

# OPTIGA™ Trust M

## Product Version: V1

### Key Features

- High-end security controller
- Common Criteria Certified EAL6+ (high) hardware
- Turnkey solution
- Up to 10kB user memory
- PG-USON-10-2 package (3 x 3 mm)
- Standard & Extended temperature ranges
- I2C interface with Shielded Connection (encrypted communication)
- Cryptographic support: ECC NIST P256/P384, SHA-256, TRNG, DRNG, RSA® 1024/2048
- OPTIGA™ Trust M Software Framework on Github (<https://github.com/Infineon/optiga-trust-m>)
- Crypto ToolBox commands for SHA-256, ECC NIST P256/P384 (sign, verify, key generation, and ECDH(E)), RSA® 1024/2048 (sign, verify, key generation, encrypt and decrypt) and key derivation (TLS v1.2 PRF)
- Device Security Monitor
- 4 Monotonic up counters
- Hibernate for zero power consumption<sup>1</sup>
- Lifetime for Industrial Automation and Infrastructure is 20 years and 15 years for other Application Profiles



### Benefits

- 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 and 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.

---

<sup>1</sup> Leakage current < 2.5µA only

## Table of Contents

### Table of Contents

<b>About this document.....</b>	<b>1</b>
<b>1 Introduction .....</b>	<b>4</b>
1.1 Broad range of benefits.....	4
1.2 Enhanced security.....	4
1.3 Fast and easy integration.....	4
1.4 Applications.....	4
1.5 Device Features .....	4
<b>2 System Block Diagram .....</b>	<b>7</b>
<b>3 Interface and Schematics .....</b>	<b>9</b>
3.1 System Integration Schematics.....	9
3.2 System Integration Schematics with Hibernation support.....	9
<b>4 Description of packages .....</b>	<b>10</b>
4.1 PG-USON-10-2 .....	10
4.2 Production sample marking pattern .....	11
<b>5 Technical Data .....</b>	<b>13</b>
5.1 I2C Interface Characteristics.....	13
5.1.1 I2C Standard/Fast Mode Interface Characteristics.....	13
5.1.2 I2C Fast Mode Plus Interface Characteristics.....	14
5.1.3 Electrical Characteristics .....	15
5.1.3.1 DC Electrical Characteristics.....	15
5.1.3.2 AC Electrical Characteristics.....	15
5.1.4 Start-Up of I2C Interface .....	16
5.1.4.1 Startup after Power-On .....	16
5.1.4.2 Startup for Warm Resets.....	17
<b>6 Connecting to Host.....</b>	<b>19</b>
6.1 OPTIGA™ Trust M Host Software Architecture .....	19
6.2 Release Package Folder Structure.....	19
6.3 Porting Notes.....	21
6.4 Communication with OPTIGA™ Trust M .....	21
6.5 Reference code on XMC4800 for communicating with OPTIGA™ Trust M.....	23
<b>7 OPTIGA™ Trust M External Interface .....</b>	<b>26</b>
7.1 Commands .....	26
7.2 Crypto Performance.....	26
<b>8 Security Monitor .....</b>	<b>28</b>
8.1 Security Events.....	28
8.2 Security Policy.....	28
<b>9 RoHS Compliance .....</b>	<b>29</b>
<b>10 Appendix A – Infineon I2C Protocol Registry Map .....</b>	<b>30</b>
10.1 Infineon I2C Protocol Variations.....	32
<b>11 Appendix B - OPTIGA™ Trust M Command/Response I2C Sample Logs .....</b>	<b>34</b>
11.1 Sequence of commands to read Coprocessor UID from OPTIGA™ Trust M .....	34
11.1.1 Check the status [I2C_STATE].....	34
11.1.2 Issue OpenApplication command .....	34
11.1.3 Read Coprocessor UID .....	35
<b>12 Appendix C – Power Management .....</b>	<b>36</b>



**Table of Contents**

12.1 Hibernation..... 36  
12.2 Low Power Sleep Mode ..... 36  
**Revision history..... 38**

## Introduction

### 1 Introduction

As embedded systems (e.g. 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 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.

#### 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 proof NVM for secure storage and Symmetric/Asymmetric crypto engines to support ECC 256/384, RSA® 1024/2048 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 footprint 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:

- a) Network node protection using Mutual Authentication such as TLS or DTLS
- b) Protect the Authenticity, Integrity and Confidentiality of your product, data and IP
- c) Secure Communication
- d) Datastore Protection
- e) Lifecycle Management
- f) Platform Integrity Protection
- g) Secure Updates

#### 1.5 Device Features

The OPTIGA™ Trust M comes with up to 10kB user memory that can be used to store X.509 certificates and data. OPTIGA™ Trust M is based on Common Criteria (CC) Certified EAL6+ (high) hardware enabling it to prevent physical attacks on the device itself and providing high assurance that the keys or arbitrary data stored cannot be accessed by an unauthorized entity. The CC certificate can be found at [www.bsi.bund.de](http://www.bsi.bund.de) by searching for BSI-DSZ-CC-0961-V2-2018 (Hardware Identifier IFX\_CCI\_00000Bh). OPTIGA™ Trust M supports a highspeed I2C communication interface of up to 1MHz (FM+).

## Introduction

**Table 1 Products**

Type	Description	Temperature range	Package
OPTIGA™ Trust M SLS 32AIA010MH	Embedded security solution for connected devices	–40°C to +105°C Extended Temperature Range (ETR)	PG-USON-10-2
OPTIGA™ Trust M SLS 32AIA010MS	Embedded security solution for connected devices	–25°C to +85°C Standard Temperature Range (STR)	PG-USON-10-2
Evaluation Kit	Includes a host micro controller XMC4800 IoT Connectivity Kit connected to the OPTIGA™ Trust M to connect to the outside world, enabling you to evaluate the OPTIGA™ Trust M features and start the Design-In activities.		Board

Infineon and its distribution partners offer a wide range of customization options (e.g. X.509 certificate generation and key provisioning) for the security chip.

**Table 2 Abbreviations**

Abbreviation	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certification Authority
CC	Common Criteria
DRNG	Deterministic Random Number Generator
DTLS	Datagram Transport Layer Security
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ETR	Extended Temperature Range
I2C	Inter-Integrated Circuit
IETF	Internet Engineering Task Force
IFX	Infineon
IOT	Internet of Things
IP	Intellectual Property
NIST	National Institute of Standards and Technology
OS	Operating System
PAL	Platform Abstraction Layer
PKI	Public Key Infrastructure
RFC	Request For Comments
SHA	Secure Hash Algorithm
SKU	Stock Keeping Unit
STR	Standard Temperature Range

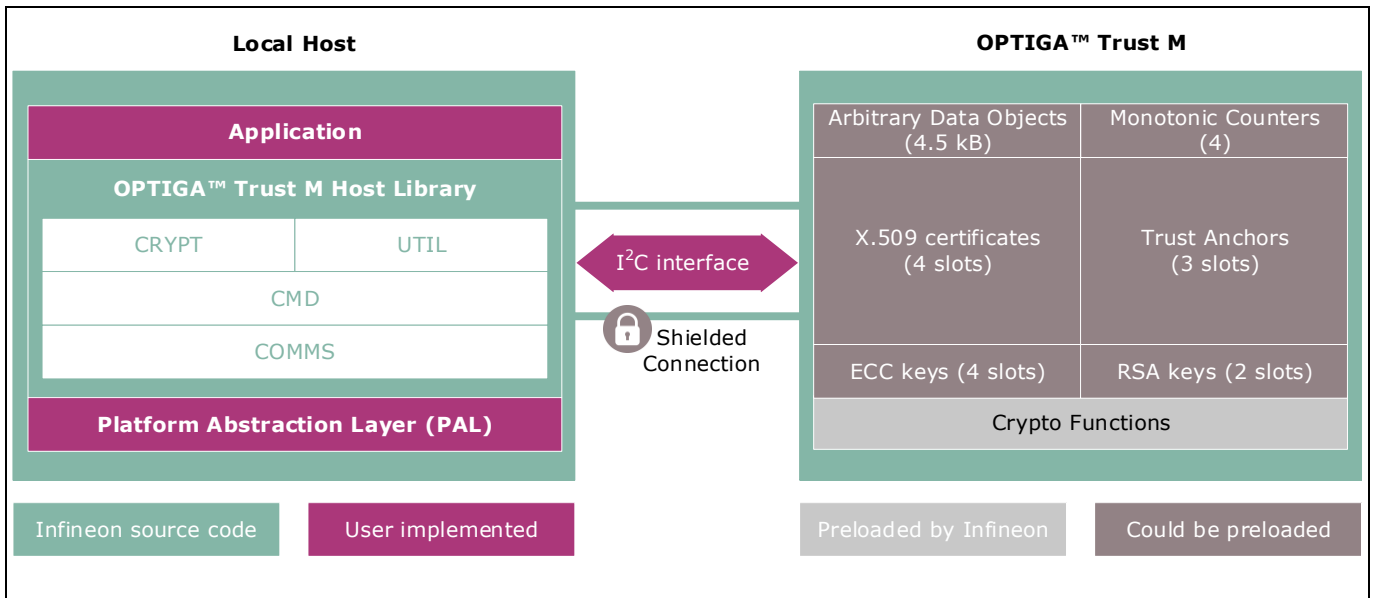
**Introduction**

<b>Abbreviation</b>	<b>Definition</b>
TLS	Transport Layer Security
TRNG	True Random Number Generator
USB	Universal Synchronous Bus

## System Block Diagram

### 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 3<sup>rd</sup> party Crypto Library to offload crypto operations to OPTIGA™ Trust M.
  - UTIL – Provides APIs such as read/write, protected update of data objects and open/close application (e.g. Hibernate)
  - CMD – Provides APIs to send and receive commands (Section 7) 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 (e.g. I2C, Timer, GPIO, platform crypto library etc.)

#### 2. OPTIGA™ Trust M

- Arbitrary Data Objects – The target application can store up to 4.5kB (~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.

---

**System Block Diagram**

- X.509 – Up to 4 X.509 based Certificates can be stored
- Keys – Up to 4 ECC and 2 RSA based keys 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

*Note: Unique ECC/RSA private keys and X.509 Certificates – During production at Infineon fab, unique asymmetric keys (private and public) are generated. 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 material at the Common Criteria Certified production site*



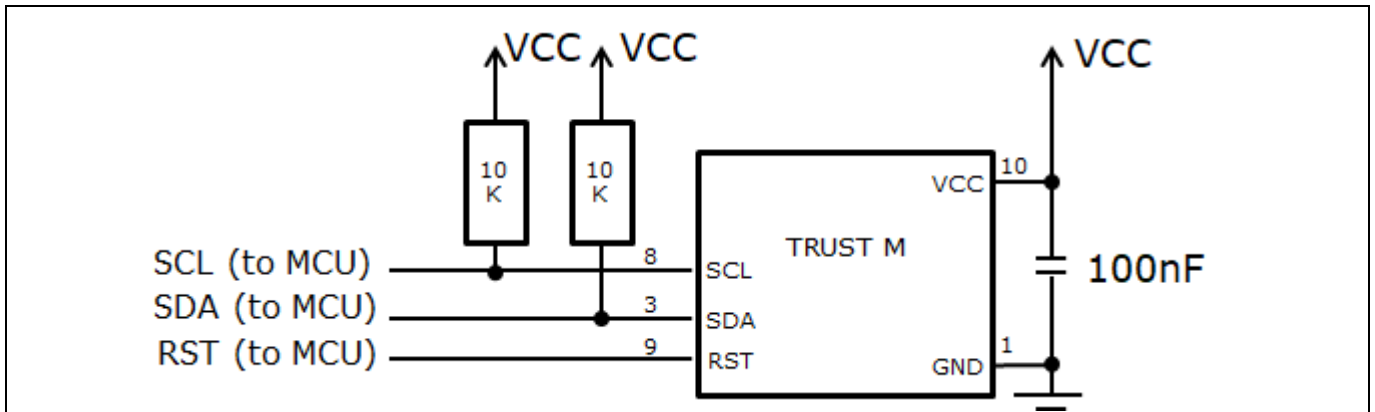
**Interface and Schematics**

**3 Interface and Schematics**

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

**3.1 System Integration Schematics**

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

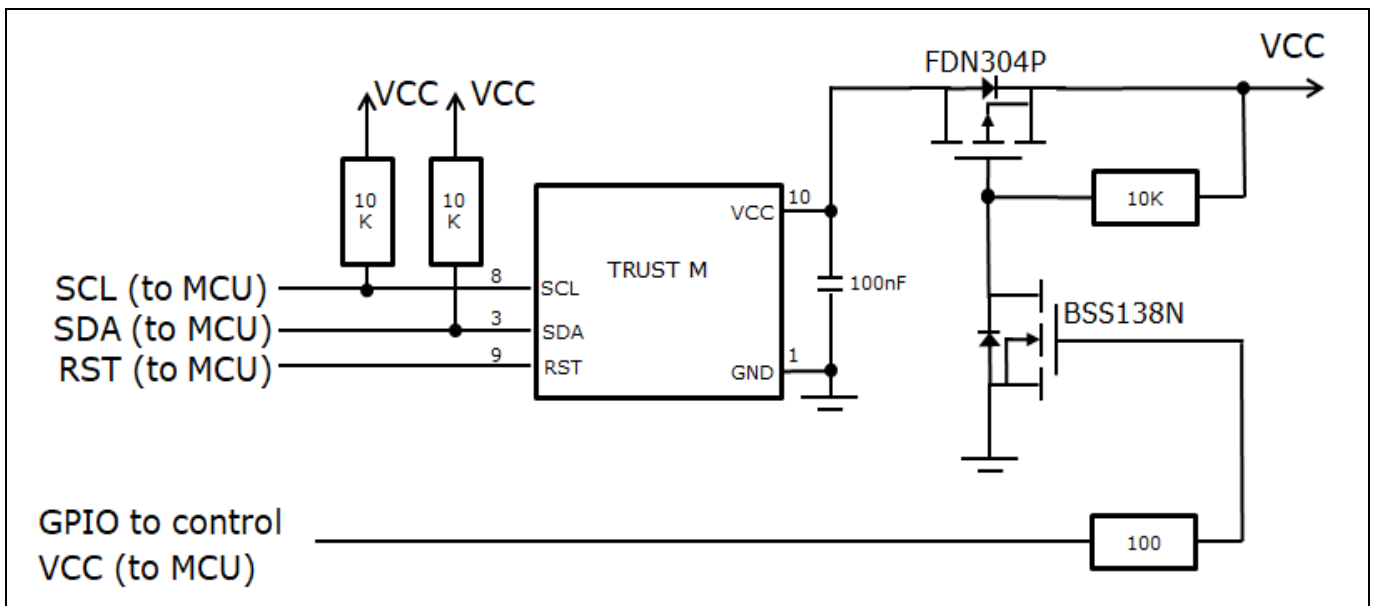


**Figure 2 System Integration Schematic Diagram**

*Note:* Value of the pullup resistors depend on the target application circuit and the targeted I2C frequency.

**3.2 System Integration Schematics with Hibernation support**

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



**Figure 3 System Integration Schematic Diagram with Hibernation**

*Note:* Value of the pullup resistors depend on the target application circuit and the targeted I2C frequency.

**Description of packages**

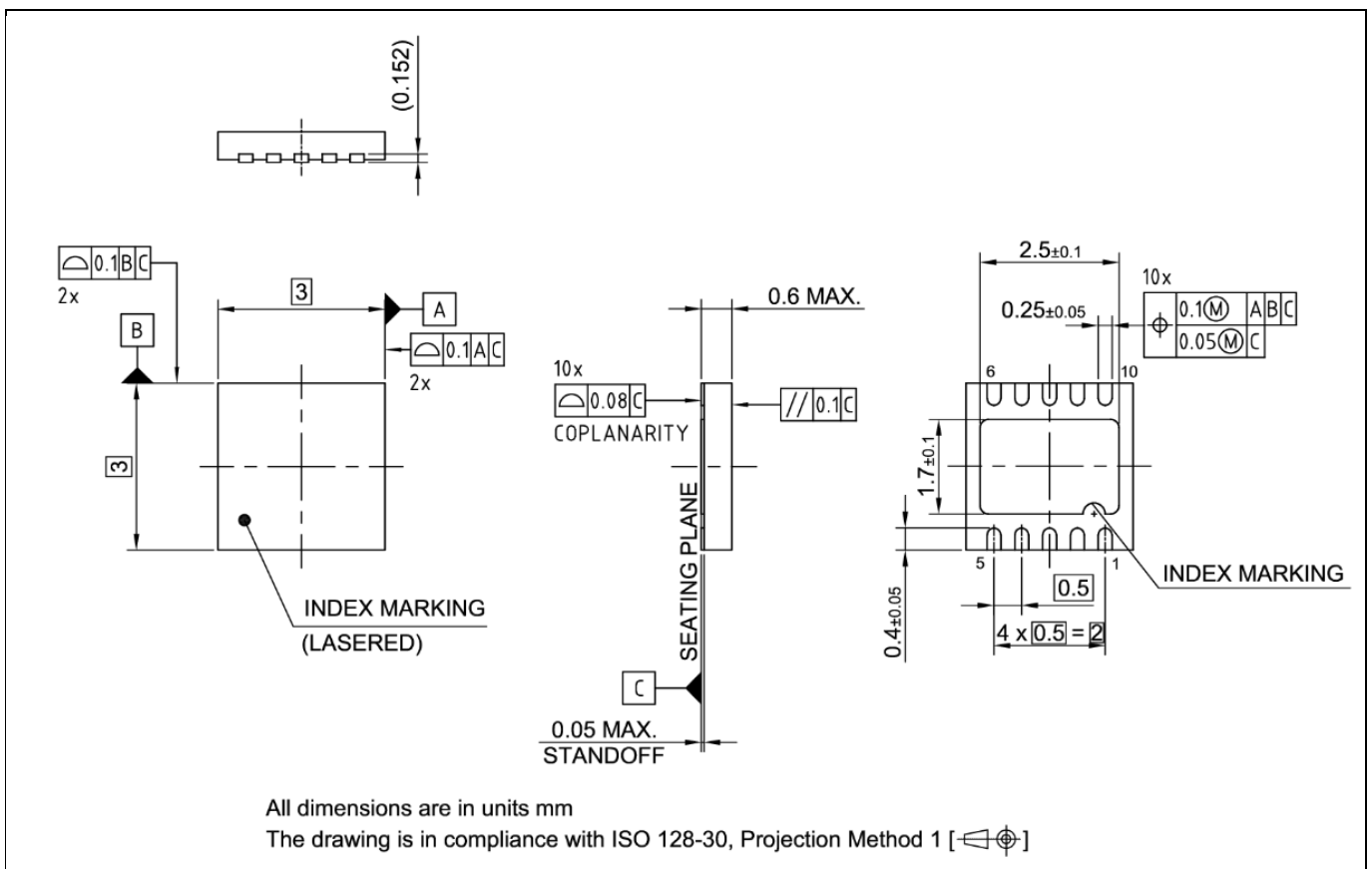
**4 Description of packages**

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**

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



**Figure 4 PG-USON-10-2 Package Outline**

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

Description of packages

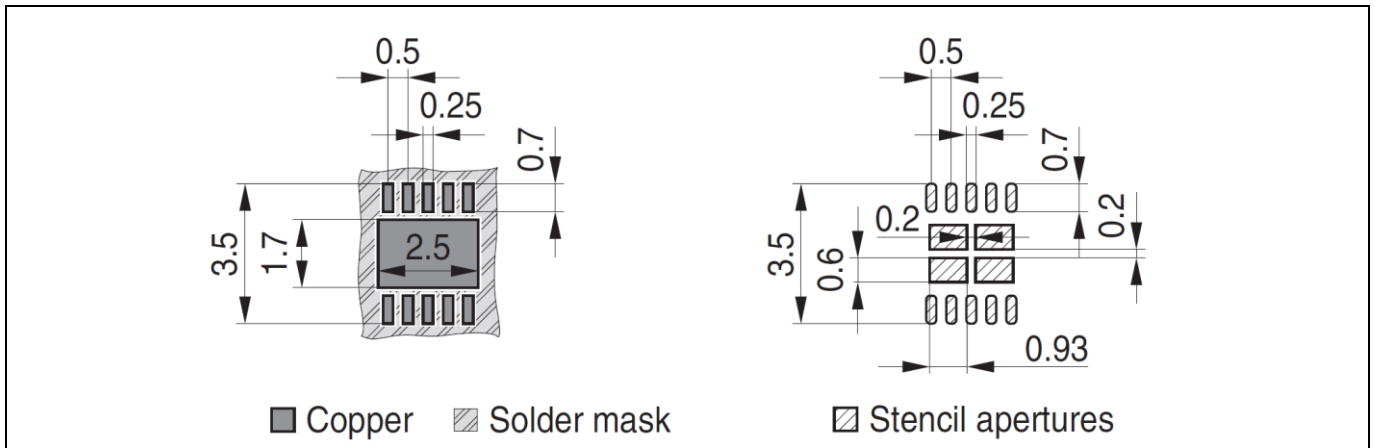


Figure 5 PG-USON-10-2 Package Footprint

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

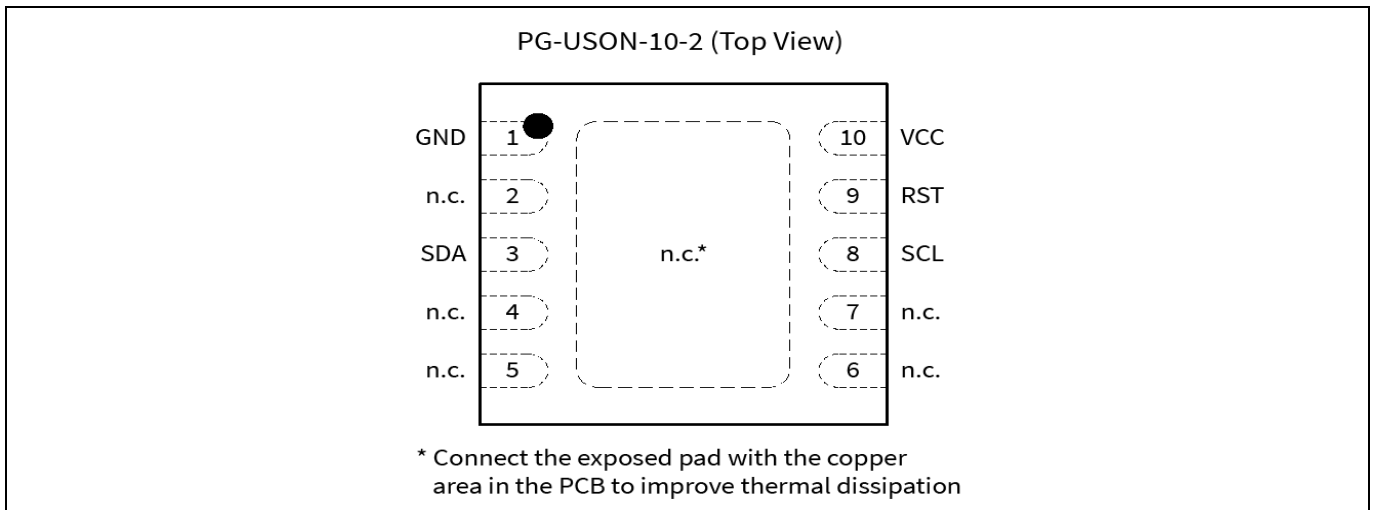


Figure 6 PG-USON-10-2 top view

4.2 Production sample marking pattern

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

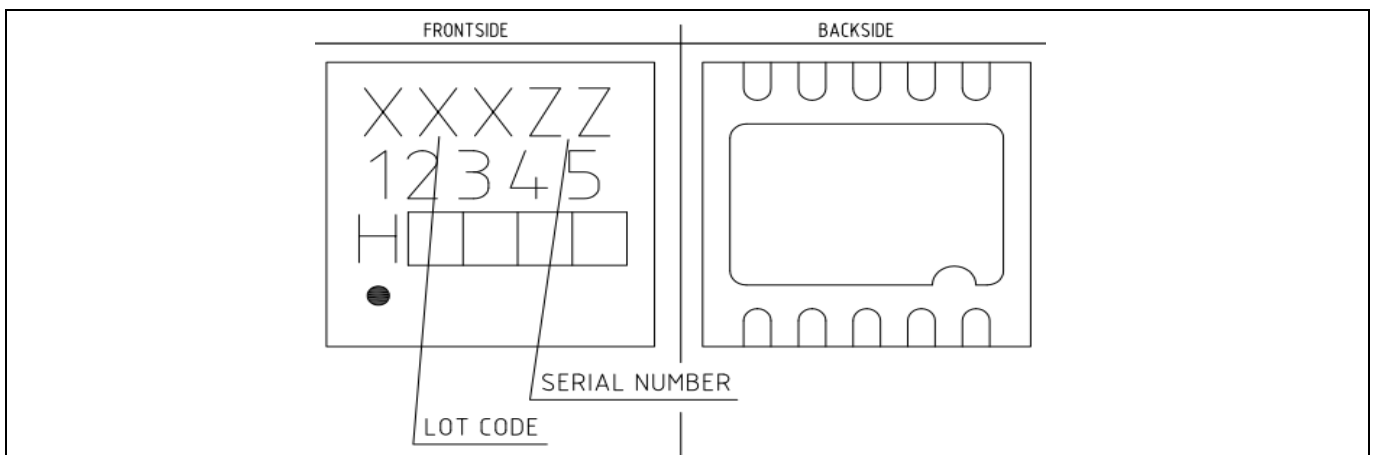


Figure 7 PG-USON-10-2 sample marking pattern

## Description of packages

The black dot indicates pin 01 for the chip. The following [Table 3](#) describes the sample marking pattern:

**Table 3** 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#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: <ul style="list-style-type: none"> <li>• The letter "T" indicates the OPTIGA Trust family</li> <li>• &amp; indicates the product is a Trust M controller</li> <li>• # indicates the controller is a STR (S) variant</li> <li>• \$ specifies the OPTIGA™ Trust M release version number</li> <li>• @ specifies the software version</li> </ul> Example: "TMS10" means 'OPTIGA™ Trust M', 'STR variant', 'release version 1', 'software version 0'

The contacts and their functionality are given in the [Table 4](#) below.

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

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

## Technical Data

### 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 5 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 <sup>1</sup>	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 I<sup>2</sup>C 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 6 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

## Technical Data

**Table 7 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 <sup>2</sup>	–	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  $t_{rmin}$

### 5.1.2 I2C Fast Mode Plus Interface Characteristics

For operation of the I2C interface, the electrical characteristics are compliant with the I<sup>2</sup>C 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 8 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 <sup>1</sup>	–	150	pF	

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

## Technical Data

### 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 9** 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 <sup>1</sup>	$I_{CC,AVG}$	–	20.0	–	mA	While running a typical authentication profile $T_A = 25^\circ\text{C}$ ; $V_{CC} = 5.0\text{ V}$
Supply current, in sleep mode	$I_{CC,S3}$	–	70	100	$\mu\text{A}$	$T_A = 25^\circ\text{C}$ ; $V_{CC,I2C} = 3.3\text{ V}$ ; 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	–	$0.2 * V_{CC}$	V	$I_{IL} = -50\ \mu\text{A}$ to $+20\ \mu\text{A}$
RST input high voltage	$V_{IH}$	$0.7 * V_{CC}$	–	$V_{CC} + 0.3$	V	$I_{IL} = -50\ \mu\text{A}$ to $+20\ \mu\text{A}$
Hibernate current	–	–	< 2.5	–	$\mu\text{A}$	$V_{CC} = 0\text{ V}$ , $\text{GND} = 0\text{ V}$ , $\text{RST} = 0\text{ V}$ , $\text{SCL} = 3.3\text{ V}$ and $\text{SCL} = 3.3\text{ V}$

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

#### 5.1.3.2 AC Electrical Characteristics

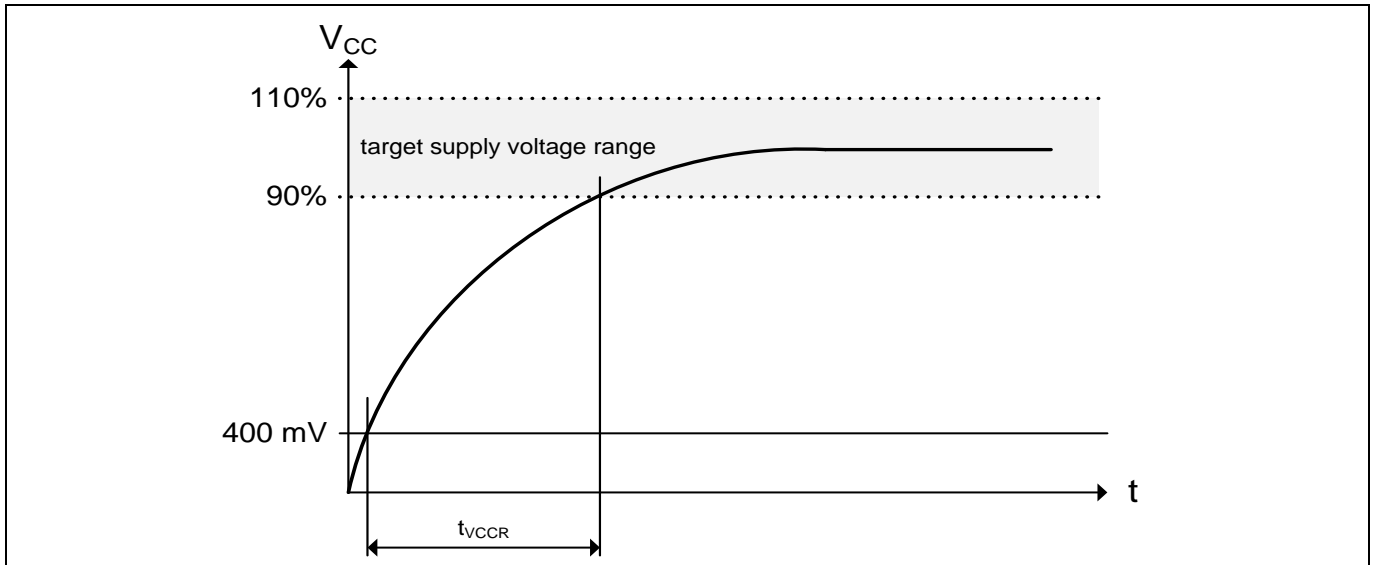
$T_A$  as given for the controller's operating ambient temperature range unless otherwise stated.

All currents flowing into the controller are considered positive.

**Table 10** AC Characteristics

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

The  $V_{CC}$  ramp is depicted in [Figure 8](#). 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  $\pm 10\%$  range.



**Figure 8** **V<sub>CC</sub> Rampup**

### 5.1.4 Start-Up of I2C Interface

There are 2 variants possible for performing the startup procedure:

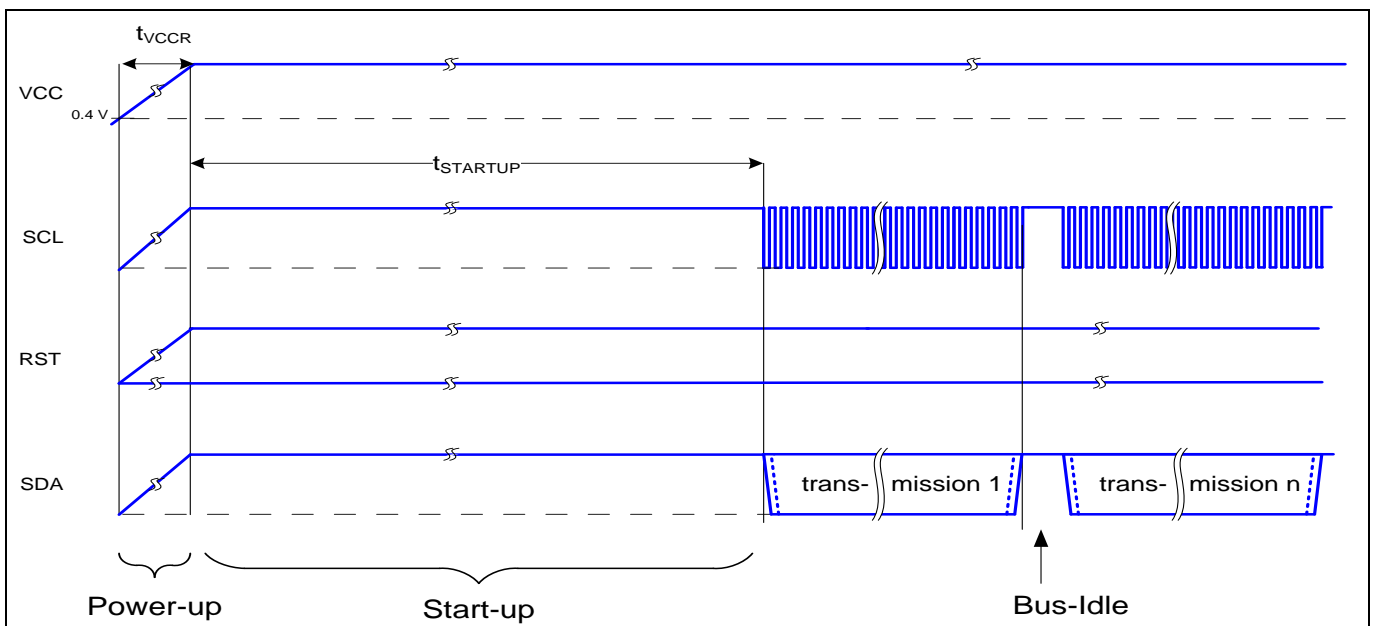
- Startup after power-on
- Startup for warm resets

#### 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 9** **Startup of I2C Interface after Power-On**



**Technical Data**

**Table 11 Startup of I2C Interface After Power-On**

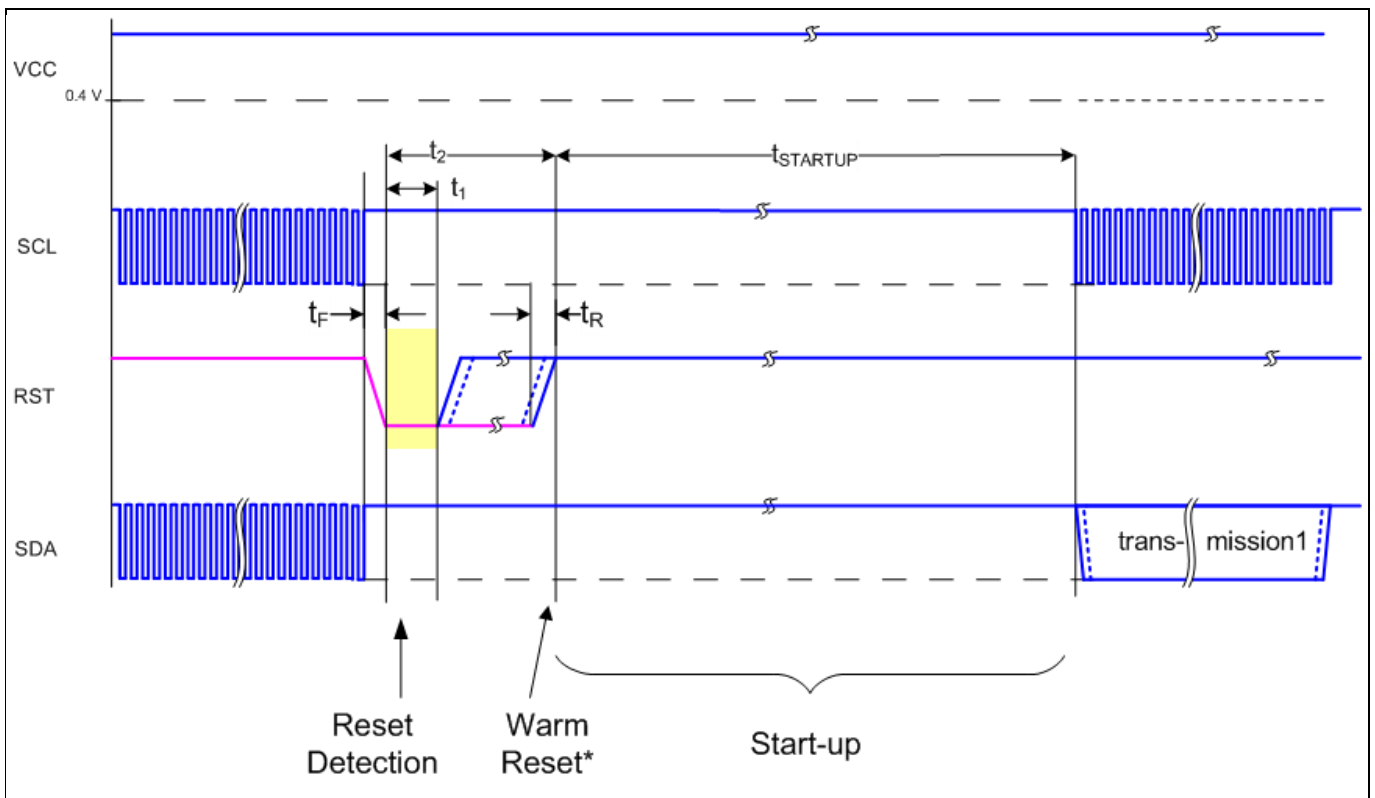
Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Startup time	$t_{STARTUP}$	15			ms	

**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 10 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.*

## Technical Data

**Table 12 Startup of I2C Interface for Warm Resets<sup>1</sup>**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Startup time	$t_{\text{STARTUP}}$	15			ms	
Rise time	$t_{\text{R}}$			1	$\mu\text{s}$	From 10% to 90% of signal amplitude
Fall time	$t_{\text{F}}$			1	$\mu\text{s}$	From 10% to 90% of signal amplitude
Reset detection	$t_1$	10			$\mu\text{s}$	
Reset low		10		2500	$\mu\text{s}$	

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

## Connecting to Host

### 6 Connecting to Host

#### 6.1 OPTIGA™ Trust M Host Software Architecture

The OPTIGA™ Trust M Host Library layers were explained in System Block Diagram [Figure 1](#). In following sections, we will cover how to communicate with OPTIGA™ Trust M using I2C.

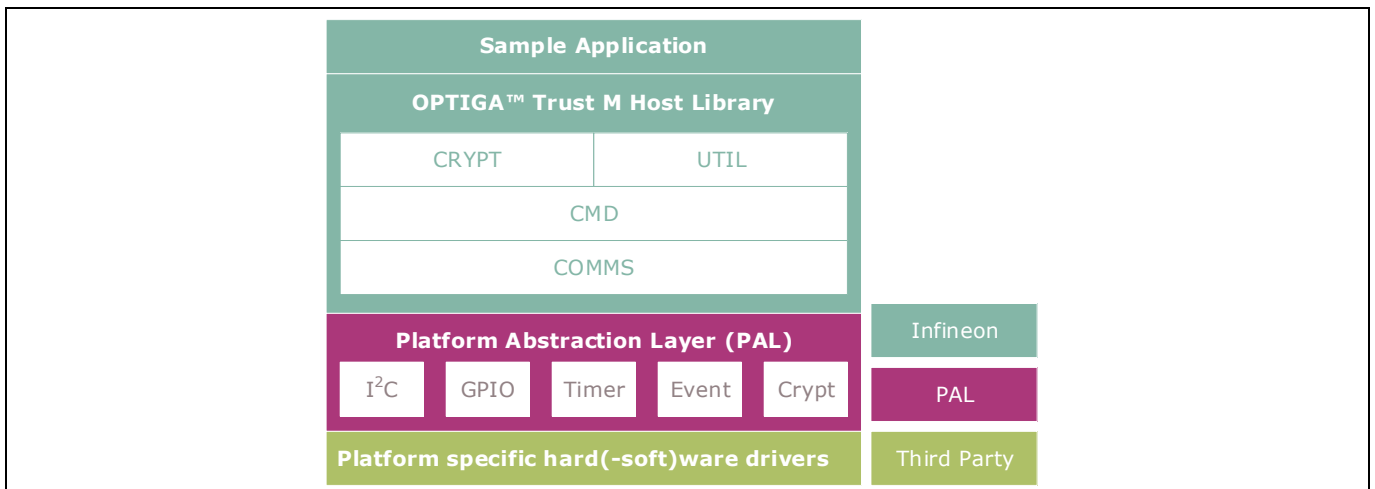


Figure 11 OPTIGA™ Trust M Host Software Architecture

#### 6.2 Release Package Folder Structure

The following figure shows the release package structure when OPTIGA™ Trust M is installed/extracted on PC.

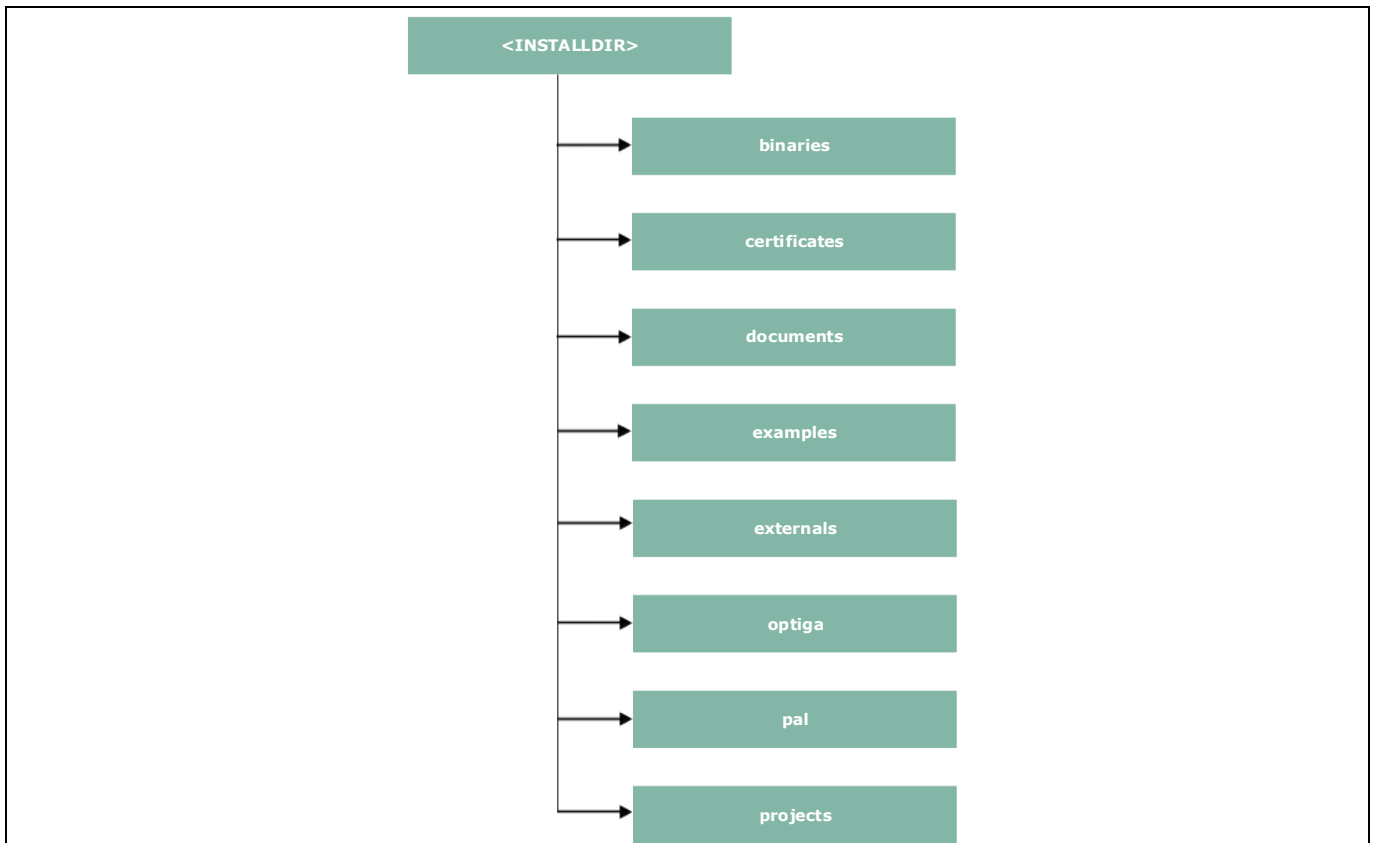


Figure 12 Release Package Folder Structure

### Connecting to Host

<INSTALLDIR> is the root directory to which the release package contents are extracted. The following section explains the contents of each subdirectory under installed directory:

3. binaries

This directory contains binaries for OPTIGA™ Trust M sample application.

4. certificates

This directory contains OPTIGA™ Trust M Test CA and Productive CA certificates.

5. documents

This directory contains all relevant OPTIGA™ Trust M documentation.

6. examples

This directory contains example usecases for Toolbox features and a tool for generation of manifest for secure data object feature.

7. externals

This directory contains mbedtls software crypto libraries.

8. optiga

This directory contains OPTIGA™ Trust M libraries.

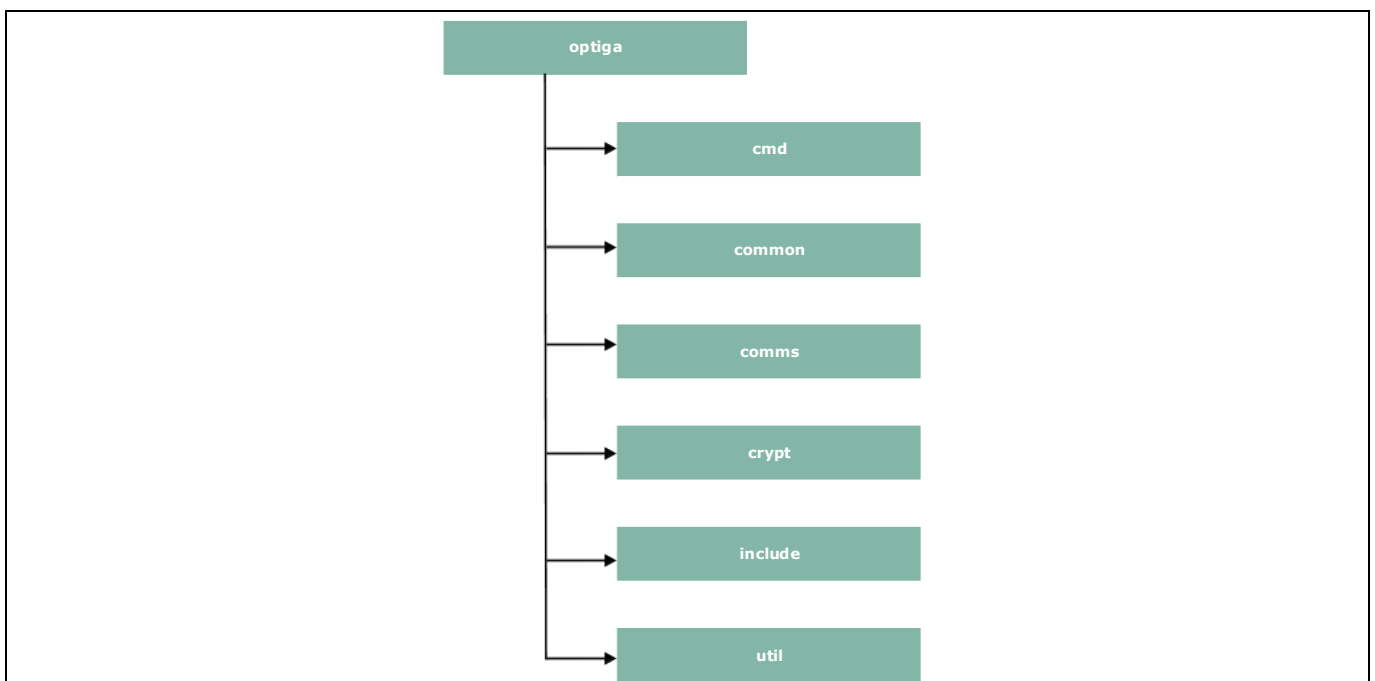
9. pal

This directory contains PAL for XMC4800 device and for mbedtls and wolfssl software crypto libraries.

10. projects

This directory contains XMC4800 device sample project in DAVE™ workspace.

Further the following figure elaborates the OPTIGA™ Trust M Host Software folder structure.



## Connecting to Host

**Figure 13 Host Source Folder Structure**

1. cmd – This folder contains sources for all OPTIGA™ Trust M commands
2. common – This folder contains the common functions used across all the modules
3. comms – This folder contains the driver to communicate with OPTIGA™ Trust M
4. crypt – This folder contains sources for cryptographic functionalities
5. include – This folder contains header files for all OPTIGA™ Trust M Host Software
6. util – This folder contains utility functions e.g. read/write and open/close application

### 6.3 Porting Notes

The implementation of Platform Abstraction Layer (PAL) needs to be updated in order to migrate to a new target platform.

The PAL reference code for the XMC4800 IoT connectivity kit is provided as part of package which can be used. The implementation can be found in “<INSTALLDIR>/pal/xmc4800” and the header files are available in “<INSTALLDIR>/optiga/include” with the required APIs used by upper layers. The header files are platform agnostic and would not require any changes. The low level drivers used by PAL for XMC4800 are configured and generated using DAVE™.

### 6.4 Communication with OPTIGA™ Trust M

The hardware/platform resource configuration with respect to I2C master and GPIOs (Vdd and Reset) are to be updated in [pal\\_ifx\\_i2c\\_config.c](#). These configurations are used by the IFX I2C implementation to communicate with OPTIGA™ Trust M.

#### 7. Update I2C master platform specific context[e.g. (void\*)&i2c\_master\_0]

```

001     /**
002     * \brief PAL I2C configuration for OPTIGA
003     */
004     pal_i2c_t optiga_pal_i2c_context_0 =
005     {
006         // Pointer to I2C master platform specific context
007         (void*)&i2c_master_0,
008         // Slave address
009         0x30,
010         // Upper layer context
011         NULL,
012         // Callback event handler
013         NULL
014     };

```

#### 8. Update platform specific context for GPIOs (Vdd and Reset)

```

001     /**
002     * \brief Vdd pin configuration for OPTIGA
003     */
004     pal_gpio_t optiga_vdd_0 =
005     {
006         // Platform specific GPIO context for the pin used to toggle Vdd
007         (void*)&vdd_pin
008     };
009
010     /**

```

## Connecting to Host

```

011     * \brief Reset pin configuration for OPTIGA
012     */
013     pal_gpio_t optiga_reset_0 =
014     {
015         // Platform specific GPIO context for the pin used to toggle Reset
016         (void*)&reset_pin
017     };

```

### 9. Update PAL I2C APIs [[pal\\_i2c.c](#)] to communicate with OPTIGA™ Trust M

The `pal_i2c` is expected to provide the APIs for I2C driver initialization, de-initialization, read, write and set bitrate kind of operations

- a) [pal\\_i2c\\_init](#)
- b) [pal\\_i2c\\_deinit](#)
- c) [pal\\_i2c\\_read](#)
- d) [pal\\_i2c\\_write](#)
- e) [pal\\_i2c\\_set\\_bitrate](#)

A few target platforms, the I2C master driver initialization ([pal\\_i2c\\_init](#)) is done during the platform start up. In such an environment, there is no need to implement [pal\\_i2c\\_init](#) and [pal\\_i2c\\_deinit](#) functions. Otherwise, these ([pal\\_i2c\\_init](#) & [pal\\_i2c\\_deinit](#)) functions must be implemented as per the upper layer expectations based on the need. The details of these expectations are available in the Host library API documentation (chm).

The reference implementation of PAL I2C based on XMC4800 IoT connectivity kit does not need to have the platform I2C driver initialization explicitly done as part of [pal\\_i2c\\_init](#) as it is taken care by the DAVE™ library initialization. Hence [pal\\_i2c\\_init](#) & [pal\\_i2c\\_deinit](#) are not implemented.

In addition to the above specified APIs, the PAL I2C must handle the events from the low level I2C driver and invoke the upper layer handlers registered with PAL I2C context for the respective transaction as shown in the below example.

```

001     //I2C driver callback function when the transmit is completed successfully
002     void i2c_master_end_of_transmit_callback(void)
003     {
004         invoke_upper_layer_callback(gp_pal_i2c_current_ctx,
005                                     (uint8_t)PAL_I2C_EVENT_TX_SUCCESS);
006     }

```

In above example the I2C driver callback, when transmission is successful invokes the handler to inform the result.

### 10. Update PAL GPIO [[pal\\_gpio.c](#)] to power on and reset the OPTIGA™ Trust M

- f) [pal\\_gpio\\_set\\_high](#)
- g) [pal\\_gpio\\_set\\_low](#)

### 11. Update PAL Timer [[pal\\_os\\_timer.c](#)] to enable timer

- h) [pal\\_os\\_timer\\_get\\_time\\_in\\_milliseconds](#)
- i) [pal\\_os\\_timer\\_delay\\_in\\_milliseconds](#)

### 12. Update Event management for the asynchronous interactions for I2C [[pal\\_os\\_event.c](#)]

- j) [pal\\_os\\_event\\_register\\_callback\\_oneshot](#)
- k) [pal\\_os\\_event\\_trigger\\_registered\\_callback](#)

## Connecting to Host

The [pal\\_os\\_event\\_register\\_callback\\_oneshot](#) function is expected to register the handler and context provided as part of input parameters and triggers the timer for the requested time. The p\_pal\_os\_event is an event instance created using [pal\\_os\\_event\\_create](#).

```

001     void pal_os_event_register_callback_oneshot(
002         pal_os_event_t * p_pal_os_event,
003         register_callback callback,
004         void* callback_args,
005         uint32_t time_us)
006     {
007         p_pal_os_event->callback_registered = callback;
008         p_pal_os_event->callback_ctx = callback_args;
009
010         //lint --e{534} suppress "Return value is not required to be checked"
011         TIMER_SetTimeInterval(&scheduler_timer, (time_us*100));
012         TIMER_Start(&scheduler_timer);
013     }

```

The handler registered must be invoked once the timer has elapsed as shown in [pal\\_os\\_event\\_trigger\\_registered\\_callback](#). The [pal\\_os\\_event\\_trigger\\_registered\\_callback](#) is to be registered with event timer interrupt to get triggered when the timer expires. The pal\_os\_event\_0 is the instance in the pal\_os\_event used store the registered callback and context.

```

001     void pal_os_event_trigger_registered_callback(void)
002     {
003         register_callback callback;
004
005         TIMER_ClearEvent(&scheduler_timer);
006         //lint --e{534} suppress "Return value is not required to be checked"
007         TIMER_Stop(&scheduler_timer);
008         TIMER_Clear(&scheduler_timer);
009
010         if (pal_os_event_0.callback_registered)
011         {
012             callback = pal_os_event_0.callback_registered;
013             callback((void * )pal_os_event_0.callback_ctx);
014         }
015     }

```

## 6.5 Reference code on XMC4800 for communicating with OPTIGA™ Trust M

```

001     static volatile uint32_t optiga_pal_event_status;
002     static void optiga_pal_i2c_event_handler(void* upper_layer_ctx,
003         uint8_t event);
004
005     pal_i2c_t optiga_pal_i2c_context_0 =
006     {
007         /// Pointer to I2C master platform specific context
008         (void*)&i2c_master_0,
009         /// Slave address
010         0x30,
011         /// Upper layer context
012         NULL,
013         /// Callback event handler

```

## Connecting to Host

```
014     NULL,
015     };
016
017     // OPTIGA pal i2c event handler
018     static void optiga_pal_i2c_event_handler(void* upper_layer_ctx,
019                                             uint8_t event)
020     {
021         optiga_pal_event_status = event;
022     }
023
024
025
026
027
028
029
030
031
032
033
034
035
036
037
038
039
040
041
042
043
044
045
046
047
048
049
050
051
052
053
054
055
056
057
058
059
060
061
062
063
064
065
066
067
068
069
070
071
072
073
074
075
076
077
078
079
080
081
082
083
084
085
086
087
088
089
090
091
092
093
094
095
096
097
098
099
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2
```



## Connecting to Host

```
048     }
049
050     /* Main Function */
051     int32_t main(void)
052     {
053         DAVE_STATUS_t status;
054         pal_status_t pal_return_status;
055
056         // Initialisation of DAVE Apps
057         status = DAVE_Init();
058
059         // Stop if DAVE init fails
060         if (DAVE_STATUS_FAILURE == status)
061         {
062             while (1U)
063             {
064             }
065             pal_return_status = test_optiga_communication();
066
067             return (int32_t)pal_return_status;
068     }
```

## OPTIGA™ Trust M External Interface

### 7 OPTIGA™ Trust M External Interface

#### 7.1 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 13 Command table**

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

**Table 14 Mapping of commands with Use cases**

Use Case	OPTIGA™ Trust M commands used
Secure Communication with (D)TLS	GetRandom, CalcHash, CalcSign, VerifySign, CalcSSec, DeriveKey, GenKeyPair, EncryptAsym and DecryptAsym
Datastore (user memory ~ 10kB)	GetDataObject and SetDataObject
Secure Firmware Update	VerifySign and DeriveKey
Secure update of Trust Anchors on Security Chip	SetObjectProtected command

#### 7.2 Crypto Performance

The performance metrics for various schemes are provided by the [Table 15](#) 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: SHA256
- Key Derivation scheme: TLS v1.2 PRF SHA256

## OPTIGA™ Trust M External Interface

- RSA Key size: 2048 bits
- ECC Key size: 256 bits (NIST P-256)

**Table 15** Crypto performance

Scheme	Algorithm	Performance in ms <sup>1</sup>	Performance with Shielded Connection in ms <sup>1</sup>	Notes
Calculate signature	RSA	~ 310	~ 315	Doesn't include message hashing before calling a toolbox function
	ECDSA	~ 60	~ 65	
Verify signature	RSA	~ 45	~ 55	
	ECDSA	~ 85	~ 90	
Diffie-Hellman key agreement	ECC	~ 60	~ 65	Based on ephemeral key pair
Key pair generation	RSA	~ 2900 <sup>2</sup>	~ 2910	Generate 2048 bit RSA key pair
	ECC	~ 75	~ 80	Generate 256 bit ECC key pair
Encryption	RSA	~ 30	~ 45	Encrypt 127 bytes
Decryption	RSA	~ 310	~ 320	Decrypt 127 bytes
Key derivation	PRF as per TLS v1.2	~135	~ 150	
Hash calculation	SHA256	~ 5 Kbyte/s	~ 4.5 Kbyte/s	In blocks of 500 bytes

<sup>1</sup>Minimum Execution of the entire sequence in milli seconds, except the External World timings

<sup>2</sup>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.

## 8 Security Monitor

The Security Monitor is a central component which enforces the security policy of the OPTIGA™ Trust M. It consumes security events sent by security aware parts of the OPTIGA™ Trust M embedded SW and takes actions accordingly as specified in Security Policy below.

### 8.1 Security Events

The events below actively influence the security monitor.

**Table 16 Security Events**

Event	Description
Private Key Use	This event occurs in case the internal services are going to use an OPTIGA™ Trust M hosted private key.
Key Derivation	This event occurs in case the DeriveKey command gets 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.
Suspect System Behavior	This event occurs in case the embedded software detects inconsistencies with the expected behavior of the system. Those inconsistencies might be redundant information which doesn't fit to their counterpart.

### 8.2 Security Policy

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 ( $\pm 5\%$ )
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 16](#)) 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, refer to bullet 3. above). This condition must be stable, at least after 500 uninterrupted executions of protected operations.

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

## 9 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 certain 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<sup>1</sup> 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.



<sup>1</sup>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.

## Appendix A – Infineon I2C Protocol Registry Map

### 10 Appendix A – Infineon I2C Protocol Registry Map

OPTIGA™ Trust M supports IFX I2C v2.01 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 17 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 (e.g. 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 <a href="#">Table 18</a> . 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
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. Fast Mode (Fm+): The allowed values are 50 up to 1000.	Read
0x85	GUARD_TIME <sup>1</sup>	4	For details refer to <a href="#">Table 21</a>	Read only
0x86	TRANS_TIMEOUT <sup>1</sup>	4	For details refer to <a href="#">Table 21</a>	Read only

<sup>1</sup> 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.

## Appendix A – Infineon I2C Protocol Registry Map

Register Address	Name	Size in Bytes	Description	Master Access
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 <a href="#">Table 19</a> . The default mode is SM & FM (011B).	Read / Write

**Table 18 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 <sup>2</sup> C base address specified by <a href="#">Table 17</a>

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 19 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 <sup>2</sup>	2:0	001 010 011 100 other values	Sm Fm SM & Fm (fab out default) Fm+ not valid; writing will be ignored

<sup>1</sup> In case the register returns 0xFFFFFFFF the register and its functionality is not supported

<sup>2</sup> This mode defines the adherence of the bus signals to the electrical characteristics according standard I2C bus specification

## Appendix A – Infineon I2C Protocol Registry Map

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 20 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

### 10.1 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 21 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



## Appendix A – Infineon I2C Protocol Registry Map

Parameter	Default Value	Description
		<p>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.</p> <p><i>Note: The acknowledge timeout on the receiver side must be shorter than the retransmission timeout to avoid unnecessary frame repetitions.</i></p>
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 $\mu$ s	<p>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.</p> <p><i>Note 1: For two consecutive accesses on the same device GUARD_TIME re-specifies the value of <math>t_{BUF}</math> as specified by [I2Cbus].</i></p> <p><i>Note 2: Even if another I2C address is accessed in between GUARD_TIME has to be respected for two consecutive accesses on the same device.</i></p>
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.

## Appendix B - OPTIGA™ Trust M Command/Response I2C Sample Logs

### 11 Appendix B - 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.

#### 11.1 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 (e.g. 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]

##### 11.1.1 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 22 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

##### 11.1.2 Issue OpenApplication command

Before issuing any application specific command; e.g. 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 23 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 <b>70 00 00 10 D2 76 00 00 04 47 65 6E 41 75 74 68 41 70 70 6C</b> 04 1A
Step 2: Read the I2C_STATE register [Repeat this step until the read contains the data as specified below]		



Appendix C – Power Management

## 12 Appendix C – 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 1mA from 6mA to 15 mA with a precision of ±5%.

### 12.1 Hibernation

This maximizes power saving (zero power consumption<sup>1</sup>), while the I2C bus stays connected. In this case OPTIGA™ Trust M saves the application context before power-off (switching off V<sub>CC</sub>) and restores it after power-up. After power-up the application continues seamlessly from the state before hibernate.

### 12.2 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 14.

1. As soon as the OPTIGA™ Trust M is idle it starts to count down the “delay to sleep” time (t<sub>SDY</sub>).
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 (e.g. counting down the SEC). In case all idle tasks are finished and no command is pending, the OPTIGA™ Trust M enters sleep mode.

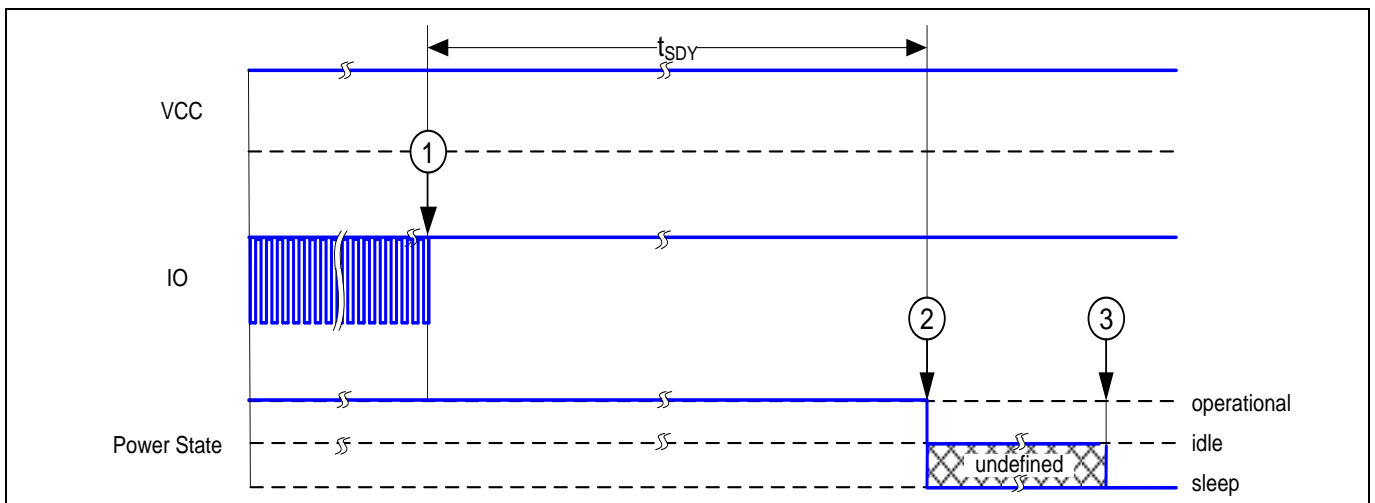


Figure 14 Go-to-Sleep Diagram

<sup>1</sup> Leakage current < 2.5µA



**Revision history****Revision history**

<b>Document version</b>	<b>Date of release</b>	<b>Description of changes</b>
1.71	2019-07-19	Hibernate current updated in section 5.1.3.1 and footnote added for zero power consumption
1.70	2019-07-17	Updated section 6 for XMC 4800 IoT connectivity kit
1.65	2019-05-23	RC Release version and update in table 23
1.61	2019-04-22	RC release version and minor updates to features on the first page
1.60	2019-03-15	RC release version
1.50	2019-02-05	ES release version
1.40	2019-01-18	Internal reviews incorporated
1.30	2019-01-07	Updates to all sections
1.20	2018-10-01	Second release with internal reviews incorporation
1.10	2018-09-24	Updates to all sections
1.00	2018-07-07	First Version Release
0.50	2018-06-29	Initial Version (Internal release)

## Trademarks

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

**Edition 2019-07-19**

**Published by**

**Infineon Technologies AG**

**81726 Munich, Germany**

**© 2019 Infineon Technologies AG.**

**All Rights Reserved.**

**Do you have a question about this document?**

**Email:**

[DSSCustomerService@infineon.com](mailto:DSSCustomerService@infineon.com)

**Document reference**

## IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office ([www.infineon.com](http://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.