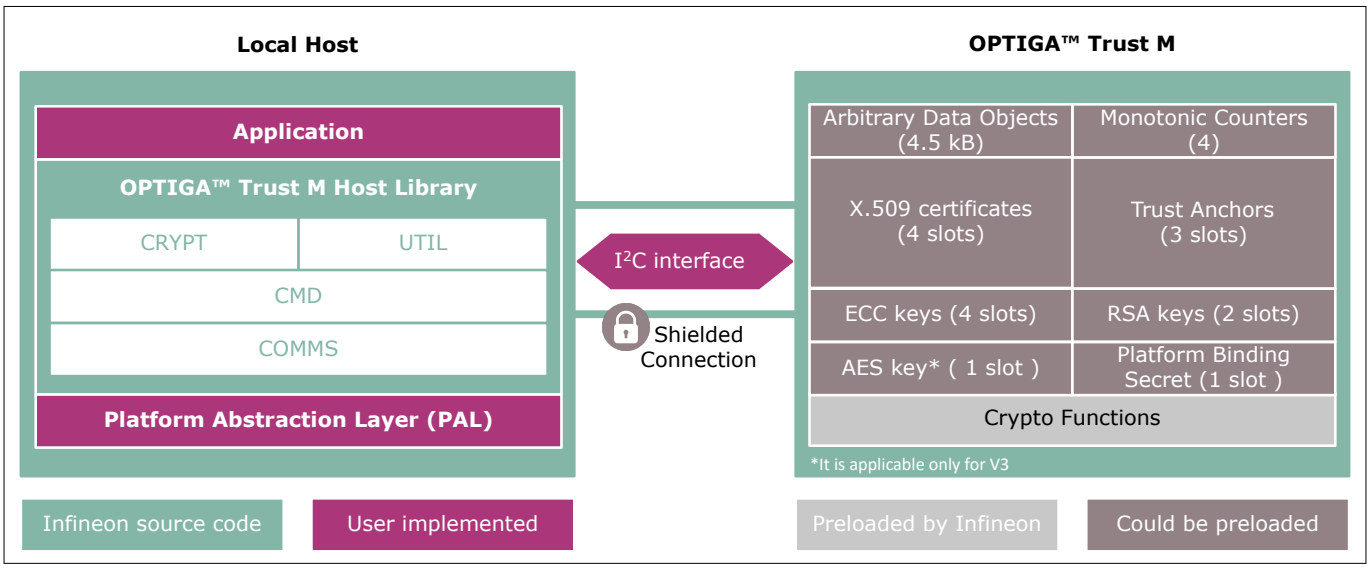


Figure 1 System block diagram

The system block diagram is explained below for each layer.

1. Local Host

- Local Host Application – This is the target application which utilizes OPTIGA™ Trust M for its security needs
- OPTIGA™ Trust M Host Library
  - CRYPT – Provides APIs to perform cryptographic functionalities. Any TLS stack can be integrated on Local Host as part of 3rd party Crypto Library to offload crypto operations to OPTIGA™ Trust M
  - UTIL – Provides APIs such as read/write, protected update of data, metadata, key objects and open/close application (for example, Hibernate)
  - CMD – Provides APIs to send and receive commands (OPTIGA™ Trust M external interface) to and from OPTIGA™ Trust M
  - COMMS – Provides wrapper APIs for communication (optional encrypted communication using Shielded Connection) with OPTIGA™ Trust M which internally uses Infineon I2C Protocol (IFX I2C)
- PAL – A layer that abstracts platform specific drivers (for example, I2C, Timer, GPIO, platform crypto library etc.)

2. OPTIGA™ Trust M

- Arbitrary Data Objects – The target application can store up to 4.5 kB (~4600 bytes) of data into OPTIGA™ Trust M. The data could be additional Trust Anchors, certificates and shared secret
- Monotonic Counters - Provides 4 monotonic counting data objects (up counters). These can be used as general purpose counter or as linked counter to other objects.

  For more information, please refer to Solution Reference Manual document available as part of the package
- X.509 – Up to 4 X.509 based Certificates can be stored
- Keys – Up to 4 ECC , 2 RSA® and 1 AES based keys can be stored
- Secret – 1 Platform binding secret can be stored
- Trust Anchors – 3 slots, for Mutual Authentication (TLS/DTLS) and Firmware Updates can be stored
- Crypto Functions - OPTIGA™ Trust M provides cryptographic functions that can be invoked via local host

2 System block diagram

***Note**: Unique AES key, ECC/RSA® private keys and X.509 Certificates – During production at Infineon fab, unique asymmetric keys (private and public) are generated and symmetric key/shared secrets are provisioned. The public key is signed by customer specific CA and the resulting X.509 certificate issued is securely stored in the OPTIGA™ Trust M. Special measures are taken to prevent the leakage and modification of private key/shared secret material at the Common Criteria Certified production site.*

3 Interface and schematics

The following figure illustrates how to integrate OPTIGA™ Trust M with your local host.

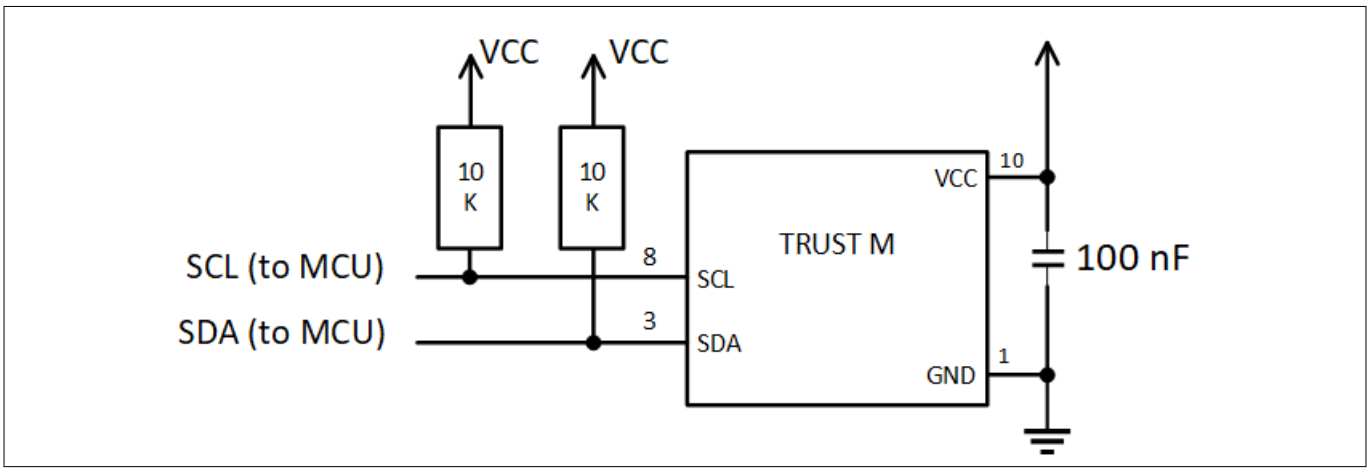


Figure 2 System integration schematic diagram

***Note**: The OPTIGA™ Trust M can be integrated with IFX I2C reset option as soft reset (IFX_I2C_SOFT_RESET), or hardware reset. Value of the pullup resistors depend on the target application circuit and the target I2C frequency.*

3.1 System integration schematics with hibernation support

The following figure illustrates how to integrate OPTIGA™ Trust M with hibernation, with local host GPIO used as VCC.

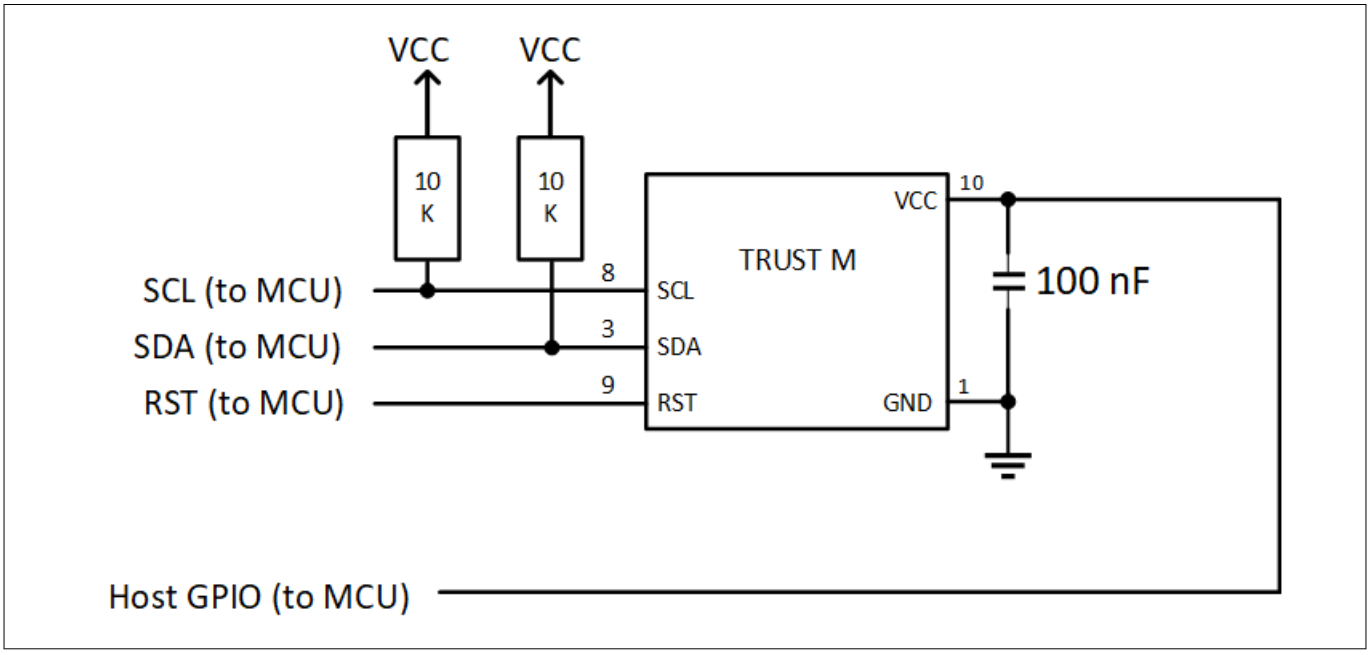


Figure 3 System integration schematic with hibernation – GPIO as VCC

***Note**: The Host GPIO pin must have sufficient current to drive the supply current, as per Table 11. Value of the pullup resistors depend on the target application circuit and the target I2C frequency.*

If the host GPIO does not supply sufficient current to OPTIGA™, additional MOSFET switching circuitry is needed to control the power supply (VCC). The below circuit diagrams depict the options to control the power supply (VCC) using GPIO from Host with the switching logic.

The following figure illustrates how to integrate OPTIGA™ Trust M with hibernation, with local host GPIO using single MOSFET to switch the VCC.

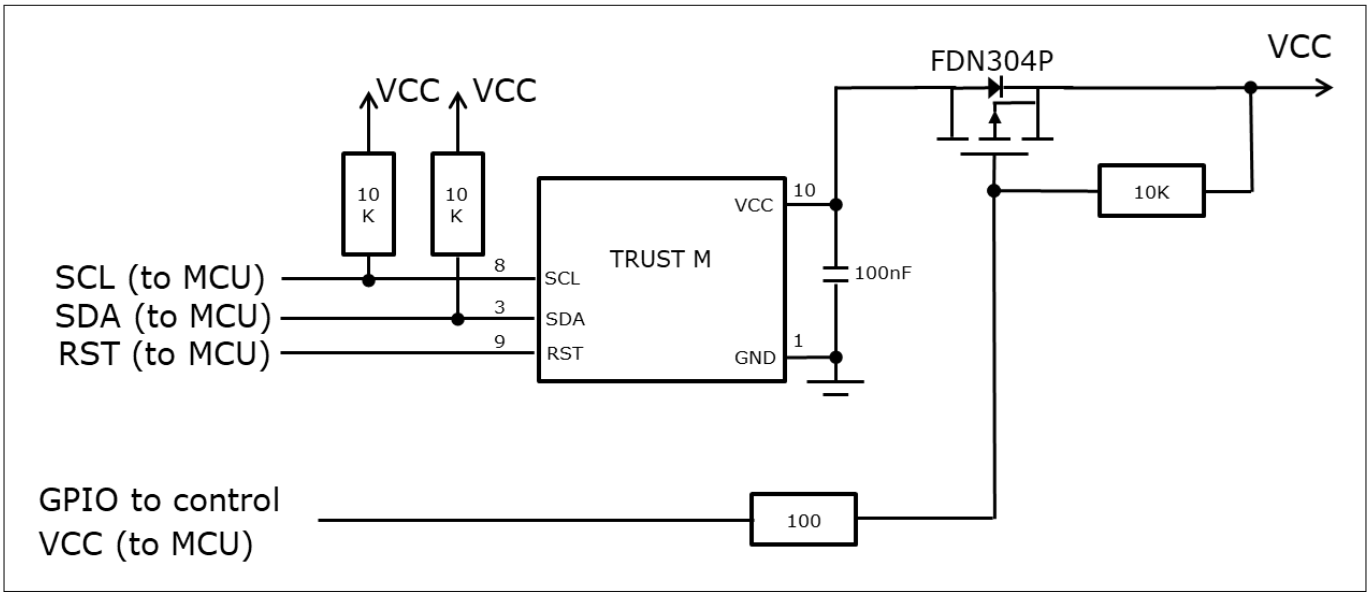


Figure 4 **System integration schematic with hibernation - GPIO controlled VCC (Single MOSFET switch)**

***Note**: Due to the single P channel MOSFET (FDN304P) behavior, GPIO must be connected and drive the pin to LOW to enable the VCC supply to OPTIGA™ Trust M. This adaption must be done in the OPTIGA™ host library (ifx_i2c.c), refer to chapter 11.1.1 for details. Value of the pullup resistors depend on the target application circuit and the target I2C frequency.*

The following figure illustrates how to integrate OPTIGA™ Trust M with hibernation, with local host using two MOSFET to switch the VCC.

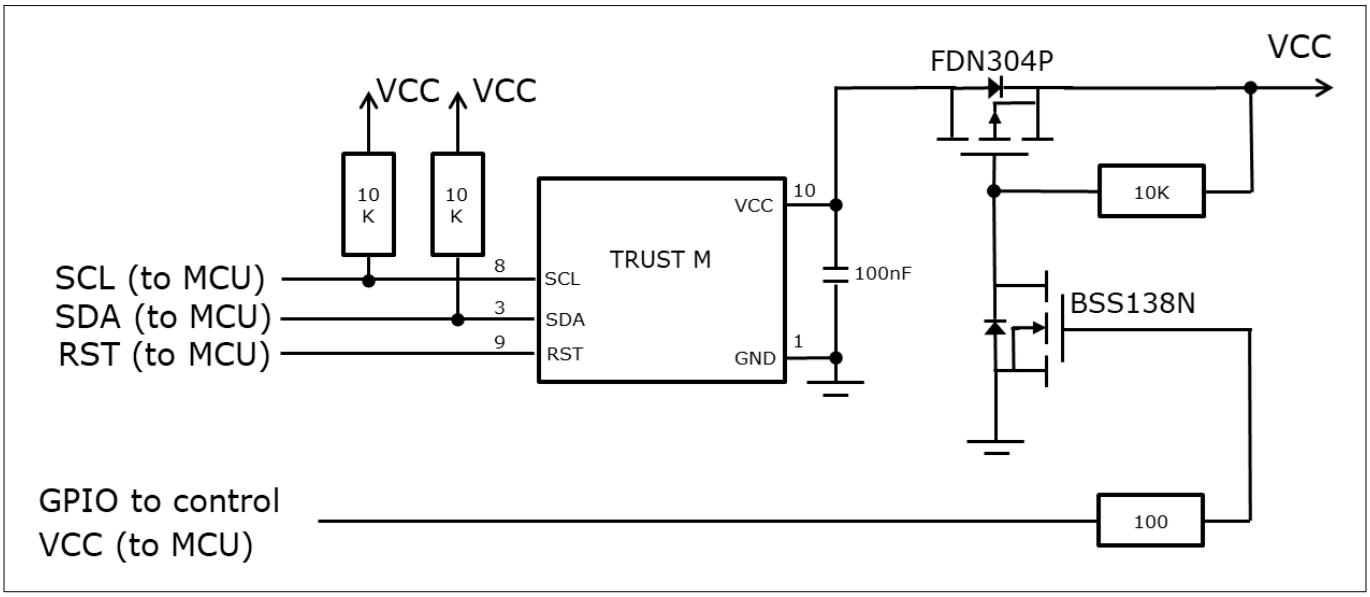


Figure 5 **System integration schematic with hibernation - GPIO controlled VCC (Dual MOSFET switch)**

***Note**: Value of the pullup resistors depend on the target application circuit and the target I2C frequency. If GPIO pin is connected, set the GPIO pin to HIGH to enable the VCC to OPTIGA™ Trust M.*

4 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 29.

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

4.1 PG-USON-10-2,-4

The package dimensions (in mm) of the controller in PG-USON-10-2,-4 packages are given below.

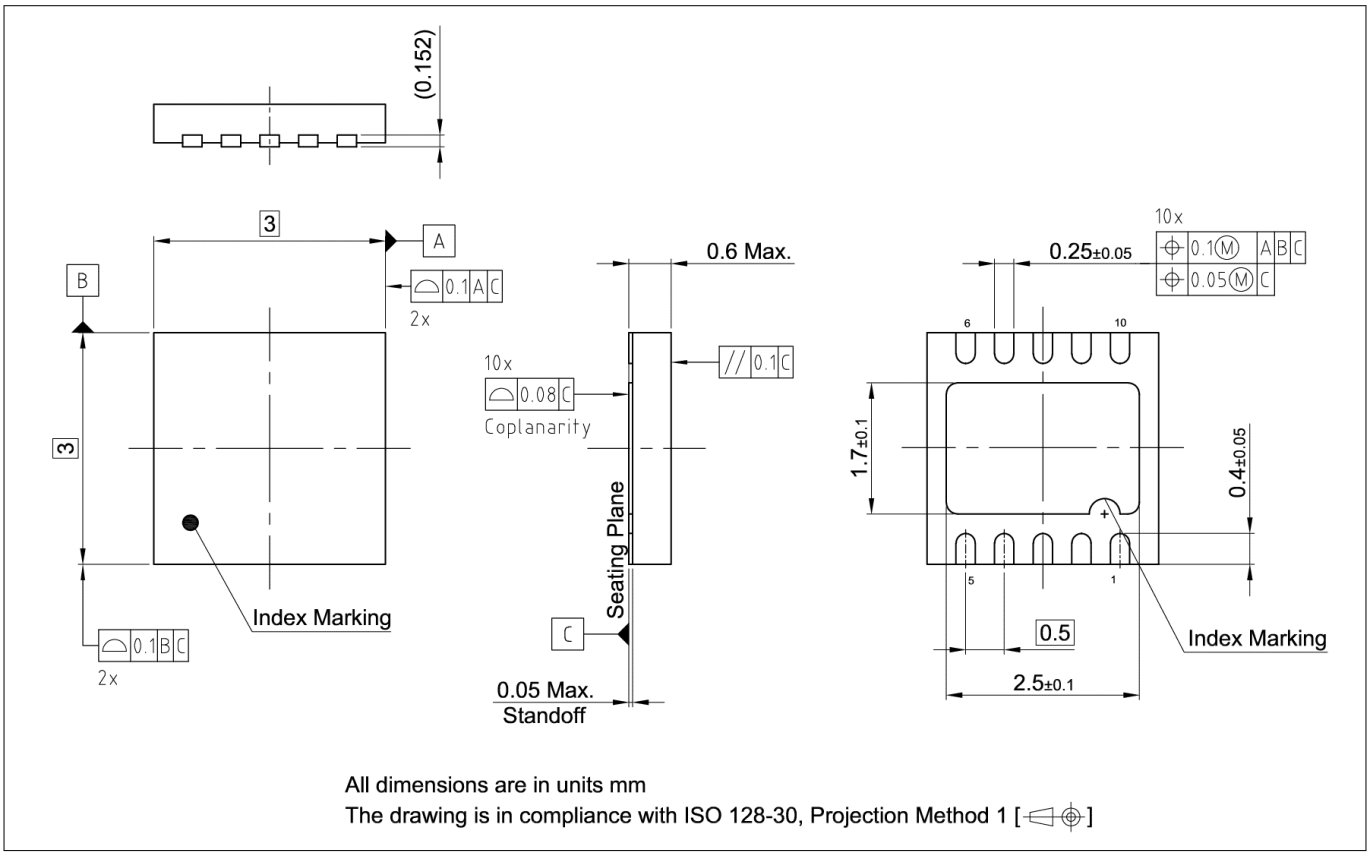


Figure 6 PG-USON-10-2,-4 Package Outline

The following figure shows the PG-USON-10-2,-4 in top view:

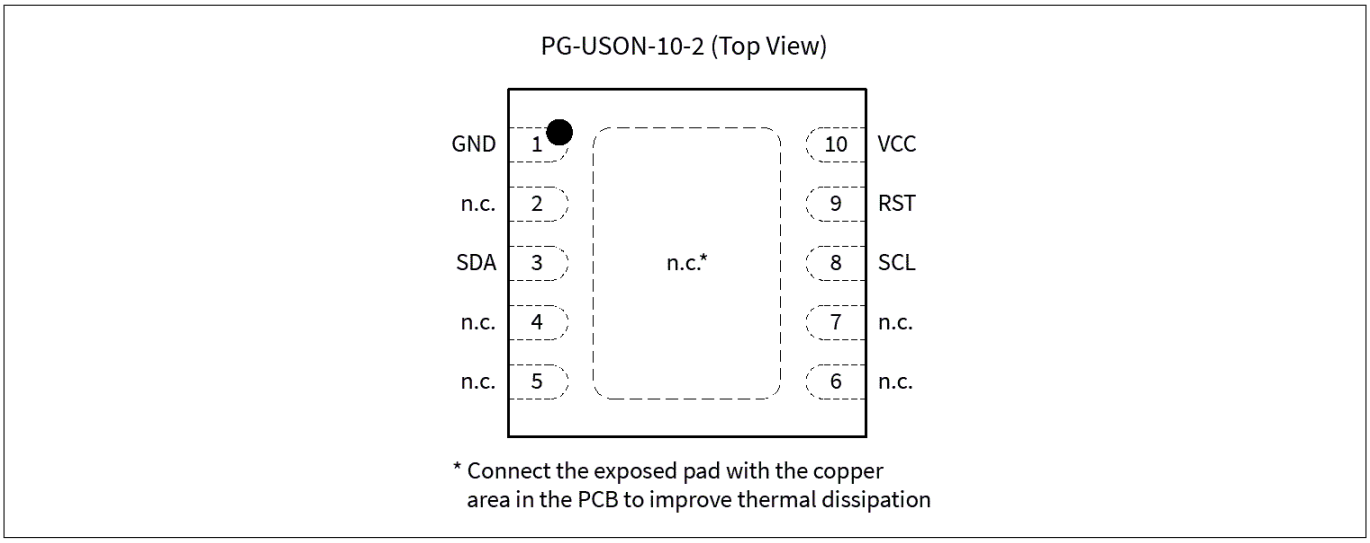


Figure 7 PG-USON-10-2,-4 top view

4.2 Production sample marking pattern

The following figure describes the productive sample marking pattern on PG-USON-10-2,-4.

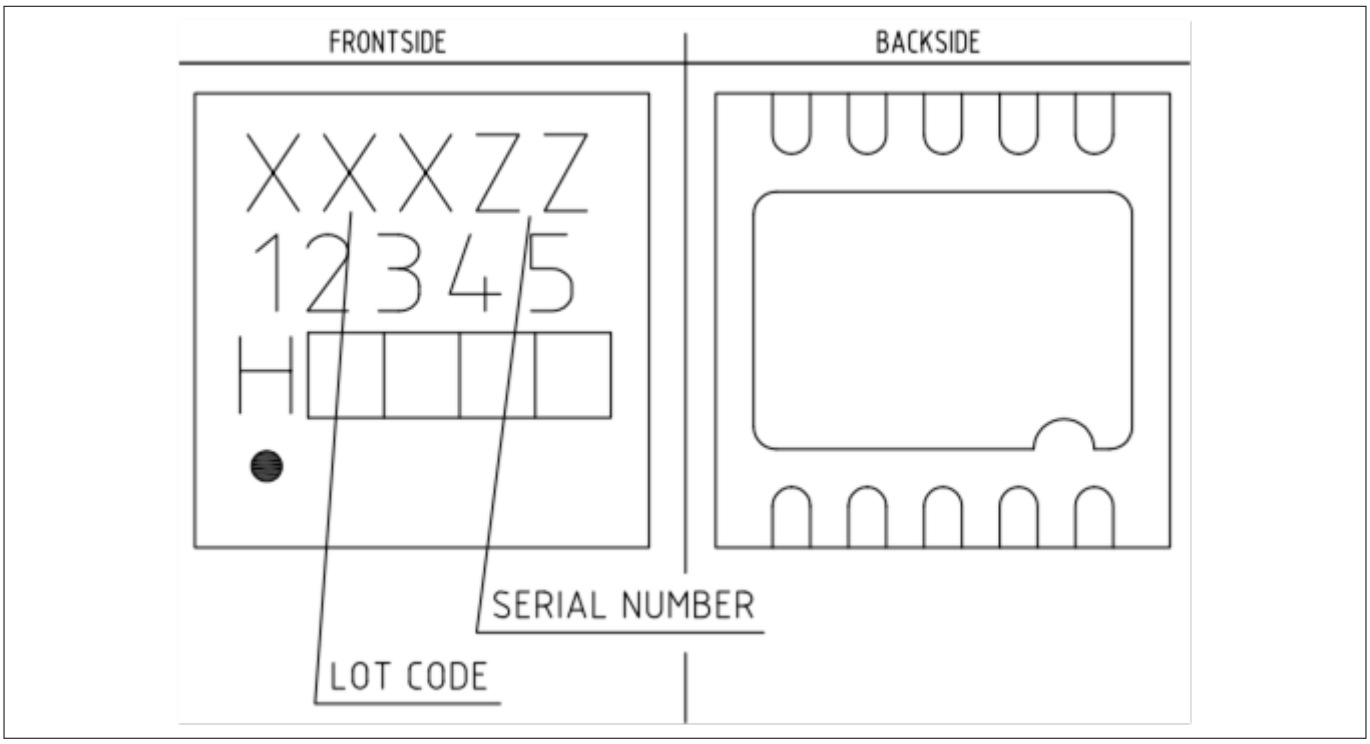


Figure 8 PG-USON-10-2,-4 sample marking pattern

The black dot indicates pin 01 for the chip. The following Table 5 describes the sample marking pattern:

Table 5 Marking table for PG-USON-10-2,-4 packages

Indicator	Description
LOT CODE	Defined and inserted during fabrication

(table continues...)

Table 5 (continued) Marking table for PG-USON-10-2,-4 packages

Indicator	Description
ZZ	Indicates the Certifying Authority Serial Number / SKU#, for example, "00" would mean "SKU#00"
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"
12345	Convention: T&#$@ where: • The letter "T" indicates the OPTIGA™ Trust family • & indicates the product is a Trust M controller • # indicates the controller is a STR (S) variant • $ specifies the OPTIGA™ Trust M release version number • @ specifies the software version Example: "TMS10" means 'OPTIGA™ Trust M', 'STR variant', 'release version 1', 'software version 0'

The contacts and their functionality are given in the Table 6 below.

Table 6 Contact definitions and functions of PG-USON-10-2,-4 packages

Pin	Type	Function
01	GND	Supply voltage (Ground)
02	NC	Not connected/Do not connect externally. Shall be left floating
03	I/O	Serial Data Line (SDA)
04	NC	Not connected/Do not connect externally. Shall be left floating
05	NC	Not connected/Do not connect externally. Shall be left floating
06	NC	Not connected/Do not connect externally. Shall be left floating
07	NC	Not connected/Do not connect externally. Shall be left floating
08	I/O	Serial Clock Line (SCL)
09	IN	Active Low Reset (RST). This pin has a weak internal pull-up resistor
10	PWR	Supply voltage (V_{CC})

5 Technical data

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

5.1 I2C interface characteristics

Table 7 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

5.1.1 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 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	–	0.3 * 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 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	–	0.3 * 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)]	–	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}

5.1.2 I2C fast mode plus interface characteristics

For operation of the I2C interface, the electrical characteristics are compliant with the I²C 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 10 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}

5.1.3 Electrical characteristics

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

5.1.3.1 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 11 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}	–	70	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	I_{IL} = −50 µA to +20 µA
RST input high voltage	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.3	V	I_{IL} = −50 µA to +20 µA
Hibernate current	–	–	< 2.5	–	µA	V_{cc} = 0 V, GND = 0 V, RST = 0 V, SCL= 3.3 V and SCL = 3.3 V

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

5.1.3.2 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.
The V_{CC} ramp is depicted in Figure 9. 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.

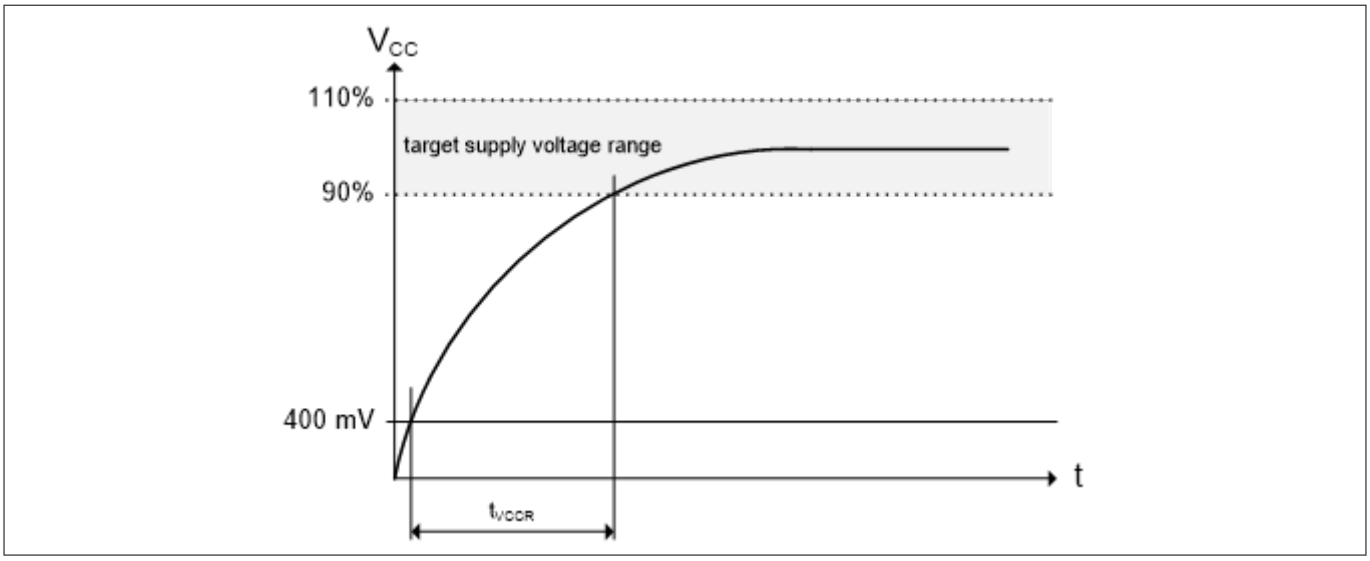


Figure 9 **V_{cc} rampup**

Table 12 **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

5.1.4 Startup of I2C interface

There are two variants possible for performing the startup procedure:

- Startup after power-on
- Startup for warm resets

5.1.4.1 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.

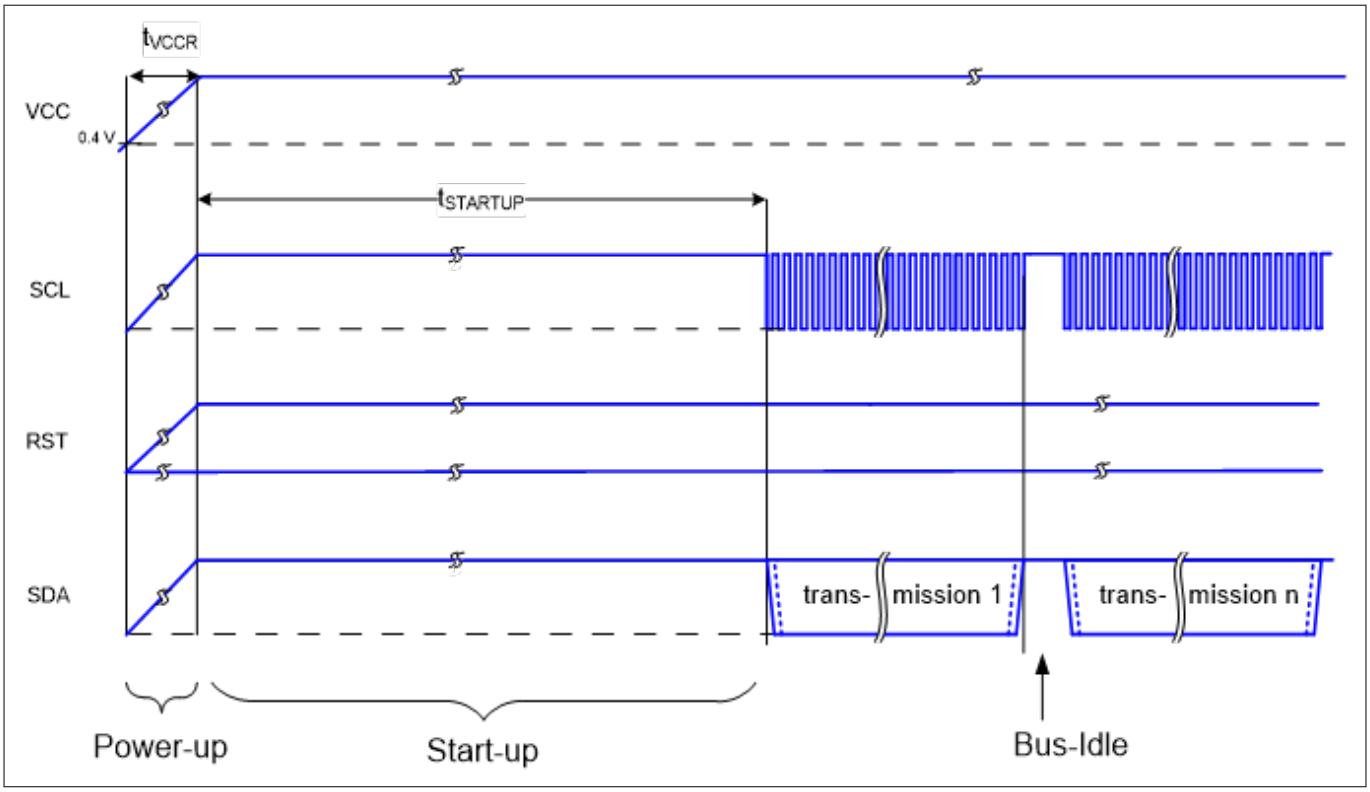


Figure 10 Startup of I2C interface after power-on

Table 13 Startup of I2C interface after power-on

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Startup time	$t_{STARTUP}$	15	–	–	ms	

5.1.4.2 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 t_1. At the latest t_2 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.

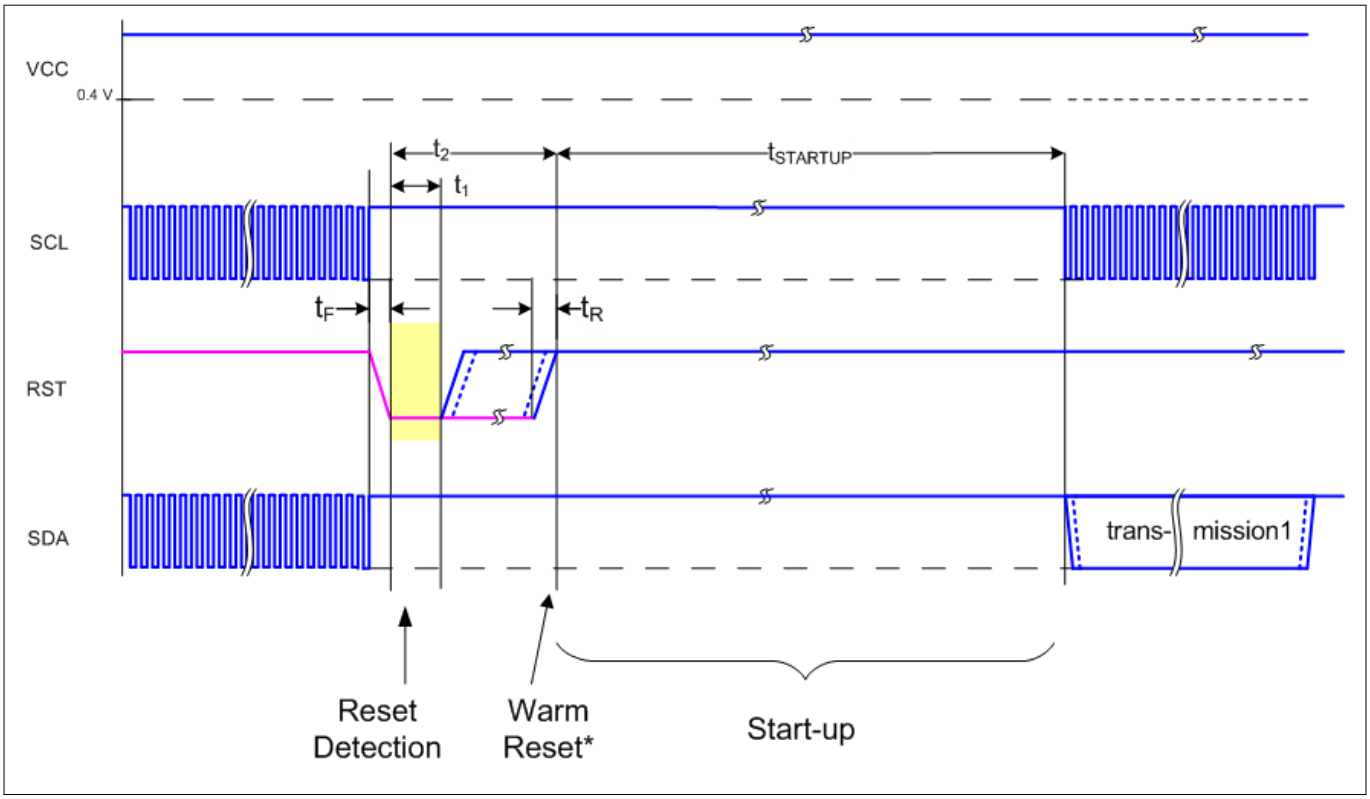


Figure 11 Startup of I2C interface for warm resets

***Note**: If NVM programming was requested prior to the reset, $t_{STARTUP}$ will be extended from a typical value of 15 ms to a maximum of 20 ms.*

Table 14 Startup of I2C interface for warm resets[1)]

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Startup time	$t_{STARTUP}$	15	–	–	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		10	–	2500	µs	

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

6 OPTIGA™ Trust M external interface

6.1 Commands

This section provides short description of the commands exposed by the OPTIGA™ Trust M security chip and mapping of these commands w.r.t Use Cases.

Table 15 Command table

Command Name	Description	V1	V3
OpenApplication	Command to launch an application	x	x
CloseApplication	Command to close/hibernate an application	x	x
GetDataObject	Command to get (read) a data object	x	x
SetDataObject	Command to set (write) a data object	x	x
SetObjectProtected	Command to set (write) data protected (integrity protection)	x	x
SetObjectProtected	Command to set (write) data/key objects and its metadata protected (integrity protection, confidentiality)		x
GetRandom	Command to generate a random stream	x	x
CalcHash	Command to calculate a Hash	x	x
CalcSign	Command to calculate a signature	x	x
VerifySign	Command to verify a signature	x	x
CalcSSec	Command to execute a Diffie-Hellmann key agreement	x	x
DeriveKey	Command to derive keys	x	x
GenKeyPair	Command to generate public/private key pairs	x	x
EncryptAsym	Command to encrypt (Asymmetric) a message	x	x
DecryptAsym	Command to decrypt (Asymmetric) a message	x	x
EncryptSym	Command to encrypt (Symmetric) a message		x
DecryptSym	Command to decrypt (Symmetric) a message		x
GenSymKey	Command to generate a symmetric key		x

Table 16 Mapping of commands with Use cases

Use Case	OPTIGA™ Trust M commands used
Secured Communication with (D)TLS	GetRandom, CalcHash, CalcSign, VerifySign, CalcSSec, DeriveKey, GenKeyPair, EncryptAsym and DecryptAsym
Datastore (user memory ~ 4.5 kB)	GetDataObject and SetDataObject
Symmetric key attestation, Security Tokens	EncryptSym and DecryptSym[1)]
Secured Firmware Update	VerifySign and DeriveKey
Secured update of Trust Anchors and Keys[2)] on Security Chip	SetObjectProtected command

1) EncryptSym and DecryptSym is supported only in v3
2) Secured key update is supported only in v3

6.2 Crypto performance

The performance metrics for various schemes are provided by the Table 18 below. If not particularly mentioned, the performance is measured @ OPTIGA™ Trust M I/O interface with:

- I2C FM (400KHz)
- Without power limitation
- @ 25°C
- VCC = 3.3V
- RSA® Signature scheme: RSA® SSA PKCS#1 v1.5 without hashing
- ECDSA Signature scheme: ECDSA FIPS 186-3 without hashing
- Encryption/Decryption scheme: RSAES PKCS#1 v1.5
- Hash scheme: SHA-256
- Key Derivation scheme: TLS v1.2 PRF SHA-256, HKDF SHA256
- RSA® Key size: 2048 bits
- ECC Key size: 256 bits (NIST P-256)
- AES Key size: 128 bits

Table 17 Crypto performance for V1

Scheme	Algorithm	Performance in ms[1)]	Performance with Shielded Connection in ms[1)]	Notes
Calculate signature	ECDSA	~ 60	~ 65	• ECC NIST P 256 • No data hashing
	RSA®	~ 310	~ 315	• 2048 bit exponentical • No data hashing
Verify signature	ECDSA	~ 85	~ 90	• ECC NIST P 256 provided by external world • No data hashing

(table continues...)

Table 17 (continued) Crypto performance for V1

Scheme	Algorithm	Performance in ms[1)]	Performance with Shielded Connection in ms[1)]	Notes
	RSA®	~ 45	~ 55	• 2048 bit exponentical provided by external world • No data hashing
Diffie-Hellman key agreement	ECC	~ 60	~ 65	Based on ephemeral key pair
Key pair generation	ECC	~ 75	~ 80	Generate 256 bit ECC key pair
	RSA®	~ 2900[2)]	~ 2910	Generate 2048 bit RSA® key pair
Encryption	RSA®	~ 30	~ 45	Encrypt 127 bytes
Decryption	RSA®	~ 310	~ 320	Decrypt 127 bytes
Key derivation	PRF as per TLS v1.2	~ 50	~ 55	• To derive a key of 40 bytes • Shared secret (32 bytes) from session context and • The input key derivation data size is 48 bytes
Hash calculation	SHA-256	~ 12 Kbyte/s	~ 11 Kbyte/s	In blocks of 1280 bytes

1) Minimum Execution of the entire sequence in milli seconds, except the External World timings
2) RSA® key pair generation performance is not predictable and typically have a variation in performance. This could be significantly higher or lower as the one specified in the table which is an average value over collected samples.

Table 18 Crypto performance for V3

Scheme	Algorithm	Performance in ms[1)]	Performance with Shielded Connection in ms[1)]	Notes
Calculate signature	ECDSA	~ 65	~ 70	• ECC NIST P 256 • No data hashing
	RSA®	~ 310	~ 320	• 2048 bit exponentical • No data hashing
Verify signature	ECDSA	~ 85	~ 95	• ECC NIST P 256 provided by external world • No data hashing
	RSA®	~ 40	~ 50	• 2048 bit exponentical provided by external world • No data hashing
Diffie-Hellman key agreement	ECDH	~ 60	~ 65	Based on ephemeral key pair
Key pair generation	ECC	~ 55	~ 60	Generate 256 bit ECC key pair in session

(table continues...)

Table 18 (continued) Crypto performance for V3

Scheme	Algorithm	Performance in ms[1)]	Performance with Shielded Connection in ms[1)]	Notes
	RSA®	~ 2900[2)]	~ 2910	Generate 2048 bit RSA® key pair
Encryption	RSA®	~ 40	~ 50	Encrypt 127 bytes
Decryption	RSA®	~ 315	~ 325	Decrypt 127 bytes
Encryption	AES-128	~ 28	~ 35	Encrypt 256 bytes, ECB mode
Decryption	AES-128	~ 35	~ 42	Decrypt 256 bytes, ECB mode
Key derivation	PRF as per TLS v1.2	~ 50	~ 55	• To derive a key of 40 bytes • Shared secret (32 bytes) from session context and • The input key derivation data size is 48 bytes
Key derivation	HKDF with SHA-256	~ 130	~ 135	Using a pre-shared secret from a data object
HMAC	HMAC with SHA-256	~ 90	~ 95	Using a pre-shared secret from a data object and 128 bytes of input data
Hash calculation	SHA-256	~ 15 Kbyte/s	~ 14 Kbyte/s	In blocks of 1280 bytes

1) Minimum Execution of the entire sequence in milli seconds, except the External World timings
2) RSA® key pair generation performance is not predictable and typically have a variation in performance. This could be significantly higher or lower as the one specified in the table which is an average value over collected samples.

7 Security monitor

The security monitor is a central component which enforces the security policy of the OPTIGA™ Trust M. It processes internal security events and takes actions accordingly as specified in security policy below.

7.1 Security events

The events below actively influence the security monitor.

Table 19 Security events

Event	Description
Decryption failure	This event indicates a case of a decryption and/or integrity check of provided data leading to a failure during protected update
Key derivation	This event indicates a case of the DeriveKey command getting applied on a persistent data object (not volatile data object as session context). In that case the persistent data object gets used as pre-shared secret
Private key use	This event indicates a case of internal services going to use an OPTIGA™ Trust M hosted private key, except temporary keys from the session context are used
Secret key use	This event indicates a case of internal services going to use a OPTIGA™ hosted secret (symmetric) key (once per respective command), except temporary keys from session context are used
Suspect system behavior	This event indicates a case of the embedded software detecting inconsistencies with the expected behavior of the system. Those inconsistencies might be redundant information which does not fit to their counterpart

7.2 Security policy

The security monitor judges the notified security events regarding the number of occurrence over time and in case those violate the permitted usage profile of the system takes actions to throttle down the performance and thus the possible frequency of attacks.

The permitted usage profile is defined as:

1. t_{max} is set to 5 seconds (± 5%)
2. A Suspect System Behavior event is never permitted and will cause setting the Security Event Counter (SEC) to its maximum (= 255)
3. One protected operation (refer to Table 19) events per t_{max} period

In other words it must not allow more than one out of the protected operations per t_{max} period (worst case, ref to bullet 3. above). This condition must be stable, at least after 500 uninterrupted executions of protected operations.

For more information, refer to Solution Reference Manual document available as part of the package.

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 (for example, 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, for example, 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.

Figure 12 RoHS Compliance

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.

A Appendix

A.1 Infineon I2C protocol registry map

OPTIGA™ Trust M supports IFX I2C v2.03 protocol and is implemented as I2C slave, which uses different address locations for status, control and data communication registers. These registers with description are outlined below in the following table.

Table 20 IFX I2C registry map table

Register address	Name	Size in Bytes	Description	Master access
0x80	DATA	DATA_REG_LEN	This is the location where data shall be read from or written to the I2C slave	Read/ Write
0x81	DATA_REG_LEN	2	This register holds the maximum data register (Addr 0x80) length. The allowed values are 0x0010 up to 0xFFFF. After writing the new data register length it becomes effective with the next I2C master access. However, in case the slave could not accept the new length it indicates its maximum possible length within this register. Therefore it is recommended to read the value back after writing it to be sure the I2C slave did accept the new value Note: the value of MAX_PACKET_SIZE is derived from this value or vice versa (MAX_PACKET_SIZE= DATA_REG_LEN-5)	Read/ Write
0x82	I2C_STATE	4	Bits 31:24 of this register provides the I2C state in regards to the supported features (for example, clock stretching …) and whether the device is busy executing a command and/or ready to return a response etc Bits 15:0 defining the length of the response data block at the physical layer	Read only
0x83	BASE_ADDR	2	This register holds the I2C base address as specified by Table 21. Default value is 0x30. After writing a different address the new address become effective with the next I2C master access. In case the bit 15 is set in addition to the new address (bit 6:0) it becomes the new default address at reset (persistent storage)	Write only

(table continues...)

Table 20 (continued) IFX I2C registry map table

Register address	Name	Size in Bytes	Description	Master access
0x84	MAX_SCL_FREQU	4	This register holds the maximum clock frequency in KHz supported by the I2C slave. The value gets adjusted to the register I2C_Mode setting Fast Mode (Fm): The allowed values are 50 up to 400 KHz Fast Mode (Fm+): The allowed values are 50 up to 1000 KHz	Read
0x85	GUARD_TIME[1)]	4	For details refer to Table 24	Read only
0x86	TRANS_TIMEOUT	4	For details refer to Table 24	Read only
0x88	SOFT_RESET	2	Writing to this register will cause a device reset. This feature is optional	Write only
0x89	I2C_MODE	2	This register holds the current I2C Mode as defined by Table 22. The default mode is SM & FM (011B)	Read/ Write

1) In case the register returns 0xFFFFFFFF the register is not supported and the default values specified in Table 'List of protocol variations' shall be applied.

Table 21 Definition of BASE_ADDR

Fields	Bits	Value	Description
DEF_ADDR	15	0 1	Volatile address setting by bit 6:0, lost after reset Persistent address setting by bit 6:0, becoming default after reset
BASE_ADDR	6:0	0x00-0x7F	I^2C base address specified by Table 20

15	14	13	12	11	10	9	8
DEF_ADDR	RFU						
7	6	5	4	3	2	1	0
RFU	BASE_ADDR						

15	14	13	12	11	10	9	8
DEF_MODE	RFU						
7	6	5	4	3	2	1	0
RFU					Mode		

Table 22 Definition of I2C_MODE

Fields	Bits	Value	Description
DEF_MODE	15	0 1	Volatile mode setting by bit 2:0, lost after reset Persistent mode setting by bit 2:0, becoming default after reset. This bit is always read as 0
MODE[1)]	2:0	001 010 011 100 other values	Sm Fm SM & Fm (fab out default) Fm+ not valid; writing will be ignored

1) This mode defines the adherence of the bus signals to the electrical characteristics according standard I2C bus specification

31	30	29	28	27	26	25	24
BUSY	RESP_RDY	RFU		SOFT_RESET	CONT_READ	REP_START	CLK_STRETCHING
23	22	21	20	19	18	17	16
PRESENT_LAYER	RFU						
15-0							
Length of data block to be read							

Table 23 Definition of I2C_STATE

Field	Bit(s)	Value	Description
BUSY	31	0 1	Device is not busy Device is busy executing a command
RESP_RDY	30	0 1	Device is not ready to return a response Device is ready to return a response
SOFT_RESET	27	0 1	SOFT_RESET not supported SOFT_RESET supported
CONT_READ	26	0 1	Continue Read not supported Continue Read supported
REP_START	25	0 1	Repeated start not supported Repeated start supported
CLK_STRETCHING	24	0 1	Clock stretching not supported Clock stretching supported
PRESENT_LAYER	23	0 1	Presentation Layer not supported Presentation Layer supported

A.1.1 Infineon I2C protocol variations

To fit best to application specific requirements the protocol might be tailored by specifying a couple of parameters which is described in the following table.

Table 24 List of protocol variations

Parameter	Default value	Description
MAX_PACKET_SIZE	0x110	Maximum packet size accepted by the receiver. The protocol limits this value to 0xFFFF, but there might be project specific requirements to reduce the transport buffers size for the sake of less RAM footprint in the communication stack. If shortened, it could be statically defined or negotiated at the physical layer
WIN_SIZE	1	Window size of the sliding windows algorithm. The value could be 1 up to 2
MAX_NET_CHAN	1	Maximum number of network channels. The value could be 1 up to 16. One indicates the OSI Layer 3 is not used and the CHAN field of the PCTR must be set to 0000
CHAINING	TRUE	Chaining on the transport layer is supported (TRUE) or not (FALSE)
TRANS_TIMEOUT	10 ms	(Re) transmission timeout specifies the number of milliseconds to be elapsed until the transmitter considers a frame transmission is lost and retransmits the non-acknowledged frame. The Timer gets started as soon as the complete frame is transmitted. The value could be 1 up to 1000. However, the higher the number, the longer it takes to recover from a frame transmission error *Note: The acknowledge timeout on the receiver side must be shorter than the retransmission timeout to avoid unnecessary frame repetitions.*
TRANS_REPEAT	3	Number of transmissions to be repeated until the transmitter considers the connection is lost and starts a re-synchronization with the receiver. The value could be 1 up to 4
BASE_ADDR	0x30	I2C (base) address. This address could be statically defined or dynamically negotiated by the physical layer
MAX_SCL_FREQU	1000 kHz	Maximum SCL clock frequency in kHz
GUARD_TIME	50 µs	Minimum time to be elapsed at the I2C master measured from read data (STOP condition) until the next write data (Start condition) is allowed to happen. ***Notes**:* ***1.*** *For two consecutive accesses on the same device GUARD_TIME re-specifies the value of t_{BUF} as specified by [I2Cbus]* ***2.*** *Even if another I2C address is accessed in between GUARD_TIME has to be respected for two consecutive accesses on the same device*

(table continues...)

Table 24 (continued) List of protocol variations

Parameter	Default value	Description
SOFT_RESET	1	Any write attempt to the SOFT_RESET register will trigger a warm reset (reset w/o power cycle). This register is optional and its presence is indicated by the I2C_STATE register's "SOFT_RESET" flag
PRESENT_LAYER	1	This flag at the I2C_STATE register indicates the optional availability of the presentation layer, which is providing confidentiality and integrity protection of payloads (APDUs) transferred across the I2C interface. The presentation layer is used as part of Shielded Connection

A.2 OPTIGA™ Trust M command/response I2C sample logs

The default I2C slave address for the OPTIGA™ Trust M is 0x30 [I2C_ADDR]. All the values in this section are specified in decimal form unless stated otherwise.

A.2.1 Sequence of commands to read coprocessor UID from OPTIGA™ Trust M

Pre-requisites

1. Ensure that the security device is powered up
2. The OPTIGA™ Trust M will not acknowledge the slave address sent by a host if it is either busy or in idle state. Hence the host must retry or repeat the transaction until it is successful or timed out for 100 milliseconds (extreme case)
3. The specified guard time must be applied between each attempt of write / read operation by the Host I2C driver
4. The log information for OPTIGA™ Trust M commands specified in below Tables contains the [IFX I2C] protocol information which comprises sequence numbers and checksum of the transactions
   a. A sequence of commands must be strict for the OPTIGA™ Trust M (for example, OpenApplication followed by GetDataObject to read a Coprocessor UID)
   b. A checksum in the data depends on the data received or sent via write/read operations. So any data change in the transaction is reflected in the check sum. Otherwise the write data transaction will not be accepted/acknowledged by the OPTIGA™ Trust M
5. The logs specified below are without the presentation layer (used for the Shielded Connection) of [IFX I2C]

A.2.1.1 Check the status [I2C_STATE]

This is a very basic register read operation which ensures the behavior of the read/write operations of the local host I2C driver.

Table 25 Check I2C_STATE Register of OPTIGA™ Trust M

I2C_ADDR	Transaction Type	Data [values in hexadecimal]
30	Write [01 Bytes]	82
30	Read [04 Bytes]	08 80 00 00

A.2.1.2 Issue OpenApplication command

Before issuing any application specific command; for example, read Coprocessor UID using GetDataObject, it is a must to send the OpenApplication command to initialize the application on the OPTIGA™ Trust M as shown below.

Table 26 OpenApplication on OPTIGA™ Trust M

I2C_ADDR	Transaction Type	Data [values in hexadecimal]
Step 1: Send OpenApplication command to initiate the application context on the OPTIGA™ Trust M		
30	Write [27 Bytes]	80 03 00 15 00 **70 00 00 10 D2 76 00 00 04 47 65 6E 41 75 74 68 41 70 70 6C** 04 1A
Step 2: Read the I2C_STATE register [*Repeat this step until the read contains the data as specified below*]		
30	Write [01 Bytes]	82
30	Read [04 Bytes]	C8 80 00 05
Step 3: Read the DATA register [*Acknowledgment from* OPTIGA™ Trust M *for the last data transaction*]		
30	Write [01 Bytes]	80
30	Read [05 Bytes]	80 00 00 0C EC
Step 4: Read the I2C_STATE register [*Repeat this step until the read contains the data as specified below*]		
30	Write [01 Bytes]	82
30	Read [04 Bytes]	48 80 00 0A
Step 5: Read the DATA register which contains the response for the command issued		
30	Write [01 Bytes]	80
30	Read [10 Bytes]	00 00 05 00 **00 00 00 00** 14 87
Step 6: Send an acknowlegment for the data read		
30	Write [06 Bytes]	80 80 00 00 0C EC

A.2.1.3 Read coprocessor UID

The coprocessor UID contains the OPTIGA™ Trust M unique ID and the build information details. The GetDataObject command is used to read the coprocessor UID information.

Table 27 Read Coprocessor UID

I2C_ADDR	Transaction Type	Data [values in hexadecimal]
Step 1: Send the GetDataObject command to read the Coprocessor UID		
30	Write [17 Bytes]	80 04 00 0B 00 **01 00 00 06 E0 C2 00 00 00 64** F0 9F
Step 2: Read the I2C_STATE register [*Repeat this step until the read contains the data as specified below*].		
30	Write [01 Bytes]	82
30	Read [04 Bytes]	48 80 00 25
Step 3: Read the DATA register which contains the response for the command issued		
30	Write [01 Bytes]	80

(table continues...)

Table 27 (continued) Read Coprocessor UID

I2C_ADDR	Transaction Type	Data [values in hexadecimal]
30	Read [37 Bytes]	05 00 20 00 **00 00 00 1B CD XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX YY YY** ZZ ZZ ***Notes:*** ***1.*** *XX is the unique ID part of the co-processor UID* ***2.*** *"YY YY" is the OPTIGA™ Trust M build number in BCD (Binary Coded Decimal) format* ***3.*** *ZZ ZZ is the checksum of the transaction*
Step 4: Send an acknowlegment for the data read		
30	Write [06 Bytes]	80 81 00 00 56 30

A.3 Power management

When operating, the power consumption of OPTIGA™ Trust M is limited to meet the requirements regarding the power limitation set by the Host. The power limitation is implemented by utilizing the current limitation feature of the underlying hardware device in steps of 1 mA from 6 mA to 15 mA with a precision of ±5%.

A.3.1 Hibernation

This maximizes power saving (zero power consumption [2]), while the I2C bus stays connected. In this case OPTIGA™ Trust M saves the application context before power-off (switching off V_{CC}) and restores it after power-up. After power-up the application continues seamlessly from the state before hibernate.

A.3.1.1 Software adaption for hibernate circuit with single MOSFET

Update the *ifx_i2c.c* file functions with the following change:

[2] Leakage current < 2.5µA only

1. Call ***pal_gpio_set_low*** *(p_ifx_i2c_context->p_slave_vdd_pin)*, to set the Vdd pin to High,
2. Call ***pal_gpio_set_high*** *(p_ifx_i2c_context->p_slave_vdd_pin)*, to set the Vdd pin to Low

```
_STATIC_H optiga_lib_status_t ifx_i2c_init
                        (ifx_i2c_context_t * p_ifx_i2c_context)
{
    optiga_lib_status_t api_status = IFX_I2C_STACK_ERROR;

    if (((uint8_t)IFX_I2C_WARM_RESET ==
                    p_ifx_i2c_context->reset_type) ||
        ((uint8_t)IFX_I2C_COLD_RESET ==
                    p_ifx_i2c_context->reset_type))
     {
         switch (p_ifx_i2c_context->reset_state)
         {
             case IFX_I2C_STATE_RESET_PIN_LOW:
             {
                 // Setting the Vdd & Reset pin to low
                 if ((uint8_t)IFX_I2C_COLD_RESET ==
                      p_ifx_i2c_context->reset_type)
                 {
                  // Set the Host GPIO as high to set Vdd to low
                     pal_gpio_set_high
                      (p_ifx_i2c_context->p_slave_vdd_pin);
                 }
                 // Setting the Reset pin to low
                 pal_gpio_set_low
                      (p_ifx_i2c_context->p_slave_reset_pin);
                 p_ifx_i2c_context->reset_state =
                       IFX_I2C_STATE_RESET_PIN_HIGH;
                 pal_os_event_register_callback_oneshot
                        (p_ifx_i2c_context->pal_os_event_ctx,
                        (register_callback)ifx_i2c_init,
                        (void * )p_ifx_i2c_context,
                        RESET_LOW_TIME_MSEC);
                 api_status = IFX_I2C_STACK_SUCCESS;
                 break;
             }
             case IFX_I2C_STATE_RESET_PIN_HIGH:
             {
                 // Setting the Vdd & Reset pin to high
                 if ((uint8_t)IFX_I2C_COLD_RESET ==
                      p_ifx_i2c_context->reset_type)
                 {
                  // Set the Host GPIO as low to set Vdd to high
                     pal_gpio_set_low
                        (p_ifx_i2c_context->p_slave_vdd_pin);
                 }
                 // Setting the Reset pin to high
                 pal_gpio_set_high
                        (p_ifx_i2c_context->p_slave_reset_pin);
                 p_ifx_i2c_context->reset_state =
                         IFX_I2C_STATE_RESET_INIT;
```

```
51                  pal_os_event_register_callback_oneshot
52                          (p_ifx_i2c_context->pal_os_event_ctx,
53                          (register_callback)ifx_i2c_init,
54                          (void * )p_ifx_i2c_context,
55                          STARTUP_TIME_MSEC);
56                  api_status = IFX_I2C_STACK_SUCCESS;
57                  break;
58              }
59              case IFX_I2C_STATE_RESET_INIT:
60              {
61                  //Frequency and frame size negotiation
62      #ifndef OPTIGA_COMMS_SHIELDED_CONNECTION
63                  api_status = ifx_i2c_tl_init
64                         (p_ifx_i2c_context,
65                                     ifx_i2c_tl_event_handler);
66      #else
67                  api_status = ifx_i2c_prl_init
68                       (p_ifx_i2c_context,
69                                     ifx_i2c_tl_event_handler);
70      #endif
71                  break;
72              }
73              default:
74                  break;
75          }
76      }
77      //soft reset
78      else
79      {
80          p_ifx_i2c_context->pl.request_soft_reset =
81                                                  (uint8_t)TRUE;
82      #ifndef OPTIGA_COMMS_SHIELDED_CONNECTION
83          api_status = ifx_i2c_tl_init(p_ifx_i2c_context,
84                                  ifx_i2c_tl_event_handler);
85      #else
86          api_status = ifx_i2c_prl_init(p_ifx_i2c_context,
87                                  ifx_i2c_tl_event_handler);
88      #endif
89      }
90      if (api_status != IFX_I2C_STACK_SUCCESS)
91      {
92          ifx_i2c_tl_event_handler(p_ifx_i2c_context, api_status,
93                                    0, 0);
94      }
95      return (api_status);
96  }
97  optiga_lib_status_t ifx_i2c_close(ifx_i2c_context_t * p_ctx)
98  {
99      optiga_lib_status_t api_status =
100                         (int32_t)IFX_I2C_STACK_ERROR;
101      // Proceed, if not busy and in idle state
102      if (IFX_I2C_STATUS_BUSY != p_ctx->status)
103      {
```

```
104             api_status = IFX_I2C_STACK_SUCCESS;
105
106         #ifdef OPTIGA_COMMS_SHIELDED_CONNECTION
107             p_ctx->close_state = IFX_I2C_STACK_ERROR;
108             p_ctx->state = IFX_I2C_STATE_UNINIT;
109                     api_status = ifx_i2c_prl_close
110                          (p_ctx, ifx_i2c_prl_close_event_handler);
111             if (IFX_I2C_STACK_ERROR == api_status)
112             {
113                 pal_i2c_deinit(p_ctx->p_pal_i2c_ctx);
114                 // Also power off the device
115                 // Set the Host GPIO as high to set Vdd to low
116                 pal_gpio_set_high(p_ctx->p_slave_vdd_pin);
117                 pal_gpio_set_low(p_ctx->p_slave_reset_pin);
118                 p_ctx->status = IFX_I2C_STATUS_NOT_BUSY;
119             }
120         #else
121             ifx_i2c_tl_event_handler
122                          (p_ctx, IFX_I2C_STACK_SUCCESS, NULL, 0);
123             // Close I2C master
124             pal_i2c_deinit(p_ctx->p_pal_i2c_ctx);
125             // Also power off the device
126             // Set the Host GPIO as high to set Vdd to low
127             pal_gpio_set_high(p_ctx->p_slave_vdd_pin);
128             pal_gpio_set_low(p_ctx->p_slave_reset_pin);
129             p_ctx->state = IFX_I2C_STATE_UNINIT;
130             p_ctx->status = IFX_I2C_STATUS_NOT_BUSY;
131         #endif
132         }
133         return (api_status);
134     }
135     _STATIC_H void ifx_i2c_prl_close_event_handler
136                               (ifx_i2c_context_t * p_ctx,
137                                optiga_lib_status_t event,
138                                const uint8_t * p_data,
139                                uint16_t data_len)
140     {
141         p_ctx->status = IFX_I2C_STATUS_NOT_BUSY;
142         switch (p_ctx->state)
143         {
144             case IFX_I2C_STATE_UNINIT:
145             {
146                 pal_i2c_deinit(p_ctx->p_pal_i2c_ctx);
147                 // Also power off the device
148                 // Set the Host GPIO as high to set Vdd to low
149                 pal_gpio_set_high(p_ctx->p_slave_vdd_pin);
150                 pal_gpio_set_low(p_ctx->p_slave_reset_pin);
151                 break;
152             }
153             default:
154                 break;
155         }
156
```

```
157         if (NULL != p_ctx->upper_layer_event_handler)
158         {
159             p_ctx->upper_layer_event_handler
160                         (p_ctx->p_upper_layer_ctx, event);
161         }
162     }
```

A.3.2 Low power sleep mode

The OPTIGA™ Trust M automatically enters a low-power mode after a configurable delay. Once it has entered Sleep mode, the OPTIGA™ Trust M resumes normal operation as soon as its address is detected on the I2C bus.

In case no command is sent to the OPTIGA™ Trust M it behaves as shown in Figure 13.

1. As soon as the OPTIGA™ Trust M is idle it starts to count down the “delay to sleep” time (t_{SDY})
2. In case this time elapses the device enters the “go to sleep” procedure
3. The “go to sleep” procedure waits until all idle tasks are finished (for example, counting down the SEC). In case all idle tasks are finished and no command is pending, the OPTIGA™ Trust M enters sleep mode

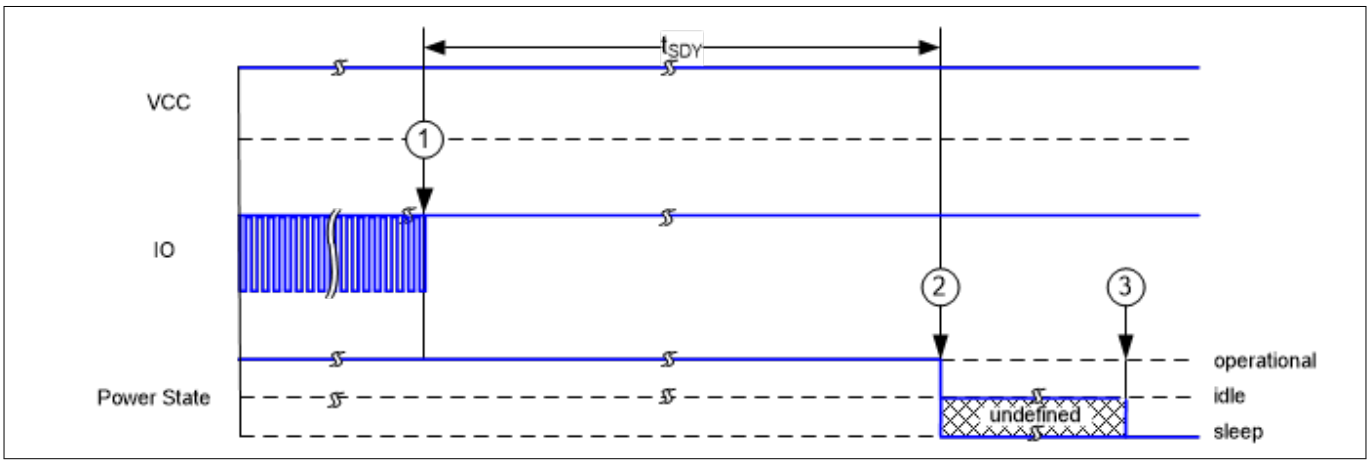


Figure 13 Go-to-sleep diagram

Glossary

AES

Advanced Encryption Standard (AES)

The standard for the encryption of electronic data established by the United States (U.S). National Institute of Standards and Technology (NIST) in 2001. The algorithm described by Advanced Encryption Standard (AES) is a symmetric-key algorithm (the same key is used for both encryption and decryption).

API

application programming interface (API)

A set of defined rules that enables various software components to communicate with each other.

CA

certificate authority (CA)

CBC

cipher block chaining (CBC)

CC

Common Criteria for Information Technology Security Evaluation (CC)

An international standard (International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408) for computer security certification.

CMAC

cipher-based MAC (CMAC)

DRNG

deterministic random number generator (DRNG)

DTLS

datagram transport layer security (DTLS)

EAL

evaluation assurance level (EAL)

ECB

electronic code book (ECB)

ECC

elliptic curve cryptography (ECC)

ECDH

elliptic curve Diffie-Hellman (ECDH)

A key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel.

ECDSA

elliptic curve digital signature algorithm (ECDSA)

ETR

extended temperature range (ETR)

HMAC
hash-based message authentication code (HMAC)

I2C
inter-integrated circuit (I2C)
A synchronous serial communication bus.

IETF
Internet Engineering Task Force (IETF)

IFX
Infineon Technologies AG (IFX)
The stock market acronym for Infineon Technologies AG shares. It is sometimes used in diagrams or tables where the long term hinders readability.

IoT
Internet of Things (IoT)

IP
intellectual property (IP)

NIST
National Institute of Standards and Technology (NIST)

OS
operating system (OS)

PAL
platform abstraction layer (PAL)

PKI
public key infrastructure (PKI)
A set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

RFC
request for comments (RFC)

SHA
Secure Hash Algorithm (SHA)

SKU
stockkeeping unit (SKU)

STR
standard temperature range (STR)

TLS
transport layer security (TLS)
Security protocol designed to facilitate privacy and data security for communications over the Internet.

TRNG

true random number generator (TRNG)

USB

universal serial bus (USB)

An industry standard that defines cables, connectors, and communication protocols used in a bus for connection, communication, and power supply between computers and electronic devices.

Revision history

Document version	Date of release	Description of changes
3.70	2024-10-09	Updated the features Editorial changes
3.61	2024-01-12	Fixed typography
3.60 (Internal review)	2023-12-20	Minor changes
3.50 (Internal review)	2023-12-04	Added OPTIGA™ Trust M MTR configurations Update block diagram on Figure 1 Update pin descriptions on Table 6
3.40	2022-06-21	Section 1.5 updated, Section 6 removed
3.30	2021-08-17	Section 6.4, 6.5 and 12 updated for pal_ifx_i2c_context structure changes and ifx_i2c_init bug fix
3.20	2020-10-20	Fixed internal review comments and released for Production
3.15	2020-10-12	Section 3.1 Hibernate circuit diagram updated for single MOSFET option and direct GPIO as power option
3.10	2020-09-24	Release to Production release
3.00	2020-06-29	Fixed internal review comments
0.70	2020-05-27	Initial version update for ES Release

Trademarks

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

Edition 2024-10-09

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about any aspect of this document?

Email:
CSSCustomerService@infineon.com

Document reference
IFX-idj1698135223684

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.

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.