OPTIGA™ Trust Charge

Product Version: V1

About this document

Scope and purpose

This document specifies the Release Notes for OPTIGA™ Trust Charge solution.

Intended audience

This document addresses the audience: customers, solution providers and system integrators.

Table of Contents

Revision History

Page	Subjects (major changes since last revision)
4	Engineering Sample Release of OPTIGA™ Trust Charge and its corresponding host libraries

1 Product Version Overview

1.1 Release versions

The Release versions defined in the below table is the overall version of OPTIGA™ Trust Charge which includes the OPTIGA™ Trust Charge Host library package and OPTIGA™ Trust Charge security chip version.

Release Version	Build Date	Description
v1.30.1039	2020-08-14	Engineering Sample Release of OPTIGA™ Trust Charge and its corresponding host libraries

1.2 Versioning Scheme

1. **Product Version:**

   It defines the version of the product. (Example: OPTIGA Trust Charge **V1**, **V2, etc...)**

2. **Release version:**

   Defines the revision of the product released with encoding scheme **Major, Minor,** and **Build** number. (**Example** – v1.30.1039, Major version = 1, Minor version = 00, Build version = 1039)

   2.1. **Major version** - It depicts the major changes/revisions of the product. Early engineering sample releases will always have the release major version as zero. (Example - v**x.**yy.zzzz)

   2.2. **Minor version** - It changes with releases or/and significant changes in the product. (Example - vx**.yy**.zzzz)

   2.3. **Build version** – It increments based on each change/release of the product. (Example - vx.yy.**zzzz**)

Note: Every release will have an OPTIGA™ security chip version [1], which defines the version of the software loaded on the OPTIGA™ security chip.

OPTIGA™ Trust Charge security chip version will have the same major and minor version numbers of that particular release version. But the build number of OPTIGA™ Trust Charge security chip version might be different from the overall release version.

Example:

Release Version = v1.30.1039 (Major version = 1, Minor version = 30, Build version = 1039)
Security chip version = v1.30.809 (Major version = 1, Minor version = 30, Build version = 809)

2 Engineering Sample Release v1.30.1039

2.1 Product Description

OPTIGA™ Trust Charge v1.30.1039 is an Embedded Security Solution covering use cases to protect the authenticity, integrity and confidentiality of your device: mutual authentication, secure communication, data storage protection, cryptographic toolbox functionalities and lifecycle management for connected devices.

2.2 Scope of Release

OPTIGA™ Trust Charge v1.30.1039 is released as Engineering Sample Release. The Product is qualified by Infineon with complete documentation describing all features as stated below.

2.3 Contents of the Evaluation Kit

1. OPTIGA™ Trust Charge security chip with software build v1.30.809
2. Package containing following Software and Documentation
   - 2.1. binaries
     - 2.1.1. Example for XMC4700 Relax Kit V1
   - 2.2. certificates
     - 2.2.1. Contains Infineon Trust Charge certificate for execution of use cases
   - 2.3. documents
     - 2.3.1. OPTIGA™ Trust Charge V1 Datasheet v1.30
     - 2.3.2. Infineon I2C Protocol v2.02
     - 2.3.3. OPTIGA™ Trust Charge V1 Solution Reference Manual v1.00
     - 2.3.4. OPTIGA™ Trust Charge V1 Release Notes v1.30
     - 2.3.5. OPTIGA™ Trust Charge V1 Host Library Documentation
     - 2.3.6. OPTIGA™ Trust Charge V1 Getting Started Guide v1.00
     - 2.3.7. OPTIGA™ Trust Charge V1 License Information
   - 2.4. examples
     - 2.4.1. optiga
       - 2.4.1.1. Example files for OPTIGA™ host library APIs
     - 2.4.2. tools
       - 2.4.2.1. Tool to generate protected update data set for the data objects (used for optiga_util_protected_update API example)
   - 2.5. externals

2.5.1. Directory for 3rd party libraries (e.g. mbedTLS etc)

2.6. optiga

2.6.1. OPTIGA™ host library with source and header files

2.7. pal

2.7.1. Platform specific implementation for XMC4700 Relax Kit V1

2.8. projects

2.8.1. DAVE™ Eclipse project for XMC4700 Relax Kit V1

3. Hardware

3.1. XMC4700 Relax Kit V1

3.2. Shield2Go with OPTIGA™ Trust Charge security chip

3.3. My IoT Adapter

4. Open Source Software – subject to separate licensing terms as below

4.1. Applicable for host library

4.1.1. mbedTLS v2.16.0 crypto library (https://tls.mbed.org/download)

4.1.2. LUFA USB stack (https://www.lufa-lib.org)

2.4 Features

1. OPTIGA™ Trust Charge Security Chip Software
   a. Infineon I2C protocol v2.02 based communication (Shielded Connection)
   b. Configurable protected data storage
   c. Life cycle management
   d. Crypto ToolBox commands with ECC NIST P256/P384, SHA-256 (sign, verify, key generation)
   e. Hibernate and restore support
   f. Integrity protected update of data object.
2. OPTIGA™ Trust Charge Host Software
   a. Infineon I2C Protocol v2.02 based communication (Shielded Connection)
   b. OPTIGA™ Trust Charge host asynchronous libraries (optiga_crypt, optiga_util)
   c. Tool to generate CBOR based manifest and payload fragments for optiga_util_protected_update API example.

2.5 Fixes

Not Applicable as it's the Initial Release

2.6 Enhancements

Not Applicable as it's the Initial Release

2.7 Known Issues

1. Disconnecting the power (VDD pin) of the Host MCU during the communication with OPTIGA™ Trust Charge and re-establishing the connection might end up in Infineon I2C protocol stack non responsive state due to the low level driver issue observed.

2.8 Limitations

1. The maximum number of OPTIGA™ crypt instances which would be based on session is limited to 4 in parallel.
2. Third-party libraries such as mbed TLS might invoke memory allocation functions during optiga comms protection (shielded connection) operations (pal_crypt). There could be collision during memory allocation, if a create API from service layer is invoked at the same time.
3. OPTIGA™ is a singleton resource. The number of instances that can run in parallel is limited to 6 (1 active instance and 5 instances will be queued up internally). To increase the maximum number of parallel instances, re-configure the macro OPTIGA_CMD_MAX_REGISTRATIONS (minimum value is 1) in optiga_lib_config.h.
4. In XMC4700 based evaluation kit, operating the I2C at lower speeds (e.g less than 200 KHz) results in communication hung state. Hence the pal_i2c_set_bitrate API is not supported to change the bitrate at run time. Currently I2C is set to run at 400 KHz by default.

2.9 Environment

None

Edition 2020-08-14

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email:
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**).

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.