OPTIGA™ Trust M

Product Version: V3

About this document

Scope and purpose

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

Intended audience

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

Table of Contents

About this document **1**
Table of Contents **2**
Revision History **3**
1 Product Version Overview **4**
1.1 Release versions 4
1.2 Versioning Scheme 4
2 Engineering Sample Release v3.00.2484 ..... **5**
2.1 Product Description 5
2.2 Scope of Release 5
2.3 Contents of the Evaluation Kit 5
2.4 Features 6
2.5 Fixes 7
2.6 Enhancements 7
2.7 Known Issues 7
2.8 Limitations 7
2.9 Environment 7

Revision History

Page	Subjects (major changes since last revision)
5	Engineering Sample Release of OPTIGA™ Trust M v3.00.2484 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 M which includes the OPTIGA™ Trust M Host library package and OPTIGA™ Trust M security chip version.

Release Version	Build Date	Description
v3.00.2484	2020-09-17	Engineering Sample Release of OPTIGA™ Trust M and its corresponding host libraries

1.2 Versioning Scheme

1. **Product Version:**

   It defines the version of the product. (Example: OPTIGA Trust M **V1**, **V2, V3 etc...)**

2. **Release version:**

   Defines the revision of the product released with encoding scheme **Major, Minor,** and **Build** number. **Example** – v3.00.2484 (Major version : 3, Minor version : 00, Build version : 2484)

   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 [5], which defines the version of the software loaded on the OPTIGA™ security chip.

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

Example:

Release Version : v3.00.2484 (Major version : 3, Minor version : 00, Build version : 2484)
Security chip version : v3.00.2440 (Major version : 3, Minor version : 00, Build version : 2440)

2 Engineering Sample Release v3.00.2484

2.1 Product Description

OPTIGA™ Trust M v3.00.2484 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 M v3.00. 2484 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 M security chip with software build v3.00.2440
2. Package containing following Software and Documentation
    2.1. binaries
        2.1.1. Examples for XMC4800 IOT Connectivity kit
    2.2. certificates
        2.2.1. Contains Infineon Test CA certificate for execution of use cases
    2.3. documents
        2.3.1. OPTIGA™ Trust M Datasheet v3.00
        2.3.2. Infineon I2C Protocol v2.02
        2.3.3. OPTIGA™ Trust M Solution Reference Manual v3.00
        2.3.4. OPTIGA™ Trust M Release Notes v3.00
        2.3.5. OPTIGA™ Trust M Keys And Certificates v3.00
        2.3.6. OPTIGA™ Trust M Host Library Documentation
        2.3.7. OPTIGA™ Trust M Getting Started Guide v3.00
        2.3.8. OPTIGA™ Trust M 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, key set for key objects and metadata set for data/key objects (used for optiga_util_protected_update API example).

2.5. externals

2.5.1. Directory for 3rd party libraries (e.g. mbed TLS)

2.6. optiga

2.6.1. OPTIGA™ host library with source and header files

2.7. pal

2.7.1. Platform specific implementation for XMC4800 IoT Connectivity Kit

2.8. projects

2.8.1. DAVE™ Eclipse project for XMC4800 IoT Connectivity Kit

3. Hardware

3.1. XMC4800 IoT Connectivity Kit

3.2. Shield2Go with OPTIGA™ Trust M security chip

3.3. My IoT Adapter

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

4.1. Applicable for XMC4800 IoT Connectivity Kit

4.1.1. mbed TLS 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 M Security Chip Software
   a. Infineon I2C protocol v2.02 based communication with Shielded Connection support.
   b. Configurable protected data storage.
   c. Life cycle management.
   d. Crypto ToolBox commands with
      i. ECC NIST P256/P384/P521, Brainpool P256/384/512, SHA-256/384/512 (sign, verify, key generation, ECDH, key derivation)
      ii. RSA 1024/2048 (Sign, Verify, Key generation, Encrypt, Decrypt, Pre-master secret generation for RSA Key exchange (reference TLS V1.2))
      iii. Symmetric encryption and decryption using AES-128/192/256 (ECB, CBC, CBC-MAC, CMAC) and HMAC SHA256/384/512.
      iv. KeyDerivation using HKDF SHA256/384/512
   e. Hibernate and restore support.
   f. Integrity and confidentiality protected update of data, metadata and key objects
   g. Boot phase flag(Global and Application security states) based access to protected keys and data

h. HMAC verification with authorization reference states.
i. Configurable security monitor.

2. OPTIGA™ Trust M Host Software
   a. Support for XMC4800 IoT Connectivity Kit added.
   b. DAVE Eclipse project added to release package. This project can be used for compilation and debugging.
   c. Optiga Crypt Library (Crypto Toolbox command APIs)
   d. Optiga Util Library (Open/Close Application, Read/Write and Protected Update command APIs)
   e. Infineon I2C protocol v2.02 based communication with Shielded Connection support.
   f. Tool to generate CBOR based manifest and payload fragments for optiga_util_protected_update API example.

2.5 Fixes

None

2.6 Enhancements

None

2.7 Known Issues

1. Disconnecting the power (VDD pin) of the Host MCU during the communication with OPTIGA™ Trust M 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. As the RSA key generation can go beyond 50 seconds, the default timeout of ifx i2c protocol (TL_MAX_EXIT_TIMEOUT) is set to 180 seconds. Otherwise, 10 seconds is sufficient.

2.9 Environment

None

Edition 2020-09-17

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.