OPTIGA™ Trust M

Product Version: V1

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

Table of Contents

Revision History

Page	Subjects (major changes since last revision)
6	Release to Production of OPTIGA™ Trust M v1.30.885 with evaluation kit based on XMC4800 IoT Connectivity Kit
9	Release Candidate release of OPTIGA™ Trust M1 v1.30.812 with personalization issue fixed
12	Release Candidate release of OPTIGA™ Trust M1 v1.20.802 with 2 million Tearing safe programming cycle support and its corresponding host libraries
15	Release Candidate release of OPTIGA™ Trust M1 v1.01.769 and its corresponding host libraries with document updates
18	Engineering Sample release of OPTIGA™ Trust M1 v1.00.769 and its corresponding host libraries with Hibernate support, Integrity protected update of data object and UP counter
21	Early Engineering Sample release of OPTIGA™ Trust M1 v0.70.631 and its corresponding host libraries with cryptographic ToolBox commands support for RSA 1024/2048
24	Early Engineering Sample release of OPTIGA™ Trust M1 v0.50.514 and its corresponding host libraries

1 Product Version Overview

Product Version / Build Number	Build Date	Description
V1.30 / Build 885 (V1.30.885)	2019-09-18	Release to Production for OPTIGA™ Trust M with evaluation kit based on XMC4800 IoT Connectivity Kit
V1.30 / Build 812 (V1.30.812)	2019-05-30	Release Candidate release of OPTIGA™ Trust M1 with personalization issue of private key defect fix.
V1.20 / Build 802 (V1.30.802)	2019-04-23	Release Candidate release of OPTIGA™ Trust M1 with 2 million Tearing safe programming cycle support and its corresponding host libraries.
V1.01 / Build 769 (V1.01.769)	2019-03-15	Release Candidate release of OPTIGA™ Trust M1 and its corresponding host libraries with document updates
V1.00 / Build 769 (V1.00.769)	2019-02-06	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)	2018-10-01	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)	2018-07-10	Early Engineering Sample Release of OPTIGA™ Trust M1 and its corresponding host libraries

2 Release to Production v1.30 (Build 885)

2.1 Product Description

OPTIGA™ Trust M v1.30 / Build 885 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 v1.30 / Build 885 is released as Release to Production. 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 v1.30.809
2. Package containing following Software and Documentation
   - 2.1. binaries
     - 2.1.1. Binaries for XMC4800 IOT Connectivity kit
   - 2.2. certificates
     - 2.2.1. Contains Infineon Test and Productive CA certificates for execution of use cases
   - 2.3. documents
     - 2.3.1. OPTIGA™ Trust M Datasheet v1.72
     - 2.3.2. Infineon I2C Protocol v2.02
     - 2.3.3. OPTIGA™ Trust M V1 Solution Reference Manual v1.13
     - 2.3.4. OPTIGA™ Trust M V1 Release Notes v1.30
     - 2.3.5. OPTIGA™ Trust M V1 Keys And Certificates v1.50
     - 2.3.6. OPTIGA™ Trust M Host Library Documentation
     - 2.3.7. OPTIGA™ Trust M V1 Getting Started Guide v1.00
     - 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 (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 adaptation 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 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 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 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 M Host Software
   a. Optiga Crypt Library (Crypto Toolbox command APIs)
   b. Optiga Util Library (Open/Close Application, Read/Write and Protected Update command APIs)
   c. Infineon I2C protocol v2.02 based communication with Shielded Connection support.

2.5 Fixes

1. Fixed strict lock execution priority issue with multiple instances in OPTIGA™ Trust M Host Library scheduler.

2.6 Enhancements

1. Scheduling mechanism updated to handle the effect of tick counter overflow.
2. WolfSSL crypto library is removed from the release package.
3. Tool to generate CBOR based manifest and payload fragments for optiga_util_protected_update API example, enhanced to support ECC NIST P384 and RSA2048 to generate the signature of manifest.

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 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 Release Candidate Release v1.30 (Build 812)

3.1 Product Description

OPTIGA™ Trust M1 V1.30 / Build 812 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 V1.30 / Build 812 is released as Release Candidate. The Product is qualified by Infineon with complete documentation describing all features as stated below.

3.3 Contents of the Evaluation Kit

1. OPTIGA™ Trust M1 security chip with software build v1.30.809
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 v1.65
     - 2.3.2. Infineon I2C Protocol v2.02
     - 2.3.3. OPTIGA™ Trust M1 Solution Reference Manual v1.12
     - 2.3.4. OPTIGA™ Trust M1 Release Notes v1.30
     - 2.3.5. OPTIGA™ Trust M1 Keys And Certificates v1.40
     - 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
     - 2.4.2. tools
       - 2.4.2.1. Tool to generate CBOR based manifest and payload fragments for optiga_util_protected_update API example.
   - 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 V

2.8. projects

2.8.1. Platform specific project files

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board with OPTIGA™ Trust M1 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)

3.4 Features

3. 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.
4. OPTIGA™ Trust M1 Host Software
   a. Optiga Crypt Library (Crypto Toolbox command APIs)
   b. Optiga Util Library (Open/Close Application, Read/Write and Protected Update command APIs)
   c. Infineon I2C protocol v2.02 based communication with Shielded Connection support.

3.5 Fixes

1. Fixed OPTIGA™ Trust M1 Security Chip software,

1.1. Personalization issue fixed.

1.2. Fixed SetobjectProtected command target OID change access condition validation issue within the complex expression in corner case scenarios.

2. Datasheet and Solution Reference manual updates.

3.6 Enhancements

None

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 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.

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. 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 Release Candidate Release v1.20 (Build 802)

4.1 Product Description

OPTIGA™ Trust M1 V1.20 / Build 802 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 V1.20 / Build 802 is released as Release Candidate. The Product is qualified 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 v1.20.802
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 v1.61
     - 2.3.2. Infineon I2C Protocol v2.02
     - 2.3.3. OPTIGA™ Trust M1 Solution Reference Manual v1.10
     - 2.3.4. OPTIGA™ Trust M1 Release Notes v1.20
     - 2.3.5. OPTIGA™ Trust M1 Keys And Certificates v1.40
     - 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 optiga
     - 2.4.2. tools
       - 2.4.2.1. Tool to generate CBOR based manifest and payload fragments for optiga_util_protected_update API example.
   - 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

2.8. projects

2.8.1. Platform specific project files

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board with OPTIGA™ Trust M1 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)

4.4 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 update (Integrity) and Update Counter
   b. Hibernate/Restore option enabled using Util open and close APIs

4.5 Fixes

1. Fixed OPTIGA™ Trust M1 Security Chip software,

1.1. Integrity validation issue in the SetObjectProtected command.

2. Fixed OPTIGA™ Trust M1 Host Library software,

2.1. With shielded connection enabled and session not established, the optiga_util_close_application API does not pull down the Vdd pin with hibernate option.

4.6 Enhancements

1. Added Production CA Certificates and updated OPTIGA™ Trust M1 Keys and Certificates document with the details of the certificates.
2. Increased the tearing safe programming cycles to 2 Million cycles for the overall data objects.
3. Updated Solution Reference Manual for tearing safe programming cycle details.

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 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.

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 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.

4.9 Environment

None

5 Release Candidate Release v1.01 (Build 769)

5.1 Product Description

OPTIGA™ Trust M1 V1.01 / 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.

5.2 Scope of Release

OPTIGA™ Trust M1 V1.01 / Build 769 is released as Release Candidate. The Product is qualified by Infineon with complete documentation describing all features as stated below.

5.3 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 v1.60
     - 2.3.2. Infineon I2C Protocol v2.02
     - 2.3.3. OPTIGA™ Trust M1 Solution Reference Manual v1.01
     - 2.3.4. OPTIGA™ Trust M1 Release Notes v1.01
     - 2.3.5. OPTIGA™ Trust M1 Keys And Certificates v1.30
     - 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

2.8. projects

2.8.1. Platform specific project files

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board with OPTIGA™ Trust M1 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)

5.4 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 update (Integrity) and Update Counter
   b. Hibernate/Restore option enabled using Util open and close APIs

5.5 Fixes

None

5.6 Enhancements

1. OPTIGA™ Trust M1 Documentation updates.

5.7 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 higher endurance specified for some of the objects in OPTIGA™ Trust M1 Security Chip (Monotonic counters, Security Event Counter etc.) cannot be achieved, since the overall endurance of the OPTIGA™ Trust M1 Security Chip is limited to 800,000 cycles.
3. 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.

5.8 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 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.

5.9 Environment

None

6 Engineering Sample Release v1.00 (Build 769)

6.1 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.

6.2 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.

6.3 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 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

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)

6.4 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

6.5 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.

6.6 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).

6.7 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.

6.8 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 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.

6.9 Environment

None

7 Early Engineering Sample Release v0.70 (Build 631)

7.1 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.

7.2 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.

7.3 Contents of the Evaluation Kit

1. OPTIGA™ Trust M1 security chip with software build v0.70.624
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 v2.02
     - 2.3.3. OPTIGA™ Trust M1 Solution Reference Manual v2.0
     - 2.3.4. OPTIGA™ Trust M1 Release Notes v0.70
     - 2.3.5. OPTIGA™ Trust M1 Keys And Certificates v1.1
     - 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

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

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)

7.4 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)

7.5 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.

7.6 Enhancements

1. OPTIGA™ Trust M1 Security Chip Software
   1.1. Cryptographic ToolBox commands enhanced to support for RSA 1024/2048. Asymmetric 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.

7.7 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.

7.8 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 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 functionally 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.

7.9 Environment

None

8 Early Engineering Sample Release v0.50 (Build 514)

8.1 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.

8.2 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.

8.3 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

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

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/)

8.4 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)

8.5 Fixes

Not Applicable

8.6 Enhancements

Not Applicable

8.7 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.

8.8 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 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.

8.9 Environment

None

Edition 2019-09-18

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.