OPTIGA™ Trust X1

Release Notes

About this document

Scope and purpose

This document specifies the Release Notes for OPTIGA™ Trust X1 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 4
1 Product Version Overview 5
2 Maintenance Release for OPTIGA™ Trust X1 Release v1.60 (Build 1179) 6
2.1 Product Description 6
2.2 Scope of Release 6
2.3 Contents of the Evaluation Kit 6
2.4 Features 7
2.5 Fixes 8
2.6 Enhancements 8
2.7 Known Issues 8
2.8 Limitations 9
2.9 Environment 9
3 Release to Production for OPTIGA™ Trust X1 Release v1.50 (Build 1153) 10
3.1 Product Description 10
3.2 Scope of Release 10
3.3 Contents of the Evaluation Kit 10
3.4 Features 11
3.5 Fixes 12
3.6 Enhancements 12
3.7 Known Issues 12
3.8 Limitations 12
3.9 Environment 13
4 Release to Production for OPTIGA™ Trust X1 Release v1.40 (Build 1118) 14
4.1 Product Description 14
4.2 Scope of Release 14
4.3 Contents of the Evaluation Kit 14
4.4 Features 15
4.5 Fixes 16
4.6 Enhancements 16
4.7 Known Issues 16
4.8 Limitations 16
4.9 Environment 16
5 Release Candidate Release v1.30 (Build 1112) 17
5.1 Product Description 17
5.2 Scope of Release 17
5.3 Contents of the Evaluation Kit 17
5.4 Features 18
5.5 Fixes 19
5.6 Enhancements 19
5.7 Known Issues 19
5.8 Limitations 19
5.9 Environment 19
6 Release Candidate Release v1.21 (Build 1103) 20
6.1 Product Description 20
6.2 Scope of Release 20

Table of Contents

6.3 Contents of the Evaluation Kit 20
6.4 Features 21
6.5 Fixes 22
6.6 Enhancements 22
6.7 Known Issues 22
6.8 Limitations 22
6.9 Environment 22
7 Engineering Sample Release v1.2 (Build 1099) 23
7.1 Product Description 23
7.2 Scope of Release 23
7.3 Contents of the Evaluation Kit 23
7.4 Features 24
7.5 Fixes 25
7.6 Enhancements 25
7.7 Known Issues 25
7.8 Limitations 25
7.9 Environment 25
8 Early Engineering Sample Release v1.1 (Build 732) 26
8.1 Product Description 26
8.2 Scope of Release 26
8.3 Contents of the Evaluation Kit 26
8.4 Features 27
8.5 Fixes 28
8.6 Enhancements 28
8.7 Known Issues 28
8.8 Limitations 28
8.9 Environment 28
9 Early Engineering Sample Release v1.0 (Build 596) 29
9.1 Product Description 29
9.2 Scope of release 29
9.3 Contents of the Evaluation Kit 29
9.4 Features 30
9.5 Fixes 31
9.6 Enhancements 31
9.7 Known Issues 31
9.8 Limitations 31
9.9 Environment 31

Revision History

Page	Subjects (major changes since last revision)
6	Maintenance Release for OPTIGA™ Trust X1 V1.60.1179 with improvements in host library and documentation updates.
10	Release to production for OPTIGA™ Trust X1 V1.50.1153. Host libraries restructured with IFX I2C asynchronous implementation and multi slave support on XMC4500 relax kit v1with corresponding documentation updates.
14	Release to production for OPTIGA™ Trust X1 V1.40.1118 and its corresponding host libraries on XMC4500 relax kit v1 with update to the Derive key command in OPTIGA™ Trust X1 Security Chip Software
17	Release Candidate release of OPTIGA™ Trust X1 V1.30.1112 and its corresponding host libraries on XMC4500 relax kit v1 with update to the Derive key command in OPTIGA™ Trust X1 Security Chip Software
20	Release Candidate release of OPTIGA™ Trust X1 V1.21.1103 and its corresponding host libraries on XMC4500 relax kit v1 with fixes in documentation
23	Engineering Sample release of OPTIGA™ Trust X1 V1.2.1099 and its corresponding host libraries on XMC4500 relax kit v1 with Cryptographic ToolBox commands
26	Early Engineering Sample release of OPTIGA™ Trust X1 V1.1.732 and its corresponding host libraries on XMC4500 relax kit v1 with USB Type-C™ commands
29	Early Engineering Sample release of OPTIGA™ Trust X1 V1.0.596 and its corresponding host libraries on XMC4500 relax kit v1

1 Product Version Overview

Product Version / Build Number	Build Date	Description
V1.60 / Build 1179 (V1.60.1179)	2019-02-28	Maintenance Release for OPTIGA™ Trust X1 Host Library with the following updates, • OPTIGA™ Trust X1 host library to support open source with MIT license. • OPTIGA™ Trust X Host library enhanced for supporting higher (–O3) optimization. • Documentation improvements.
V1.50 / Build 1153(V1.50.1153)	03.02.2018	Release to production for OPTIGA™ Trust X1 with following updates done as part of this release, • IFX I2C implementation in OPTIGA™ Trust X1 host library is enhanced to support the asynchronous behaviour with multi slave support • Restructured the host libraries in the package with corresponding documentation updates.
V1.40 / Build 1118 (V1.40.1118)	16.10.2017	Release to production for OPTIGA™ Trust X1 with following updates done as part of this release, • Added OPTIGA™ Trust X1 Productive CA certificate • Fixed known issues [4.5] to OPTIGA™ Trust X1 Demo User Interface • OPTIGA™ Trust X1 Getting Started Guide and Demo User Interface Manual
V1.30 / Build 1103 (V1.30.1112)	16.08.2017	Release Candidate Release of OPTIGA™ Trust X1 and its corresponding host libraries on XMC4500 Relax Kit v1 with update to the Derive key command in OPTIGA™ Trust X1 Security Chip Software
V1.21 / Build 1103 (V1.21.1103)	28.07.2017	Release Candidate Release of OPTIGA™ Trust X1 and its corresponding host libraries on XMC4500 Relax Kit v1 with documentation fixes
V1.2 / Build 1099 (V1.2.1099)	06.07.2017	Engineering Sample Release of OPTIGA™ Trust X1 and its corresponding host libraries on XMC4500 Relax Kit v1 with Cryptographic ToolBox commands
V1.1 / Build 732 (V1.1.732)	03.03.2017	Early Engineering Sample Release of OPTIGA™ Trust X1 and its corresponding host libraries on XMC4500 Relax Kit v1 with USB Type-C™ commands
V1.0 / Build 596 (V1.0.596)	05.12.2016	Early Engineering Sample Release of OPTIGA™ Trust X1 and its corresponding host libraries on XMC4500 Relax Kit v1

2 Maintenance Release for OPTIGA™ Trust X1 Release v1.60 (Build 1179)

2.1 Product Description

OPTIGA™ Trust X1 V1.60 / Build 1179 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 X1 V1.60 / Build 1179 is released as Maintenance 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 X1 security chip with software build v1.40.1118
2. OPTIGA™ Trust X1_1.60.1179.zip containing the following Software and Documentation

   2.1. PC

      2.1.1. Bin

      2.1.2. Documentation

         2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.3

         2.1.2.2. OPTIGA™ Trust X API Documentation v1.60.1179

      2.1.3. Source

         2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library and User Interface sources

         2.1.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)

   2.2. Host

      2.2.1. Bin

      2.2.2. Projects

         2.2.2.1. Contains platform specific folder which contains project files and use case sample sources

      2.2.3. Source

         2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources

         2.2.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)

   2.3. DemoUI

      2.3.1. Contains the binaries to run the User interface Demo

2.4. Documentation

2.4.1. OPTIGA™ Trust X Datasheet Revision v2.70

2.4.2. OPTIGA™ Trust X Getting Started Guide v1.60

2.4.3. IFX I2C Protocol Spec v1.65

2.4.4. OPTIGA™ Trust X Solution Reference Manual v1.35

2.4.5. OPTIGA™ Trust X Release Notes v1.60

2.4.6. OPTIGA™ Trust X Keys and Certificates v1.30

2.4.7. OPTIGA™ Trust X License Information

2.4.8. OPTIGA™ Trust X User Interface Manual v1.20

2.4.9. OPTIGA™ Trust X Host Library API Documentation v1.60.1179

2.4.10. OPTIGA™ Trust X XMC Application Notes v1.60

2.5. CACertificates

2.5.1. Contains Certificates required for execution of use cases

2.6. Test Server

2.6.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.5 with OPTIGA™ Trust X SLS 32AIA020X2 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. PC

4.1.1. User Interface utilizing MVVM Light (https://mvvmlight.codeplex.com/) and Extended WPF Toolkit sources (http://wpftoolkit.codeplex.com)

4.2. XMC

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

2.4 Features

1. OPTIGA™ Trust X1 Security Chip Software

   a. Infineon I2C protocol v1.65 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage
   d. Life cycle management
   e. Cryptographic functionalities for Secure Communication - DTLS-Client [Mutual Authentication] and Encrypted Communication
   f. USB Type-C™ supporting commands
   g. Cryptographic ToolBox commands to perform cryptographic operations like hash generation (HASH), signature calculation and verification (SIGN/VERIFY), Shared secret agreement (ECDH) and derivation of keys.
2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.65 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Secure Communication - DTLS-Client [Mutual Authentication]
   d. Encrypt communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
   f. Cryptographic Toolbox commands
3. OPTIGA™ Trust X PC Software
   a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Join customer PKI domain
   d. Cryptographic Toolbox commands

2.5 Fixes

1. Fixed the following issues in optiga_comms (ifx_i2c functions) layer functionalities.
   a. 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.
   b. Fixed the corruption of frame length of the repeated frame in Infineon I2C protocol, when calculate hash is called after reset.

2.6 Enhancements

1. OPTIGA™ Trust X1 host library is now open source with MIT license.
2. OPTIGA™ Trust X Host library enhanced for supporting higher (O3) optimization.
3. Documents in the package are updated.
4. Setup Installer is removed and the release package is available as archived package.

2.7 Known Issues

1. In User Interface Demo, continuous invocation of Join customer PKI Domain or Read General Purpose data use case fails to execute and hangs for few seconds, when the security event counter value of OPTIGA™ Trust X1 is more than 7.
2. In User Interface Demo, after executing the secure communication – DTLS client, the auto update of security event counter (SEC) value in the status bar gets disabled. The auto update of SEC value happens only when the One Way Authentication use case is successfully executed.

2.8 Limitations

1. The below DAVE™ generated files in the package are modified to fix the issues seen when integrated with OPTIGA™ TrustX1 host libraries.
    a. I2C_MASTER APP (Digital filter feature additionally added)
    b. ETH_LWIP APP(In cc.h file “time.h” inclusion is commented)
    c. TIMER APP (Typecasting in timer.c file for fixing the compilation warning in Keil)

   Hence, if the DAVE™ project is re-generated, the above files in the sample projects gets overwritten with the DAVE™ installed configuration.

   The above APPs (applications) will be fixed and released in the next version of DAVE™ public release. Use the APP migration feature of DAVE™ to update these APPs to latest versions.
2. The below are the limitations in the Certificate parser for OPTIGA™ Trust X1 security chip
    a. The certificate parser at OPTIGA™ Trust X1 cannot parse the certificates which has the subject name or issuer field attributes other than issued by joint-iso-itu-t (OID starting with 2, e.g “1.2.840.113549.1.9.1” email address of the issuer).
    b. Certificate Parser does not validate the following sections in the certificates and allow to parse the certificate even for incorrect values,
        i. Sequence Tag in the Validity field.
        ii. Validation of second level tag length in 3 level hierarchical tag lengths.
    c. Length of the ASN tag extraction is limited to 2 bytes, even if the length is more than 2 byte value.

2.9 Environment

The details of reference environment are explained in Getting Started Guide document.

3 Release to Production for OPTIGA™ Trust X1 Release v1.50 (Build 1153)

3.1 Product Description

OPTIGA™ Trust X1 V1.50 / Build 1153 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 X1 V1.50 / Build 1153 is released as Release Candidate Release. 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 X1 security chip with software build v1.40.1118

2. Setup.zip containing Setup.exe which installs the following Software and Documentation

    2.1. PC

        2.1.1. Bin

        2.1.2. Documentation

            2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.3

            2.1.2.2. OPTIGA™ Trust X API Documentation v1.50.1153

        2.1.3. Source

            2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library and User Interface sources

            2.1.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)

    2.2. Host

        2.2.1. Bin

        2.2.2. Projects

            2.2.2.1. Contains platform specific folder which contains project files and use case sample sources

        2.2.3. Source

            2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources

            2.2.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)

    2.3. DemoUI

        2.3.1. Contains the binaries to run the User interface Demo

2.4. Documentation

2.4.1. OPTIGA™ Trust X Datasheet Revision v2.5

2.4.2. OPTIGA™ Trust X Getting Started Guide v1.5

2.4.3. IFX I2C Protocol Spec v1.65

2.4.4. OPTIGA™ Trust X Solution Reference Manual v1.35

2.4.5. OPTIGA™ Trust X Release Notes v1.50

2.4.6. OPTIGA™ Trust X Keys and Certificates v1.2

2.4.7. OPTIGA™ Trust X License Information

2.4.8. OPTIGA™ Trust X User Interface Manual v1.2

2.4.9. OPTIGA™ Trust X Host Library API Documentation v1.50.1153

2.4.10. OPTIGA™ Trust X XMC Application Notes v1.50

2.5. CACertificates

2.5.1. Contains Certificates required for execution of use cases

2.6. Test Server

2.6.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.5 with OPTIGA™ Trust X SLS 32AIA020X2 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. PC

4.1.1. User Interface utilizing MVVM Light (https://mvvmlight.codeplex.com/) and Extended WPF Toolkit sources (http://wpftoolkit.codeplex.com)

4.2. XMC

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

3.4 Features

1. OPTIGA™ Trust X1 Security Chip Software

   a. Infineon I2C protocol v1.65 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage
   d. Life cycle management
   e. Cryptographic functionalities for Secure Communication - DTLS-Client [Mutual Authentication] and Encrypted Communication
   f. USB Type-C™ supporting commands
   g. Cryptographic ToolBox commands to perform cryptographic operations like hash generation (HASH), signature calculation and verification (SIGN/VERIFY), Shared secret agreement (ECDH) and derivation of keys.

2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.65 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Secure Communication - DTLS-Client [Mutual Authentication]
   d. Encrypt communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
   f. Cryptographic Toolbox commands
3. OPTIGA™ Trust X PC Software
   a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Join customer PKI domain
   d. Cryptographic Toolbox commands

3.5 Fixes

None

3.6 Enhancements

1. The IFX I2C implementation on OPTIGA™ Trust X1 host library is enhanced to support the asynchronous behaviour with I2C multislave support.
2. Added platform abstraction layer (pal) and optiga comms layer (optiga_comms).
3. Restructured the host library folder in the package.
4. All the documents in the package are updated.

3.7 Known Issues

1. First un-installation/upgrade of any one of the installed software OPTIGA™ Trust X1 and OPTIGA™ Trust E2 on the same system will not remove few folders from the installed directory.
2. In User Interface Demo, continuous invocation of Join customer PKI Domain or Read General Purpose data use case fails to execute and hangs for few seconds, when the security event counter value of OPTIGA™ Trust X1 is more than 7.
3. In User Interface Demo, after executing the secure communication – DTLS client, the auto update of security event counter (SEC) value in the status bar gets disabled. The auto update of SEC value happens only when the One Way Authentication use case is successfully executed.

3.8 Limitations

1. The below DAVE™ generated files in the package are modified to fix the issues seen when integrated with OPTIGA™ TrustX1 host libraries.

a. I2C_MASTER APP (Digital filter feature additionally added)
b. ETH_LWIP APP(In cc.h file “time.h” inclusion is commented)
c. TIMER APP (Typecasting in timer.c file for fixing the compilation warning in Keil)

Hence, if the DAVE™ project is re-generated, the above files in the sample projects gets overwritten with the DAVE™ installed configuration.

The above APPs (applications) will be fixed and released in the next version of DAVE™ public release. Use the APP migration feature of DAVE™ to update these APPs to latest versions.

3.9 Environment

The details of reference environment are explained in Getting Started Guide document.

4 Release to Production for OPTIGA™ Trust X1 Release v1.40 (Build 1118)

4.1 Product Description

OPTIGA™ Trust X1 V1.40 / Build 1118 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 X1 V1.40 / Build 1118 is released as Release Candidate Release. 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 X1 security chip with software build v1.40.1118
2. Setup.zip containing Setup.exe which installs the following Software and Documentation

    2.1. PC

        2.1.1. Bin

        2.1.2. Documentation

            2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.25

            2.1.2.2. API Documentation v1.40.1118

        2.1.3. Source

            2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library and User Interface sources

            2.1.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)

    2.2. XMC

        2.2.1. Bin

        2.2.2. Documentation

            2.2.2.1. OPTIGA™ Trust X XMC Application Notes v1.45

            2.2.2.2. API Documentation v1.40.1118

        2.2.3. Source

            2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources

            2.2.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)

    2.3. DemoUI

        2.3.1. Contains the binaries to run the User interface Demo

2.4. Documentation

2.4.1. OPTIGA™ Trust X Datasheet Revision v2.1

2.4.2. OPTIGA™ Trust X Getting Started Guide v1.4

2.4.3. IFX I2C Protocol Spec v1.65

2.4.4. OPTIGA™ Trust X Solution Reference Manual v1.32

2.4.5. OPTIGA™ Trust X Release Notes v1.40

2.4.6. OPTIGA™ Trust X Keys and Certificates v1.2

2.4.7. OPTIGA™ Trust X License Information

2.4.8. OPTIGA™ Trust X User Interface Manual v1.12

2.5. CACertificates

2.5.1. Contains Certificates required for execution of use cases

2.6. Test Server

2.6.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.5 with OPTIGA™ Trust X SLS 32AIA020X2 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. PC

4.1.1. User Interface utilizing MVVM Light (https://mvvmlight.codeplex.com/) and Extended WPF Toolkit sources (http://wpftoolkit.codeplex.com)

4.2. XMC

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

4.4 Features

1. OPTIGA™ Trust X1 Security Chip Software
   a. Infineon I2C protocol v1.65 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage
   d. Life cycle management

   e. Cryptographic functionalities for Secure Communication - DTLS-Client [Mutual Authentication] and Encrypted Communication
   f. USB Type-C™ supporting commands
   g. Cryptographic ToolBox commands to perform cryptographic operations like hash generation (HASH), signature calculation and verification (SIGN/VERIFY), Shared secret agreement (ECDH) and derivation of keys.
2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.65 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Secure Communication - DTLS-Client [Mutual Authentication]
   d. Encrypt communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
   f. Cryptographic Toolbox commands
3. OPTIGA™ Trust X PC Software
   a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Join customer PKI domain

4.5 Fixes

1. Fixed following issues in OPTIGA™ Trust X1 Demo User Interface,
   a. It doesn't update when security event counter value is greater than zero, while executing Write General Purpose Use case for specific data objects (Current limitation, Life cycle state Application, and Life cycle state Global).
   b. Reading of certificate greater than 1024 bytes failing in OneWayAuthentication usecase
   c. No warning message was prompted while user closes UI demo user interface when status shows Connected to OPTIGA™ Trust X1.
2. Fixed following documents,
   a. OPTIGA™ Trust X1 Getting Started Guide.
   b. OPTIGA™ Trust X1 Demo User Interface Manual.

4.6 Enhancements

1. Updated OPTIGA™ Trust X1 Keys and Certificates document for production CA certificates details.
2. OPTIGA™ Trust X1 security chip data store changes
   a. To enable personalization for additional private keys.
   b. To enable write option for the Infineon Private Key and Public key certificate slots.

4.7 Known Issues

1. First un-installation of any one of the installed software OPTIGA™ Trust X1 and OPTIGA™ Trust E2 on the same system will not remove few folders from the installed directory.

4.8 Limitations

None

4.9 Environment

The details of reference environment are explained in Getting Started Guide document.

5 Release Candidate Release v1.30 (Build 1112)

5.1 Product Description

OPTIGA™ Trust X1 V1.3 / Build 1112 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 X1 V1.3 / Build 1112 is released as Release Candidate Release. 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 X1 security chip with software build v1.30.1112
2. Setup.zip containing Setup.exe which installs the following Software and Documentation
    - 2.1. PC
        - 2.1.1. Bin
        - 2.1.2. Documentation
            - 2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.25
            - 2.1.2.2. API Documentation v1.30.1112
        - 2.1.3. Source
            - 2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library and User Interface sources
            - 2.1.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
    - 2.2. XMC
        - 2.2.1. Bin
        - 2.2.2. Documentation
            - 2.2.2.1. OPTIGA™ Trust X XMC Application Notes v1.45
            - 2.2.2.2. API Documentation v1.30.1112
        - 2.2.3. Source
            - 2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources
            - 2.2.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
    - 2.3. DemoUI
        - 2.3.1. Contains the binaries to run the User interface Demo

2.4. Documentation

2.4.1. OPTIGA™ Trust X Datasheet Revision v2.1

2.4.2. OPTIGA™ Trust X Getting Started Guide v1.3

2.4.3. IFX I2C Protocol Spec v1.65

2.4.4. OPTIGA™ Trust X Solution Reference Manual v1.32

2.4.5. OPTIGA™ Trust X Release Notes v1.30

2.4.6. OPTIGA™ Trust X Keys and Certificates v1.1

2.4.7. OPTIGA™ Trust X License Information

2.4.8. OPTIGA™ Trust X User Interface Manual v1.11

2.5. CACertificates

2.5.1. Contains Certificates required for execution of use cases

2.6. Test Server

2.6.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.5 with OPTIGA™ Trust X SLS 32AIA020X2 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. PC

4.1.1. User Interface utilizing MVVM Light (https://mvvmlight.codeplex.com/) and Extended WPF Toolkit sources (http://wpftoolkit.codeplex.com)

4.2. XMC

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

5.4 Features

1. OPTIGA™ Trust X1 Security Chip Software
   a. Infineon I2C protocol v1.65 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage
   d. Life cycle management

   e. Cryptographic functionalities for Secure Communication - DTLS-Client [Mutual Authentication] and Encrypted Communication
   f. USB Type-C™ supporting commands
   g. Cryptographic ToolBox commands to perform cryptographic operations like hash generation (HASH), signature calculation and verification (SIGN/VERIFY), Shared secret agreement (ECDH) and derivation of keys.
2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.65 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Secure Communication - DTLS-Client [Mutual Authentication]
   d. Encrypt communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
   f. Cryptographic Toolbox commands
3. OPTIGA™ Trust X PC Software
   a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Join customer PKI domain

5.5 Fixes

1. Fixed issue in OPTIGA™ Trust X1 demo user interface such that at any point of time, both OPTIGA™ Trust X1 and OPTIGA™ Trust E demo user interface instances can be opened.
2. Fixed heap memory value in OPTIGA_Trust_X_ServiceApplication project settings, so that XMC sample continues its execution after mutual authentication use case is completed.

5.6 Enhancements

1. Updated the Derive key Cryptographic Toolbox command in OPTIGA™ Trust X1 Security Chip Software to take the shared secret from the data object or session context.
2. Updated OPTIGA™ Trust X Solution Reference Manual

5.7 Known Issues

1. First un-installation of any one of the installed software OPTIGA™ Trust X1 and OPTIGA™ Trust E2 on the same system will not remove few folders from the installed directory.
2. The OPTIGA™ Trust X1 demo user interface does not update, when the security event counter is greater than zero while executing Write General Purpose Use case for specific data objects (Current limitation, Life cycle state Application, and Life cycle state Global).

5.8 Limitations

None

5.9 Environment

The details of reference environment are explained in Getting Started Guide document.

6 Release Candidate Release v1.21 (Build 1103)

6.1 Product Description

OPTIGA™ Trust X1 V1.21 / Build 1103 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 X1 V1.21 / Build 1103 is released as Release Candidate 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 X1 security chip with software build v1.2.1048
2. Setup.zip containing Setup.exe which installs the following Software and Documentation
    - 2.1. PC
        - 2.1.1. Bin
        - 2.1.2. Documentation
            - 2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.25
            - 2.1.2.2. API Documentation v1.21.1103
        - 2.1.3. Source
            - 2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library and User Interface sources
            - 2.1.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
    - 2.2. XMC
        - 2.2.1. Bin
        - 2.2.2. Documentation
            - 2.2.2.1. OPTIGA™ Trust X XMC Application Notes v1.45
            - 2.2.2.2. API Documentation v1.21.1103
        - 2.2.3. Source
            - 2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources
            - 2.2.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
    - 2.3. DemoUI
        - 2.3.1. Contains the binaries to run the User interface Demo

2.4. Documentation

2.4.1. OPTIGA™ Trust X Datasheet Revision v2.1

2.4.2. OPTIGA™ Trust X Getting Started Guide v1.3

2.4.3. IFX I2C Protocol Spec v1.65

2.4.4. OPTIGA™ Trust X Solution Reference Manual v1.31

2.4.5. OPTIGA™ Trust X Release Notes v1.21

2.4.6. OPTIGA™ Trust X Keys and Certificates v1.1

2.4.7. OPTIGA™ Trust X License Information

2.4.8. OPTIGA™ Trust X User Interface Manual v1.11

2.5. CACertificates

2.5.1. Contains Certificates required for execution of use cases

2.6. Test Server

2.6.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.5 with OPTIGA™ Trust X SLS 32AIA020X2 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. PC

4.1.1. User Interface utilizing MVVM Light (https://mvvmlight.codeplex.com/) and Extended WPF Toolkit sources (http://wpftoolkit.codeplex.com)

4.2. XMC

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

6.4 Features

1. OPTIGA™ Trust X1 Security Chip Software
   a. Infineon I2C protocol v1.65 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage
   d. Life cycle management

   e. Cryptographic functionalities for Secure Communication - DTLS-Client [Mutual Authentication] and Encrypted Communication
   f. USB Type-C™ supporting commands
   g. Cryptographic ToolBox commands to perform cryptographic operations like hash generation (HASH), signature calculation and verification (SIGN/VERIFY), Shared secret agreement (ECDH) and derivation of keys.
2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.65 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Secure Communication - DTLS-Client [Mutual Authentication]
   d. Encrypt communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
   f. Cryptographic Toolbox commands
3. OPTIGA™ Trust X PC Software
   a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Join customer PKI domain

6.5 Fixes

1. Updates to the following documentation
   a. OPTIGA™ Trust X Release Notes
   b. OPTIGA™ Trust X Solution Reference Manual
   c. OPTIGA™ Trust X XMC Application Notes
   d. OPTIGA™ Trust X PC Application Notes
   e. OPTIGA™ Trust X User Interface Manual

6.6 Enhancements

None

6.7 Known Issues

1. At any point of time, only one instance of OPTIGA™ Trust X1 or OPTIGA™ Trust E demo user interface (DemoUI) can be opened.
2. First un-installation of any one of the installed software OPTIGA™ Trust X1 and OPTIGA™ Trust E2 on the same system will not remove few folders from the installed directory.

6.8 Limitations

None

6.9 Environment

The details of reference environment are explained in Getting Started Guide document.

7 Engineering Sample Release v1.2 (Build 1099)

7.1 Product Description

OPTIGA™ Trust X1 V1.2 / Build 1099 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 X1 V1.2 / Build 1099 is released as 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 X1 security chip with software build v1.2.1048
2. Setup.zip containing Setup.exe which installs the following Software and Documentation
   - 2.1. PC
     - 2.1.1. Bin
     - 2.1.2. Documentation
       - 2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.24
       - 2.1.2.2. API Documentation v1.2.1099
     - 2.1.3. Source
       - 2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library and User Interface sources
       - 2.1.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
   - 2.2. XMC
     - 2.2.1. Bin
     - 2.2.2. Documentation
       - 2.2.2.1. OPTIGA™ Trust X XMC Application Notes v1.44
       - 2.2.2.2. API Documentation v1.2.1099
     - 2.2.3. Source
       - 2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources
       - 2.2.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
   - 2.3. DemoUI

[1] Reliability tests are not covered as part of qualification

2.3.1. Contains the binaries to run the User interface Demo

2.4. Documentation

2.4.1. OPTIGA™ Trust X Datasheet Revision v2.1

2.4.2. OPTIGA™ Trust X Getting Started Guide v1.3

2.4.3. IFX I2C Protocol Spec v1.65

2.4.4. OPTIGA™ Trust X Solution Reference Manual v1.30

2.4.5. OPTIGA™ Trust X Release Notes v1.2

2.4.6. OPTIGA™ Trust X Keys and Certificates v1.1

2.4.7. OPTIGA™ Trust X License Information

2.4.8. OPTIGA™ Trust X User Interface Manual v1.1

2.5. CACertificates

2.5.1. Contains Certificates required for execution of use cases

2.6. Test Server

2.6.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.5 with OPTIGA™ Trust X SLS 32AIA020X2 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. PC

4.1.1. User Interface utilizing MVVM Light (https://mvvmlight.codeplex.com/) and Extended WPF Toolkit sources (http://wpftoolkit.codeplex.com)

4.2. XMC

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

7.4 Features

1. OPTIGA™ Trust X1 Security Chip Software
   a. Infineon I2C protocol v1.65 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage

   d. Life cycle management
   e. Cryptographic functionalities for Secure Communication - DTLS-Client [Mutual Authentication] and Encrypted Communication
   f. USB Type-C™ supporting commands
   g. Cryptographic ToolBox commands to perform cryptographic operations like hash generation (HASH), signature calculation and verification (SIGN/VERIFY), Shared secret agreement (ECDH) and derivation of keys.
2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.65 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Secure Communication - DTLS-Client [Mutual Authentication]
   d. Encrypt communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
   f. Cryptographic Toolbox commands
3. OPTIGA™ Trust X PC Software
   a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Join customer PKI domain

7.5 Fixes

None

7.6 Enhancements

1. Cryptographic Toolbox commands support in OPTIGA™ Trust X1 Security Chip Software and in OPTIGA™ Trust X1 XMC4500 Relax Kit v1 Software command library
2. Migration to Infineon I2C protocol specification v1.65

7.7 Known Issues

1. At any point of time, only one instance of OPTIGA™ Trust X1 or OPTIGA™ Trust E demo user interface (DemoUI) can be opened.
2. First un-installation of any one of the installed software OPTIGA™ Trust X1 and OPTIGA™ Trust E2 on the same system will not remove few folders from the installed directory.

7.8 Limitations

None

7.9 Environment

The details of reference environment are explained in Getting Started Guide document.

8 Early Engineering Sample Release v1.1 (Build 732)

8.1 Product Description

OPTIGA™ Trust X1 V1.1 / Build 732 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 and lifecycle management for connected devices.

8.2 Scope of Release

OPTIGA™ Trust X1 V1.1 / Build 732 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 X1 Security Chip with Software build v1.1.715
2. Setup.zip containing Setup.exe which installs the following Software and Documentation
    - 2.1. PC
        - 2.1.1. Bin
        - 2.1.2. Documentation
            - 2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.1
            - 2.1.2.2. API Documentation v1.1.732
        - 2.1.3. Source
            - 2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library sources
            - 2.1.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
    - 2.2. XMC
        - 2.2.1. Bin
        - 2.2.2. Documentation
            - 2.2.2.1. OPTIGA™ Trust X XMC Application Notes v1.1
            - 2.2.2.2. API Documentation v1.1.732
        - 2.2.3. Source
            - 2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources
            - 2.2.3.2. wolfSSL Crypto library v3.10.2 (compiled library and header files)
    - 2.3. Documentation
        - 2.3.1. OPTIGA™ Trust X Datasheet Revision v1.4

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

2.3.2. OPTIGA™ Trust X Getting Started Guide v1.1

2.3.3. IFX I2C Protocol Spec v1.40

2.3.4. OPTIGA™ Trust X Solution Reference Manual v1.25

2.3.5. OPTIGA™ Trust X Release Notes v1.1

2.3.6. OPTIGA™ Trust X Keys and Certificates v1.0

2.3.7. OPTIGA™ Trust X License Information

2.4. CACertificates

2.4.1. Contains Certificates required for execution of use cases

2.5. Test Server

2.5.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.4 with OPTIGA™ Trust X SLS 32AIA020X2 Security Chip

3.3. USB to Micro USB Cable

3.4. LAN Cable

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

4.1. XMC

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

8.4 Features

1. OPTIGA™ Trust X1 Security Chip Software
   a. Infineon I2C protocol v1.40 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage
   d. Life cycle management
   e. Cryptographic functionalities for Mutual Authentication (DTLS-Client) and Protect Communication data
   f. USB Type-C™ supporting commands
2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.40 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Mutual Authentication (DTLS-Client)
   d. Protect communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
3. OPTIGA™ Trust X PC Software

   a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Join customer PKI domain

8.5 Fixes

1. OPTIGA™ Trust X1 security chip software fixed for R & S[1] components used in Signature Verification as part of Server Key Exchange Handshake Message

8.6 Enhancements

1. USB Type-C™ commands support in OPTIGA™ Trust X1 Security Chip Software and in OPTIGA™ Trust X1 XMC4500 Relax Kit v1 Software command library

8.7 Known Issues

1. The GUARD_TIME for OPTIGA™ Trust X1 security chip has not been tested below 100µs

8.8 Limitations

None

8.9 Environment

The details of reference environment are explained in Getting Started Guide document.

[1] Refer to FIPS 186-3 from NIST for more details

9 Early Engineering Sample Release v1.0 (Build 596)

9.1 Product Description

OPTIGA™ Trust X1 V1.0 / Build 596 is an Embedded Security Solution covering use cases to protect the authenticity, integrity and confidentiality in your device: mutual authentication, secure communication, data store protection and lifecycle management for Connected Devices.

9.2 Scope of release

OPTIGA™ Trust X1 V1.0 / Build 596 is released as Early Engineering Sample Release. The Product is qualified[1] by Infineon with complete documentation describing all features as stated below.

9.3 Contents of the Evaluation Kit

1. OPTIGA™ Trust X1 Security Chip with Software build v1.0.510

2. Setup.zip containing Setup.exe which installs the following Software and Documentation

2.1. PC

2.1.1. Bin

2.1.2. Documentation

2.1.2.1. OPTIGA™ Trust X PC Application Notes v1.0

2.1.2.2. API Documentation v1.0.596

2.1.3. Source

2.1.3.1. OPTIGA™ Trust X Command, Integration & PKI Library sources

2.1.3.2. wolfSSL Crypto library v3.9.8 (compiled library and header files)

2.2. XMC

2.2.1. Bin

2.2.2. Documentation

2.2.2.1. OPTIGA™ Trust X XMC Application Notes v1.0

2.2.2.2. API Documentation v1.0.596

2.2.3. Source

2.2.3.1. OPTIGA™ Trust X Command, Integration and OCP Library sources

2.2.3.2. wolfSSL Crypto library v3.9.8 (compiled library and header files)

2.3. Documentation

2.3.1. OPTIGA™ Trust X Integration Guide Revision 1.7

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

2.3.2. OPTIGA™ Trust X Product Brief (Nov-2016)

2.3.3. OPTIGA™ Trust X Getting Started Guide v1.0

2.3.4. IFX I2C Protocol Spec v1.40

2.3.5. OPTIGA™ Trust X Solution Reference Manual v1.0

2.3.6. OPTIGA™ Trust X Release Notes v1.0

2.3.7. OPTIGA™ Trust X Keys and Certificates v1.0

2.3.8. OPTIGA™ Trust X License Information

2.4. CACertificates

2.4.1. Contains Certificates required for execution of use cases

2.5. Test Server

2.5.1. Contains all relevant test keys and certificates required for DTLS server and DTLS Test Server

3. Hardware

3.1. XMC4500 Relax Kit V1

3.2. Extension Board v2.4 with OPTIGA™ Trust X SLS 32AIA020X2 Security Chip

3.3. USB to Micro USB Cable

3.4. LAN Cable

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

4.1. XMC

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

9.4 Features

1. OPTIGA™ Trust X1 Security Chip Software
   a. Infineon I2C protocol v1.40 based communication
   b. Signature generation based on (ECC NIST P256 / SHA256)
   c. Configurable protected data storage
   d. Life cycle management
   e. Cryptographic functionalities for Mutual Authentication (DTLS-Client) and Protect Communication data
2. OPTIGA™ Trust X XMC4500 Relax Kit v1 Software
   a. Infineon I2C Protocol v1.40 based communication
   b. One Way Authentication using Infineon Certificate or Customer Certificate
   c. Mutual Authentication (DTLS-Client)
   d. Protect communication data using security chip
   e. Transparent channel to communicate from PC to OPTIGA™ Trust X1 security chip
3. OPTIGA™ Trust X PC Software

a. Transparent channel to communicate to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit v1
b. One Way Authentication using Infineon Certificate or Customer Certificate
c. Join customer PKI domain

9.5 Fixes

Not Applicable as it's the Initial Release

9.6 Enhancements

Not Applicable as it's the Initial Release

9.7 Known Issues

1. The GUARD_TIME for OPTIGA™ Trust X1 security chip has not been tested below 100µs

9.8 Limitations

1. OPTIGA™ Trust X1 security chip software accepts only 32 bytes for R & S components used in Signature Verification as part of Server Key Exchange Handshake Message

9.9 Environment

The details of reference environment are explained in Getting Started Guide document.

Edition 2019-02-28

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@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.