# OPTIGA™ Trust M1

## Release Notes

## About this document

### Scope and purpose

This document specifies the Release Notes for OPTIGA™ Trust M1 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) |
|------|---------------------------------------------|
| 5 | Engineering Sample release of OPTIGA™ Trust M1v1.00.769 and its corresponding host libraries with Hibernate support, Integrity protected update of data object and UP counter |
| 8 | Early Engineering Sample release of OPTIGA™ Trust M1v0.70.631 and its corresponding host libraries with cryptographic ToolBox commands support for RSA 1024/2048 |
| 11 | Early Engineering Sample release of OPTIGA™ Trust M1v0.50.514 and its corresponding host libraries |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# 1    Product Version Overview

| Product Version / Build Number | Build Date | Description |
|---|---|---|
| V1.00 / Build 769 (V1.00.769) | 06.02.2019 | Engineering Sample Release of OPTIGA™ Trust M1 and its corresponding host libraries with hibernate support, integrity protected update of data object and UP counter |
| V0.70 / Build 631 (V0.70.631) | 01.10.2018 | Early Engineering Sample Release of OPTIGA™ Trust M1 and its corresponding host libraries  with cryptographic ToolBox commands support for RSA 1024/2048 |
| V0.50/Build 514 (V0.50.514) | 10.07.2018 | Early Engineering Sample Release of OPTIGA™ Trust M1 and its corresponding host libraries |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 2 Engineering Sample Release v1.00 (Build 769)

## 2.1 Product Description

OPTIGA™ Trust M1 V1.00 / Build 769 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 M1 V1.00 / Build 769 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 M1 security chip with software build v1.00.751

2. Package containing following Software and Documentation

    2.1. binaries

        2.1.1. Sample for XMC4500 Relax Kit V1

    2.2. certificates

        2.2.1. Contains Infineon Test CA certificate for execution of use cases

    2.3. documents

        2.3.1. OPTIGA™ Trust M1 Datasheet v1.50

        2.3.2. Infineon I2C Protocol v2.02

        2.3.3. OPTIGA™ Trust M1 Solution Reference Manual v1.00

        2.3.4. OPTIGA™ Trust M1 Release Notes v1.00

        2.3.5. OPTIGA™ Trust M1 Keys And Certificates v1.2

        2.3.6. OPTIGA™ Trust M1 Host Library Documentation

    2.4. examples

        2.4.1. optiga

            2.4.1.1. Example files for OPTIGA™ host library APIs

    2.5. externals

        2.5.1. Directory for 3$^{rd}$ party libraries (e.g. mbedTLS, wolfSSL 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 XMC4500 Relax Kit V1

2.8. projects

    2.8.1.     Platform specific project files

3. Hardware

   3.1. XMC4500 Relax Kit V1

   3.2. Extension Board v2.5 with OPTIGA™ Trust M1 SLS 32AIA010MC security chip

   3.3. USB to Micro USB Cable

   3.4. LAN Cable

   3.5. USB Ethernet adapter

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

   4.1. Applicable for XMC4500 Relax Kit V1

      4.1.1.     lwIP for UDP Communication sources (http://savannah.nongnu.org/projects/lwip/)

      4.1.2.     mbedTLS 2.7.0 crypto library (https://tls.mbed.org/download)

## 2.4     Features

1. OPTIGA™ Trust M1 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 ECC NIST P256/P384, SHA-256 (sign, verify, key generation, ECDH, key derivation), RSA 1024/2048 (Sign, Verify, Key generation, Encrypt, Decrypt, Pre-master secret generation for RSA Key exchange (reference TLS V1.2))
   e. Hibernate and restore support.
   f. Integrity protected update of data object.
2. OPTIGA™ Trust M1 Host Software
   a. Added Protected(Integrity) update and Update Counter
   b. Hibernate/Restore option enabled using Util open and close APIs

## 2.5     Fixes

1. OPTIGA™ Trust M1 Host library enhancements

   1.1. Fixed corruption of private key OID passed in RSA optiga_crypt_decrypt_and_store and optiga_crypt_decrypt_and_export APIs.

   1.2. Fixed the issue in pal_i2c_set_bitrate API, which releases the I2C bus locking semaphore, even if it is not acquired within the API.

   1.3. Fixed the corruption of the frame length of the repeated frame in Infineon I2C protocol, when calculate hash is called after a reset.

   1.4. Fixed missing initialization (Initialize to NULL) of service layer instance pointer in example code.

## 2.6     Enhancements

1. OPTIGA™ Trust M1 Security Chip Software

1.1. Open and Close Application enhanced to support hibernate and restore options.

1.2. Generate key Pair command enhanced to support key generation with same key usage, when key object provided write access conditions are satisfied.

1.3. SetDataObject command enhanced to support up counter feature(count data object).

1.4. Data store Enhanced for the following

  1.4.1. Added additional Trust Anchor data object and 4 Monotonic Counter data objects.

  1.4.2. Removed Arbitrary Type 1 data objects and added Arbitrary Type 3 data object of size 140 bytes.

  1.4.3. Enhancements in endurance for data objects.

2. OPTIGA™ Trust M1 Host library enhancements

2.1. Scheduler mechanism updated to handle strict sequence for Protected (Integrity) Update.

2.2. Util open and close enhanced to support hibernate/restore option.

2.3. Optiga Comms shielded connection APIs added for individual service layers (Crypt and Util).

## 2.7 Known Issues

1. Disconnecting the power (VDD pin) of the Host MCU during the communication with OPTIGA™ Trust M1 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. The scheduler "optiga_cmd_queue_scheduler" relies on tick counts provided by "pal_os_timer_get_time_in_microseconds" to schedule the API requests of service layer. In case the tick count overflows, the API request after the overflow gets scheduled before any pending API request.

## 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 wolfssl/ mbedtls 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_cmd.c.

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

# 3 Early Engineering Sample Release v0.70 (Build 631)

## 3.1 Product Description

OPTIGA™ Trust M1 V.70/ Build 631 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.

## 3.2 Scope of Release

OPTIGA™ Trust M1 V0.70 / Build 631 is released as Early Engineering Sample Release. The Product is qualified[1] by Infineon with complete documentation describing all features as stated below.

## 3.3 Contents of the Evaluation Kit

5. OPTIGA™ Trust M1 security chip with software build v0.70.624

6. Package containing following Software and Documentation

    6.1. binaries

        6.1.1. Sample for XMC4500 Relax Kit V1

    6.2. certificates

        6.2.1. Contains Infineon Test CA certificate for execution of use cases

    6.3. documents

        6.3.1. OPTIGA™ Trust M1 Datasheet v1.0

        6.3.2. Infineon I2C Protocol v2.02

        6.3.3. OPTIGA™ Trust M1 Solution Reference Manual v2.0

        6.3.4. OPTIGA™ Trust M1 Release Notes v0.70

        6.3.5. OPTIGA™ Trust M1 Keys And Certificates v1.1

        6.3.6. OPTIGA™ Trust M1 Host Library Documentation

    6.4. examples

        6.4.1. optiga

            6.4.1.1. Example files for OPTIGA™ host library APIs

    6.5. externals

        6.5.1. Directory for 3rd party libraries (e.g. mbedTLS, wolfSSL etc)

    6.6. optiga

        6.6.1. OPTIGA™ host library with source and header files

    6.7. pal

---

[1] Functional tests are executed, but all corner case scenarios are not covered as part of qualification.

## 3.4      Features

1.   OPTIGA™ Trust M1 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, ECDH, key derivation), RSA 1024/2048 (Sign, Verify, Key generation, Encrypt, Decrypt, Pre-master secret generation)
2.   OPTIGA™ Trust M1 Host Software
     a.   Infineon I2C Protocol v2.02 based communication (Shielded Connection)
     b.   OPTIGA™ Trust M1 host asynchronous libraries (optiga_crypt, optiga_util)

## 3.5      Fixes

1.   Fixed the certificate parser length validation for signature sub tags in OPTIGA™ Trust M1 Security chip software.

2.   Fixed the public key length check validation issue in VerifySign command with public key certificate OID as input in OPTIGA™ Trust M1 Security chip software.

3.   Fixed the issue in Derive key command to handle maximum APDU data input, when presentation layer is enabled with protection level set to Master or both Master and Slave Payload protection in OPTIGA™ Trust M1 Security chip software.

4.   Fixed the APDU formation for optiga_crypt_tls_prf_sha256 API to handle maximum APDU data input of 1557 in the OPTIGA™ Host library.

5.   Fixed system hang issue when optiga_util_destroy API is called, while an util instance is already in use in the OPTIGA™ Host library.

## 3.6    Enhancements

1. OPTIGA™ Trust M1 Security Chip Software

    1.1. Cryptographic ToolBox commands enhanced to support for RSA 1024/2048. Asymemtric Encrypt and Decrypt commands added to support RSA 1024/2048.

    1.2. Data store enhanced with Integrity and Confidentiality protection support with shielded connection.

2. OPTIGA™ Trust M1 Host library enhancements

    2.1. Cryptographic ToolBox (optiga_crypt) APIs added to support for RSA 1024/2048.

    2.2. Scheduler mechanism is enhanced.

    2.3. PAL OS event module is enhanced to support instance based usage.

    2.4. Added macros for shielded connection options.

## 3.7    Known Issues

1. Disconnecting the power (VDD pin) of the Host MCU during the communication with OPTIGA™ Trust M1 and re-establishing the connection might end up in Infineon I2C protocol stack non responsive state.

## 3.8    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 wolfssl/ mbedtls 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_cmd.c.

4. Hibernate feature is not supported in the OPTIGA™ Host Library. The options provided in the util layer functions to hibernate/restore OPTIGA™ security chip application are not funtionally complete. This will be enhanced in future.

5. 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.

## 3.9    Environment

None

# 4       Early Engineering Sample Release v0.50 (Build 514)

## 4.1      Product Description

OPTIGA™ Trust M1 V0.50 / Build 514 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.

## 4.2      Scope of Release

OPTIGA™ Trust M1 V0.50 / Build 514 is released as Early Engineering Sample Release. The Product is qualified[1] by Infineon with complete documentation describing all features as stated below.

## 4.3      Contents of the Evaluation Kit

1. OPTIGA™ Trust M1 security chip with software build v0.50.501

2. Package containing following Software and Documentation

    2.1. binaries

        2.1.1.     Sample for XMC4500 Relax Kit V1

    2.2. certificates

        2.2.1.     Contains Infineon Test CA certificate for execution of use cases

    2.3. documents

        2.3.1.     OPTIGA™ Trust M1 Datasheet v1.0

        2.3.2.     Infineon I2C Protocol v2.00

        2.3.3.     OPTIGA™ Trust M1 Solution Reference Manual v0.50

        2.3.4.     OPTIGA™ Trust M1 Release Notes v0.50

        2.3.5.     OPTIGA™ Trust M1 Keys And Certificates v1.0

        2.3.6.     OPTIGA™ Trust M1 Host Library Documentation

    2.4. examples

        2.4.1.     optiga

            2.4.1.1.     Example files for OPTIGA™ host library APIs

    2.5. externals

        2.5.1.     Directory for 3rd party libraries (e.g. mbedTLS, wolfSSL 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 XMC4500 Relax Kit V1

---

[1] Limited functional tests are executed but not all corner case scenarios and reliability tests are covered as part of qualification

2.8. projects

    2.8.1.      Platform specific project files

3. Hardware

    3.1. XMC4500 Relax Kit V1

    3.2. Extension Board v2.5 with OPTIGA™ Trust M1 SLS 32AIA010MC security chip

    3.3. USB to Micro USB Cable

    3.4. LAN Cable

    3.5. USB Ethernet adapter

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

    4.1. Applicable for XMC4500 Relax Kit V1

        4.1.1.      lwIP for UDP Communication sources ([http://savannah.nongnu.org/projects/lwip/](http://savannah.nongnu.org/projects/lwip/))

## 4.4      Features

1. OPTIGA™ Trust M1 Security Chip Software
   a. Infineon I2C protocol v2.00 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, ECDH, key derivation)
2. OPTIGA™ Trust M1 Host Software
   a. Infineon I2C Protocol v2.00 based communication (Shielded Connection)
   b. OPTIGA™ Trust M1 host asynchronous libraries (optiga_crypt, optiga_util)

## 4.5      Fixes

Not Applicable

## 4.6      Enhancements

Not Applicable

## 4.7      Known Issues

1. Disconnecting the power (VDD pin) of the Host MCU during the communication with OPTIGA™ Trust M1 and re-establishing the connection might end up in Infineon I2C protocol stack non responsive state.

## 4.8      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 wolfssl/ mbedtls 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_cmd.c.

4. The configuration option to enable and disable shielded connection feature is not provided in optiga_lib_config.h file. This must be configured in the project settings by defining the macro IFX_I2C_PRESENTATION_LAYER_ENABLED.

## 4.9     Environment

None