OPTIGA™ Trust X1

PC Application Notes

About this document

Scope and purpose

The scope of this document is to describe the architecture and usage of OPTIGA™ Trust X1 PC Library implementation

Intended audience

This document is intended for any customer who wants to integrate the libraries into their environment for the Authentication features provided by OPTIGA™ Trust X1 security chip.

Table of Contents

About this document **1**
Table of Contents **2**
1 Introduction **4**
1.1 Out of scope 4
1.2 References 4
1.3 Abbreviations 4
1.4 Reference Platform 4
2 System Overview **5**
3 OPTIGA™ Trust X1 Library Architecture **6**
3.1 Sample 6
3.2 Integration Library 6
3.3 Crypto Lib Wrapper 6
3.4 Crypto Library 6
3.5 PKI Library 7
3.6 Command Library 7
3.7 Transparent Channel 7
3.8 Host Protocol 7
3.9 Communication APIs 7
3.10 UDP/IP 7
4 PC Directory Structure **8**
4.1 Source 8
4.1.1 CmdLib 8
4.1.2 IntLib 8
4.1.3 CryptoLib 8
4.1.4 Transparent Channel 8
4.1.5 OCPRemote Procedure Call 9
4.1.6 PKILib 9
4.1.7 Project 9
4.1.8 Include 9
4.1.9 Sample 9
4.2 Bin 9
4.3 Documentation 9
5 Implementation Details **10**
5.1 Integration Library 10
5.1.1 IntLib_Authenticate 10
5.1.2 IntLib_ReadGPData 10
5.1.3 IntLib_WriteGPData 10
5.2 Command Library 10
5.2.1 CmdLib_RegisterItsIO 10
5.2.2 CmdLib_OpenApplication 10
5.2.3 CmdLib_GetDataObject 10
5.2.4 CmdLib_SetDataObject 11
5.2.5 CmdLib_GetRandom 11
5.2.6 CmdLib_GetSignature 11
5.2.7 CmdLib_CalcHash 11
5.2.8 CmdLib_VerifySign 11
5.2.9 CmdLib_GenerateKeyPair 11
5.2.10 CmdLib_CalculateSignature 11
5.2.11 CmdLib_CalculateSharedSecret 11
5.2.12 CmdLib_DeriveKey 11
5.3 Crypto Lib Wrapper 11
5.3.1 CryptoLib_ParseCertificate 11

5.3.2 CryptoLib_VerifySignature 11
5.3.3 CryptoLib_GetRandom 12
5.3.4 CryptoLib_GenerateCertificate 12
5.3.5 CryptoLib_GenKeyPair 12
5.4 PKI Library 12
5.4.1 PKILib_GenKeyPair 12
5.4.2 PKILib_StoreKeyPair 12
5.4.3 PKILib_JoinCustDomain 12
5.4.4 PKILib_GenerateCertificate 12
5.4.5 PKILib_StoreCert 12
5.5 Crypto Library 13
5.6 Transparent Channel 13
5.7 Host Protocol 13
5.8 Communication APIs 13
5.9 UDP/IP 13
6 Use Case Sequence Diagrams 14
6.1 IntLib_Authenticate 14
6.2 IntLib_ReadGPData 15
6.3 IntLib_WriteGPData 16
6.4 Key Pair Generation and Storage (PKILib_GenKeyPair, PKILib_StoreKeyPair) 17
6.5 Join End Customer PKI Domain 18
6.6 Transceive Command over Transparent Channel 20
7 Porting to a Different Platform 21
7.1 Platform Independent 21
7.2 Platform Dependent 21
7.3 Endianness 21
7.4 Feature Selection 21
Revision History 22

1 Introduction

This document describes the architecture and usage of OPTIGA™ Trust X1 PC Library implementation.

1.1 Out of scope

Following are not within the scope of this document:

Design, implementation and usage details of Transparent channel, Host Protocol, Communication APIs and UDP/IP. Refer Figure 2.
Design, implementation and usage details of third party crypto library. Refer Figure 2.
Usage and execution of the binaries provided with the release package.

1.2 References

[1] OPTIGA_Trust_X_PC_API_Documentation.chm, API help file

[2] OPTIGA_Trust_X_Getting_Started_Guide.pdf

[3] OPTIGA_Trust_X_SolutionReferenceManual.pdf

[4] OPTIGA_Trust_X_KeysAndCertificates.pdf

1.3 Abbreviations

Table 1 Abbreviations

Abbreviation	Definition
API	Application Programming Interface
CHM	Microsoft Compiled HTML Help
ESW	Embedded Software
HTML	Hyper Text Mark-up Language
OS	Operating System
PDF	Portable Document Format
TBD	To be defined
USB	Universal Serial Bus
Win32	Windows Native 32bit
DLL	Dynamic Link library
PC	Personal Computer
UDP/IP	User Datagram Protocol/ Internet Protocol

1.4 Reference Platform

The binaries and the sample application provided with this application note are meant for PC running on Windows 7. These binaries may not work as expected if executed on a different platform.

2 System Overview

The system overview is as shown below and it is explained in OPTIGA_Trust_X_Getting_Started_Guide [2]

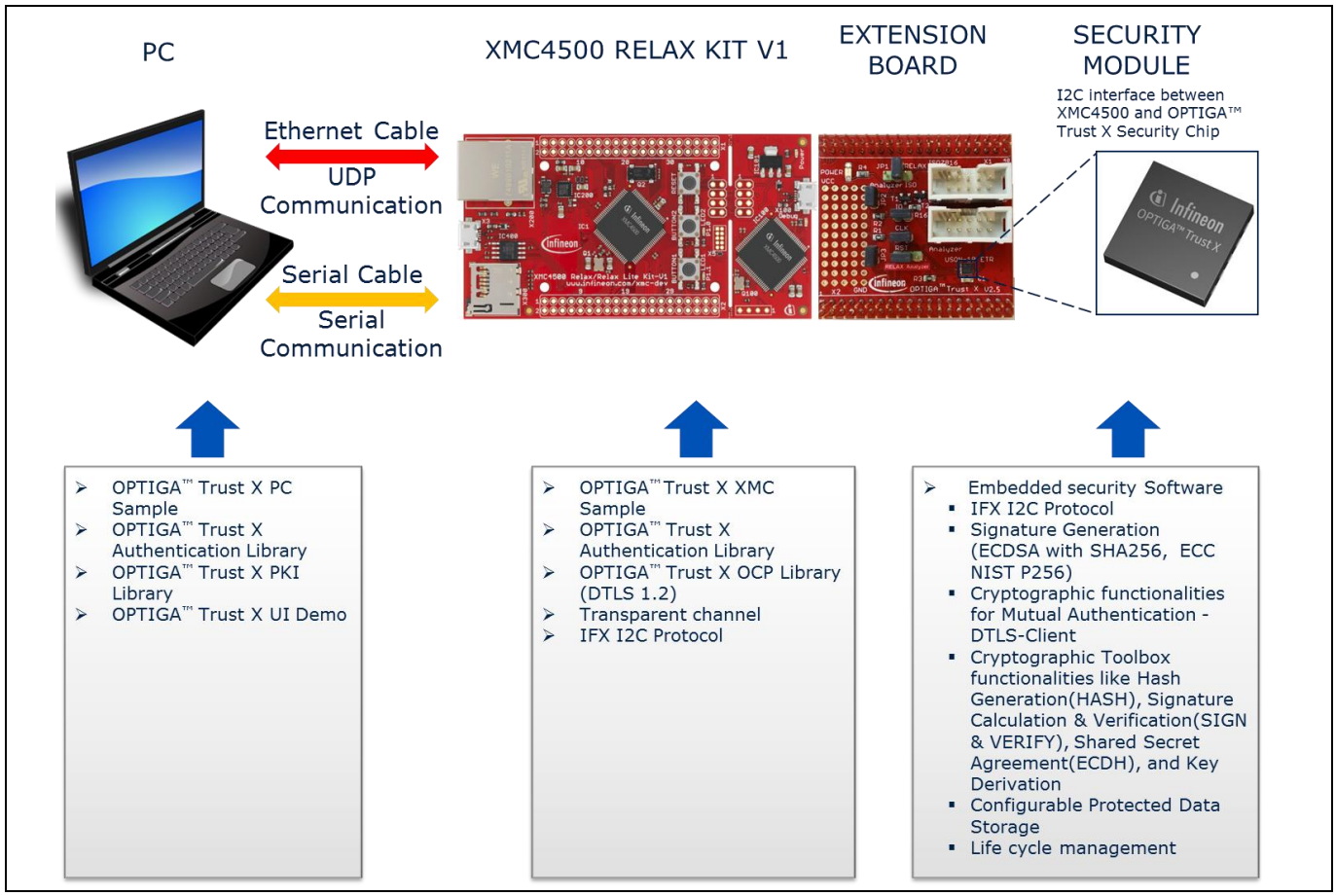

Figure 1 System Overview

3 OPTIGA™ Trust X1 Library Architecture

The architecture of the OPTIGA™ Trust X1 PC Library implementation is as shown below.

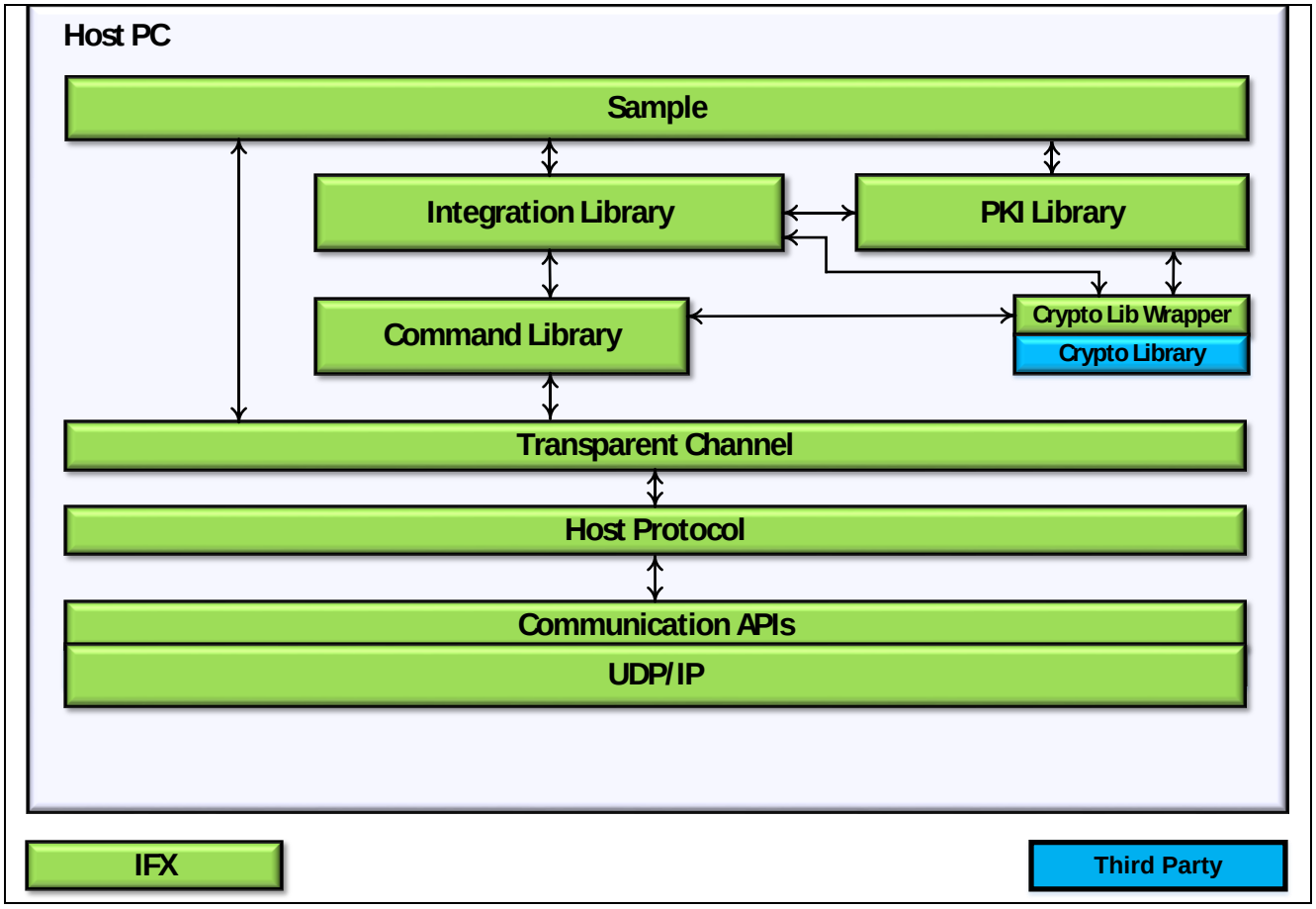

Figure 2 OPTIGA™ Trust X1 Library Architecture

3.1 Sample

This sample application demonstrates usage of One Way Authentication, Cryptographic ToolBox Functionalities, Read/Write General Purpose Data and Join End Customer PKI Domain use cases.

3.2 Integration Library

This library abstracts and provides APIs to perform One Way Authentication, Read/Write General Purpose Data from/to OPTIGA™ Trust X1 security chip.

3.3 Crypto Lib Wrapper

This is a wrapper for third party crypto library and exposes functionality such as Verify Signature, Parse Certificate, Generate Random Number, Generate Key Pair and Generate Certificate.

3.4 Crypto Library

This is a third party software cryptographic library from WolfSSL.

3.5 PKI Library

This library abstracts and provides APIs to generate Certificate Authority NIST P256 key pair, generation of X509 v3 certificates and Join End Customer PKI Domain use case.

3.6 Command Library

This library abstracts and provides APIs to format OPTIGA™ Trust X1 commands for user supplied parameters.

3.7 Transparent Channel

This channel allows a direct communication with OPTIGA™ Trust X1 via XMC 4500 Relax Kit.

3.8 Host Protocol

The host protocol is used to communicate with XMC4500 Relax Kit from PC. The parameters are serialized as per the protocol and transmitted to OPTIGA™ Trust X1 security chip via XMC4500 Relax Kit over UDP. Similarly, the recovered data is de-serialized before passing the response to upper layer.

3.9 Communication APIs

Communication APIs are used by Host protocol to communicate with underlying hardware interface like UDP/IP which is connected to XMC4500 Relax Kit. Basically takes care of seamless transfer of data over the communication channel.

3.10 UDP/IP

This library implements the UDP over IP.

4 PC Directory Structure

The installed directory structure for PC is shown below.

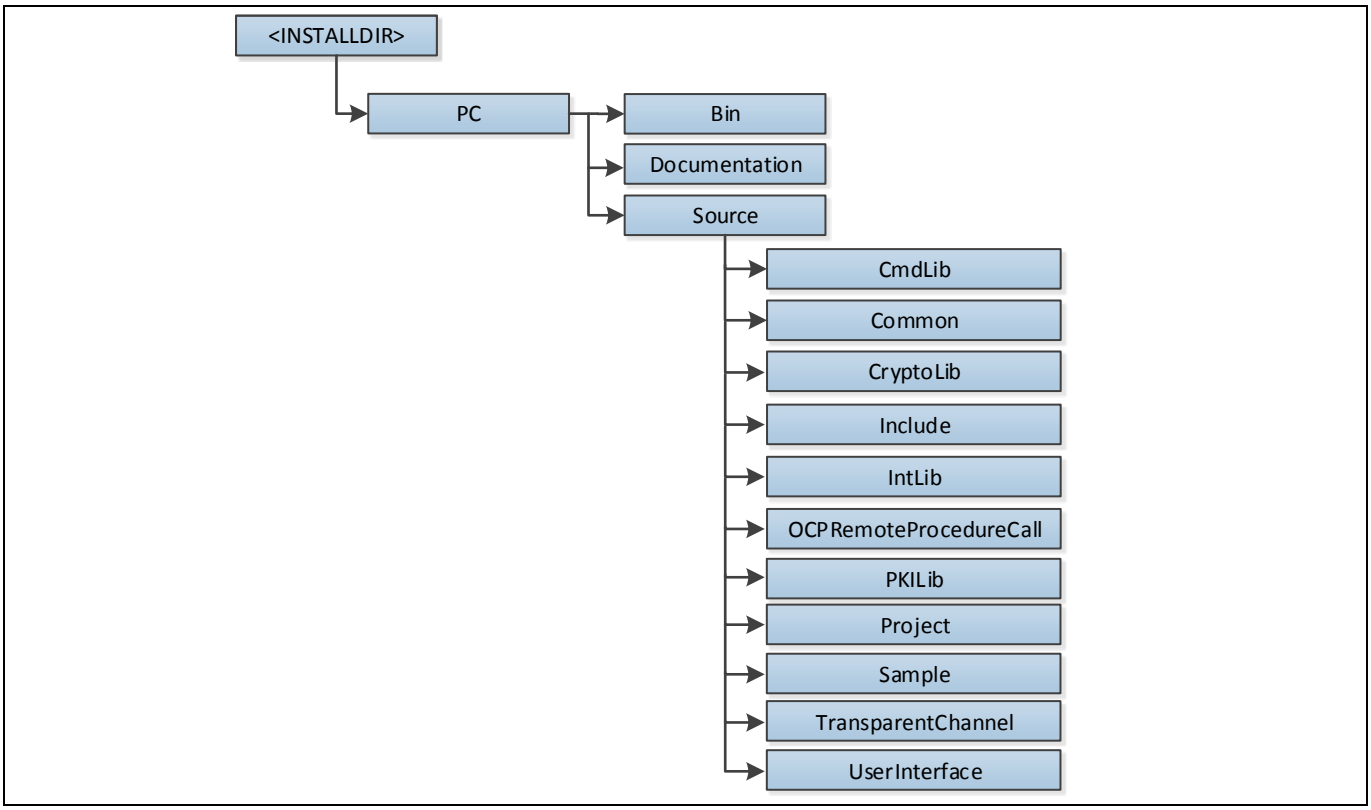

Figure 3 PC Directory Structure

<INSTALLDIR> is the root directory where the software is installed. The following sections explain the content of each subdirectory under the PC directory.

4.1 Source

This directory contains the source code of the OPTIGA™ Trust X1 PC Library implementation.

4.1.1 CmdLib

This directory contains the implementation for Command Library.

4.1.2 IntLib

This directory contains the implementation for Integration Library.

4.1.3 CryptoLib

This directory contains the binary of third party crypto library.

4.1.4 Transparent Channel

This directory contains the source files for direct communication interfaces which include transparent channel, Host protocol and Communication APIs.

4.1.5 OCPRemote Procedure Call

This directory contains the source files for invoking the OCP APIs on XMC4500 from a remote PC using Host protocol and Communication APIs.

4.1.6 PKILib

This directory contains the implementation for PKI Library.

4.1.7 Project

This directory contains the project files for,

1. AuthenticationLibrary – It Includes CommandLib, IntegrationLib and CryptoLib wrapper implementation files.
2. PKILibrary – It Includes PKILibrary, CryptoLib wrapper and Platform dependent implementation files.
3. TransparentChannel – It Includes Transparent channel, Host protocol and communication APIs (via UDP) implementation files.
4. Sample – It includes sample [for Write General Purpose Data, Read General Purpose Data, One Way Authentication, Cryptographic ToolBox functionalities and Join End Customer PKI Domain use cases] implementation files.

4.1.8 Include

This directory contains the header files for OPTIGA™ Trust X1 PC Library. These header files shall be used if the user wants to integrate the binaries of the release package with his environment.

4.1.9 Sample

This directory contains a sample application which demonstrates how to use the OPTIGA™ Trust X1 PC Library.

4.2 Bin

This directory contains the following binary files:

1. OPTIGA_Trust_X_PCSample.exe: This is a pre-built Win32 console application which demonstrates the usage of One Way Authentication, Read/ Write General Purpose Data and Join End Customer PKI Domain use cases.
2. OPTIGA_Trust_X_AuthenticationLibrary.dll: This is a Win32 DLL containing the implementation of Integration library and Command library.
3. OPTIGA_Trust_X_PKILibrary.dll: This is a Win32 DLL containing the implementation of PKI library.
4. OPTIGA_Trust_X_TransparentChannel.dll: This is a Win32 DLL containing the implementation of transparent communication channel.
5. OPTIGA_Trust_X_AuthenticationLibrary.lib: This library contains the implementation of Integration library and Command library.
6. OPTIGA_Trust_X_PKILibrary.lib: This library contains the implementation of PKI library.
7. OPTIGA_Trust_X_TransparentChannel.lib: This library contains the implementation of transparent communication channel.

4.3 Documentation

This directory contains the documentations such as OPTIGA_Trust_X_PC_API_Documentation.chm [1] and OPTIGA_Trust_X_PC_AppNote.

5 Implementation Details

This section explains each of the OPTIGA™ Trust X1 PC Library components.

A reference implementation for explaining the usage of the library components is available within the release package, which is located under Source\Sample.

Note:

1. *The primitive data types that are used within the document are defined in Datatypes.h header file under Source\Include\Common directory.*
2. *For details about the APIs in the reference implementation, refer to [1] which is available under Documentation folder.*

5.1 Integration Library

The source code of this layer is located under Source\IntLib directory. The Integration Library exposes the following APIs to the user. The APIs are defined in the IntegrationLib.h header file which is located under Source\Include\IntLib.

5.1.1 IntLib_Authenticate

Performs One Way Authentication with OPTIGA™ Trust X1 security chip. Refer 6.1 for sequence diagram.

5.1.2 IntLib_ReadGPData

Reads requested data for the specified general purpose data object from OPTIGA™ Trust X1 Security Chip. Refer 6.2 for sequence diagram.

5.1.3 IntLib_WriteGPData

Writes given data to the specified general purpose data object in OPTIGA™ Trust X1 Security Chip. Refer 6.3 for sequence diagram.

5.2 Command Library

The source code of this layer is located under Source\CmdLib directory. The Command Library exposes the following APIs to the user. The APIs are defined in the CommandLib.h header file which is located under Source\Include\CmdLib.

5.2.1 CmdLib_RegisterItsIO

The Command Library is platform independent; hence it requires the communication function to be registered before usage. This API registers the communication function that is required by the command library.

5.2.2 CmdLib_OpenApplication

Opens the application in OPTIGA™ Trust X1 Security Chip.

5.2.3 CmdLib_GetDataObject

Reads the specified data object from OPTIGA™ Trust X1 Security Chip by issuing GetDataObject command.

5.2.4 CmdLib_SetDataObject

Writes to the specified data object in OPTIGA™ Trust X1 Security Chip by issuing SetDataObject command.

5.2.5 CmdLib_GetRandom

Gets the random number generated by OPTIGA™ Trust X1 Security Chip.

5.2.6 CmdLib_GetSignature

Gets the signature generated by OPTIGA™ Trust X1 Security Chip. The message to be signed is provided by the user.

5.2.7 CmdLib_CalcHash

Calculates the hash of input data using OPTIGA™ Trust X1 Security Chip, by issuing CalcHash command.

5.2.8 CmdLib_VerifySign

Verifies the signature of the input digest using OPTIGA™ Trust X1 Security Chip, by issuing VerifySign command.

5.2.9 CmdLib_GenerateKeyPair

Generates a key pair using the OPTIGA™ Trust X1 Security Chip, by issuing GenKeyPair command.

5.2.10 CmdLib_CalculateSignature

Calculates signature of a digest using the OPTIGA™ Trust X1 Security Chip, by issuing CalcSign command.

5.2.11 CmdLib_CalculateSharedSecret

Calculates shared secret using the OPTIGA™ Trust X1 Security Chip, by issuing CalcSSec command.

5.2.12 CmdLib_DeriveKey

Derives session key from a pre-shared/pre-calculated secret using the OPTIGA™ Trust X1 Security Chip, by issuing DeriveKey command.

5.3 Crypto Lib Wrapper

The source code of this layer is located under Source\IntLib directory. The Crypto Lib wrapper exposes the following APIs to the user. The APIs are defined in the CryptoLib.h header file which is located under Source\Include\ IntLib.

5.3.1 CryptoLib_ParseCertificate

Parses an X509v3 certificate passed as a parameter and returns a parsed certificate as a structure. Refer [4] and RFC 5280 for X509 certificate format details.

5.3.2 CryptoLib_VerifySignature

Verifies signature using the public key and message which are passed as parameters.

5.3.3 CryptoLib_GetRandom

Returns the random number generated by the Crypto Library.

5.3.4 CryptoLib_GenerateCertificate

Generates DER encoded X509 v3 certificate.

5.3.5 CryptoLib_GenKeyPair

This is a wrapper on top of the third party crypto library and exposes API to generate ECC key pair based on the NIST curve for the private key length.

5.4 PKI Library

The source code of this layer is located under Source\PKILib directory. The PKI Library Wrapper exposes the following APIs to the user. The APIs are defined in the PKILibrary.h header file which is located under Source\Include\PKILib.

5.4.1 PKILib_GenKeyPair

Generates NIST P256 key pair. Refer 6.4 for sequence diagram.

5.4.2 PKILib_StoreKeyPair

Stores ECC key pair in a removable disk or user specified location. Refer 6.4 for sequence diagram.

5.4.3 PKILib_JoinCustDomain

Performs Join End Customer PKI Domain use cases. Refer 6.5 for sequence diagram.

Note: Following are the limitations with respect to certificate generation feature provided by this library:

1. Only Basic Constraint extension is supported
2. Only following name attributes are supported in the Issuer field:
   a) Country
   b) Common Name
   c) Organization
   d) Organizational Unit Name
3. For Leaf certificate, only Common Name attribute is supported in the Subject field

5.4.4 PKILib_GenerateCertificate

Generates X509 v3 certificate.

OPTIGA_Trust_X_SolutionReferenceManual.pdf [3] describes the limitations of OPTIGA™ Trust X1 with respect to certificate parser and validation and points to be considered while generating Server certificates for Mutual Authentication (DTLS Client).

5.4.5 PKILib_StoreCert

Stores the certificate in a removable disk or user specified location.

5.5 Crypto Library

The binary of crypto library layer is located under Source\ CryptoLib\WolfSSL_Commercial directory. Header files are located under Source\Include\CryptoLib\WolfSSL_Commercial.

5.6 Transparent Channel

The source code of this layer is located under Source\TransparentChannel directory. This allows a direct communication with OPTIGA™ Trust X1 via XMC4500 Relax Kit. Refer 6.6 for sequence diagram.

5.7 Host Protocol

The host protocol is used to communicate with XMC4500 Relax Kit. The parameters are serialized as per the protocol and transmitted to XMC4500 Relax Kit over UDP .This serialized data is processed in XMC4500 Relax Kit and will be sent to OPTIGA™ Trust X1 security chip. Similarly, the received data from OPTIGA™ Trust X1 security chip is de-serialized before passing the response to upper layer. The parameters to be passed to sample are serialized and de-serialized using ASN.1 DER TLV encoding rules.

5.8 Communication APIs

This defines APIs, types and data structures that used by Host protocol to communicate with underlying hardware interface like UDP/IP which is connected to XMC4500 Relax Kit. These API’s are meant for reference purpose only and is used in sample project to demonstrate transparent channel communication. Refer 4.1.4 Transparent Channel section for details on implementation specifics.

5.9 UDP/IP

This file implements the UDP Client APIs. These API’s are meant for reference purpose only and is used in sample project to demonstrate transparent channel communication over Ethernet. Refer 4.1.4 Transparent Channel section for details on implementation specifics.

6 Use Case Sequence Diagrams

6.1 IntLib_Authenticate

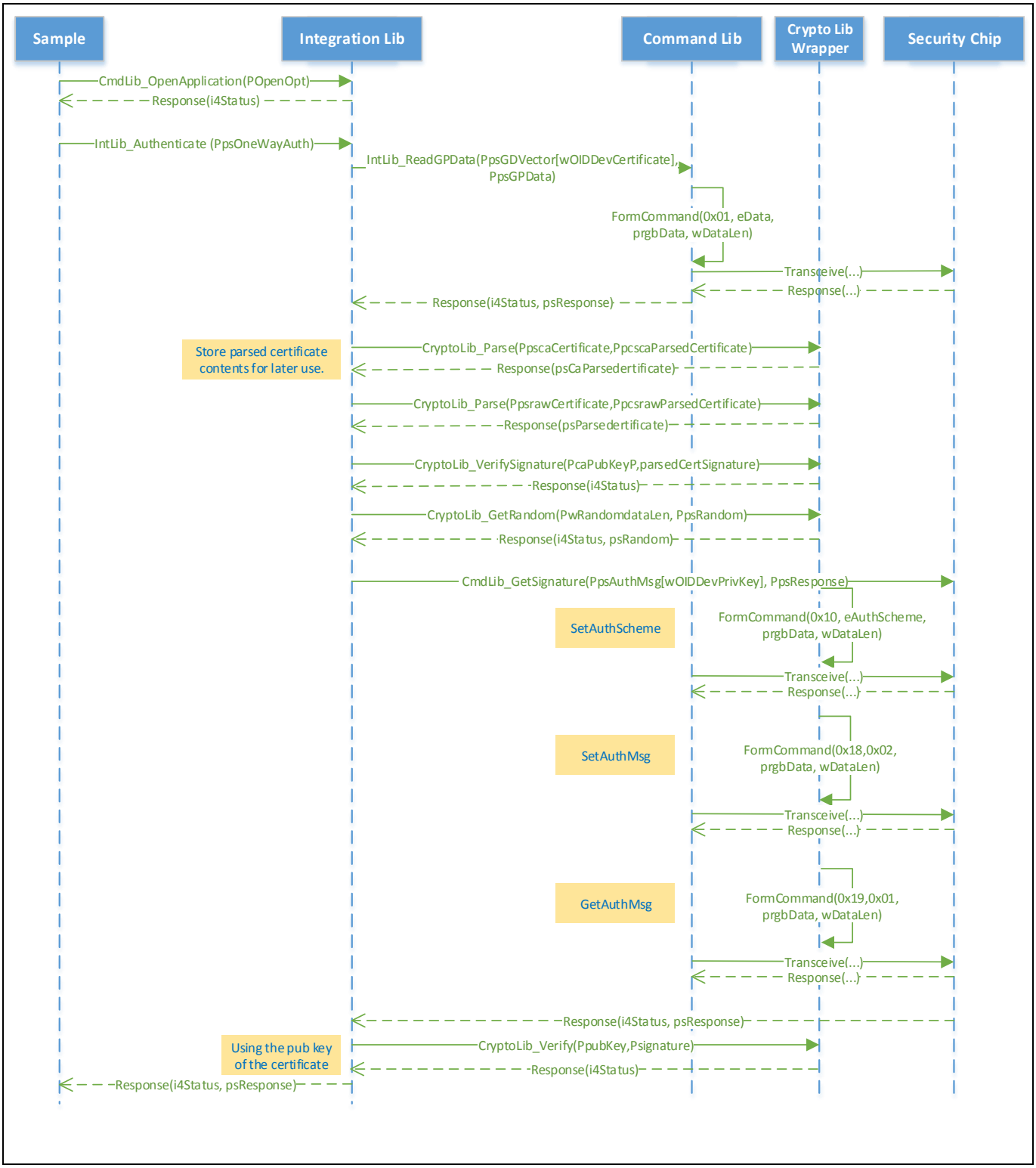

Figure 4 Use Case IntLib_Authenticate

6.2 IntLib_ReadGPData

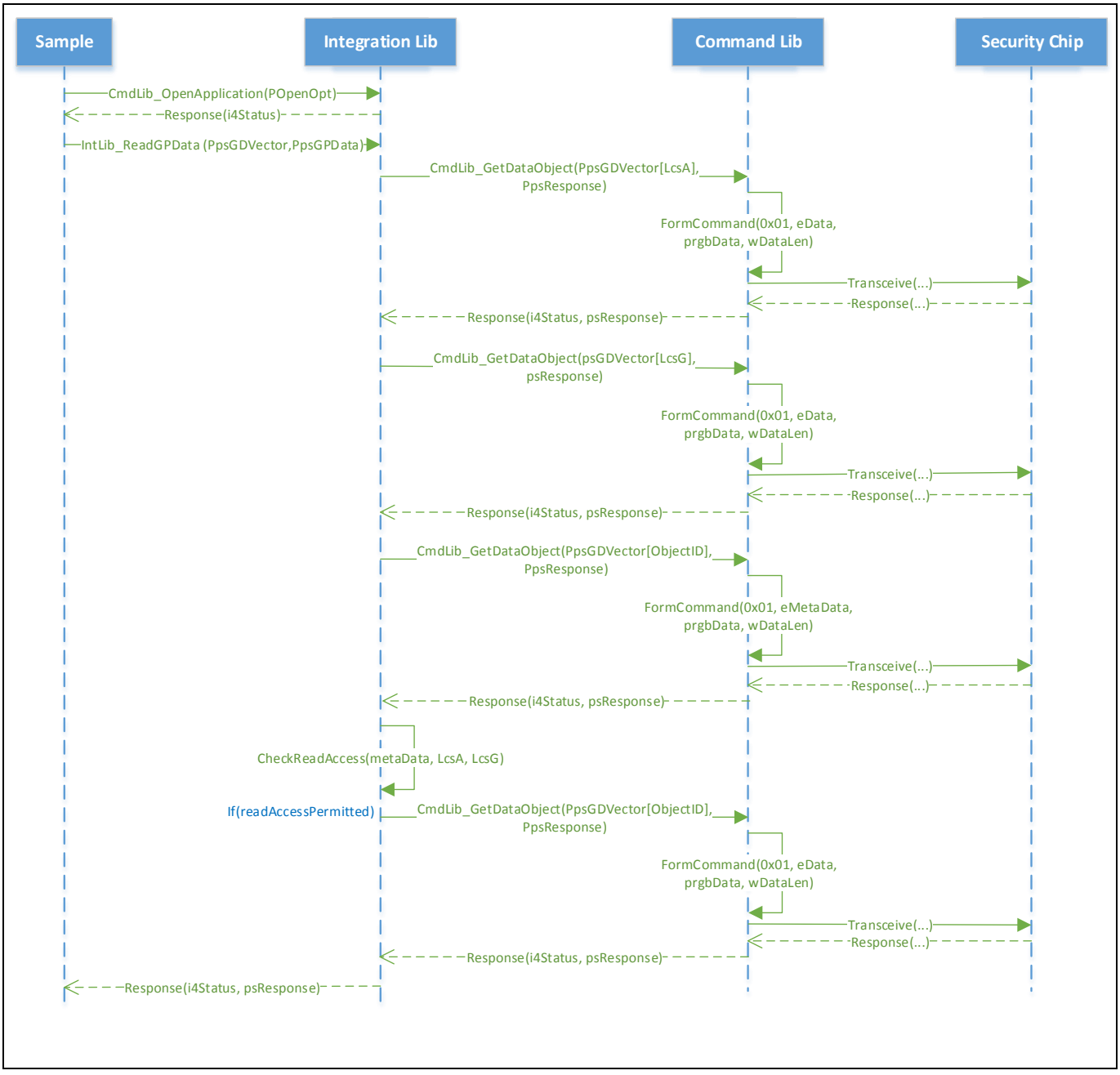

Figure 5 Use Case IntLib_ReadGPData

6.3 IntLib_WriteGPData

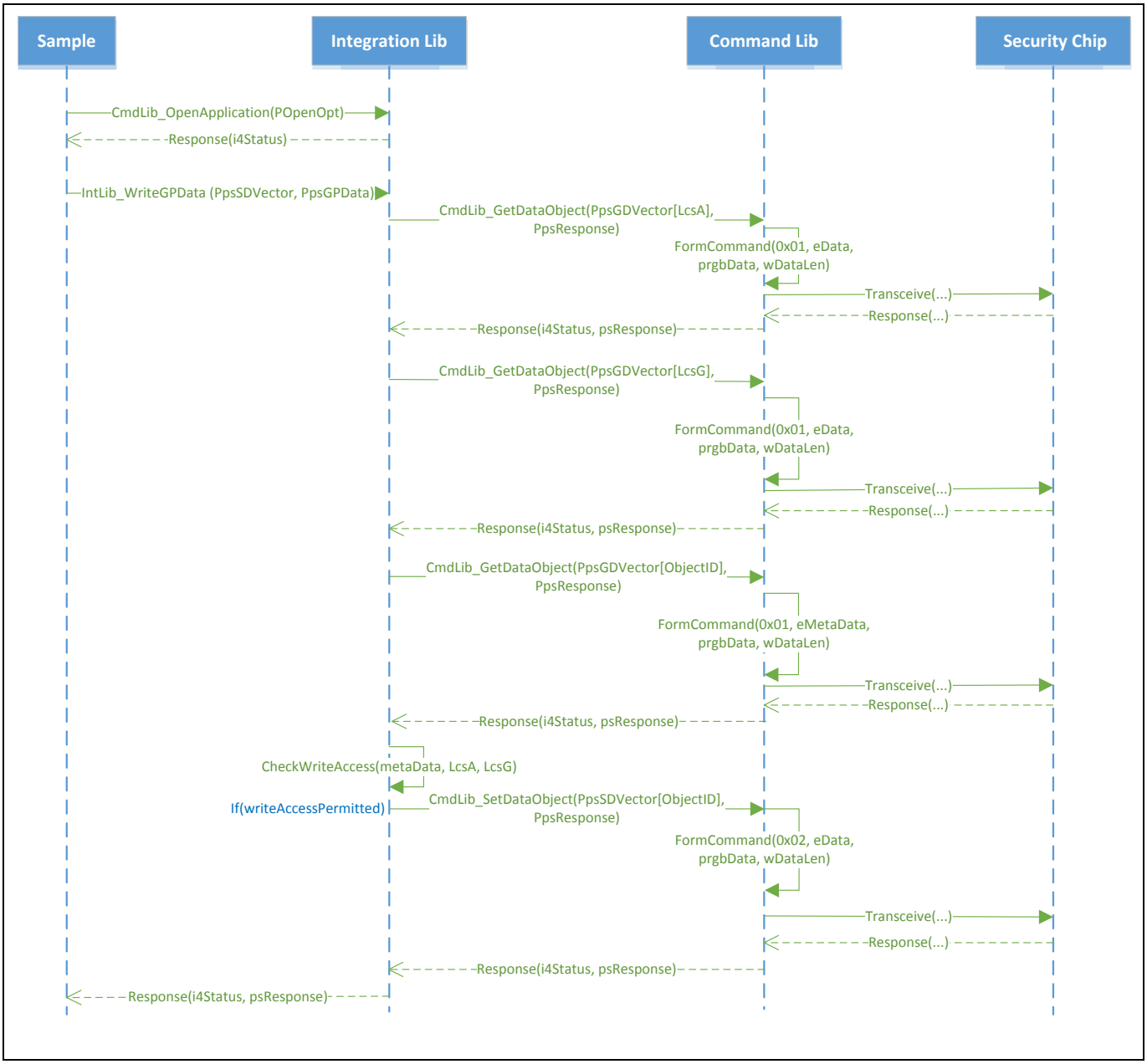

Figure 6 Use Case IntLib_WriteGPData

6.4 Key Pair Generation and Storage (PKILib_GenKeyPair, PKILib_StoreKeyPair)

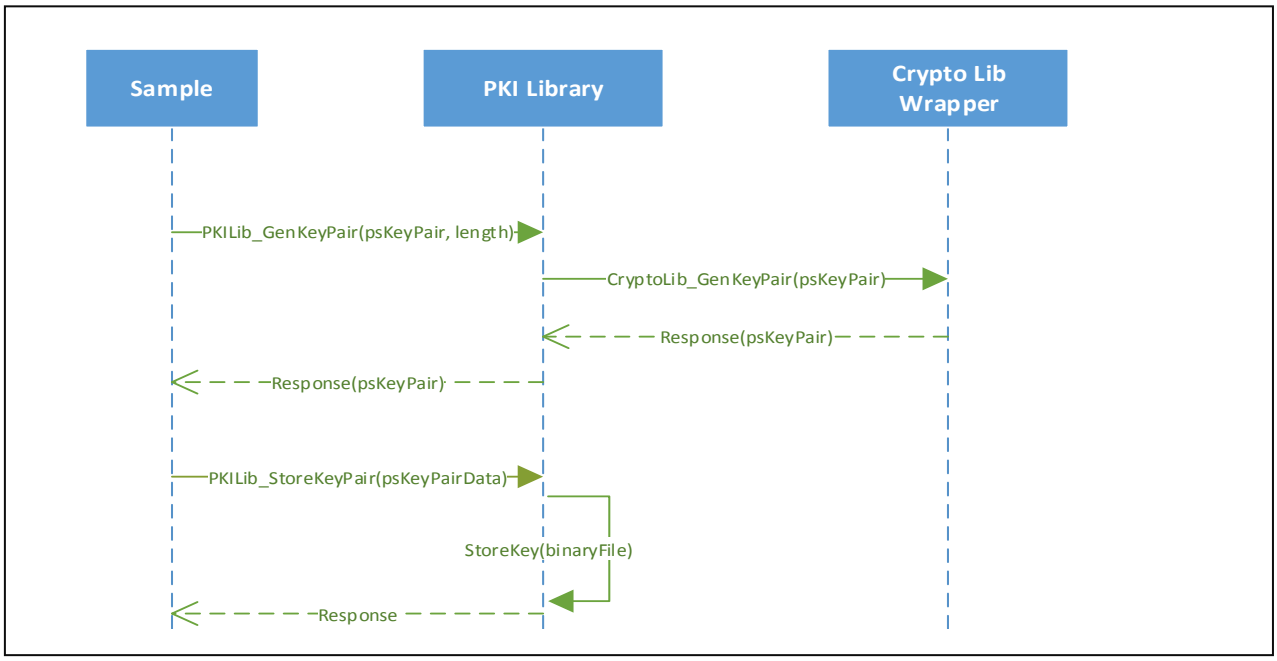

Figure 7 Generate Key Pair and Storage

6.5 Join End Customer PKI Domain

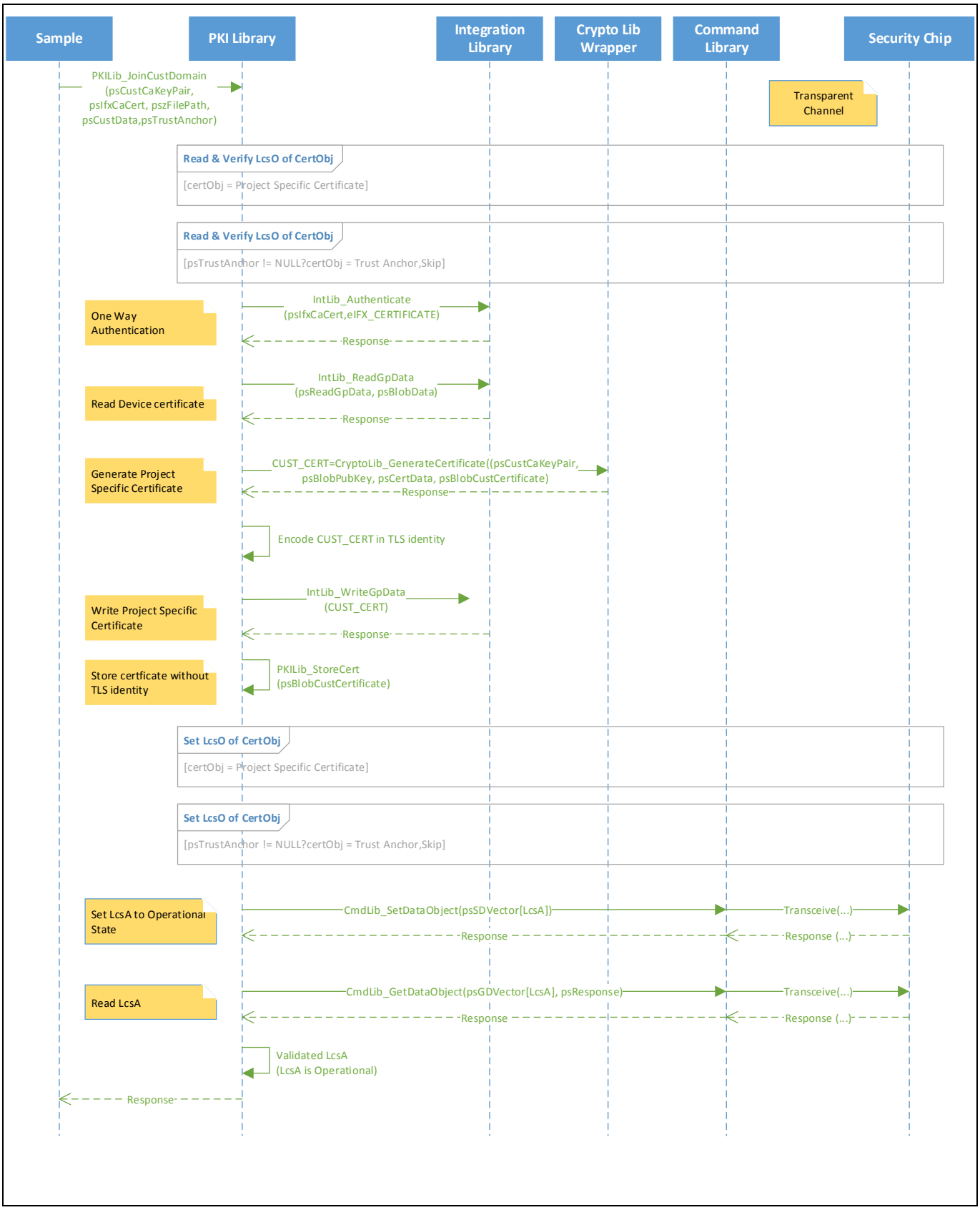

Figure 8 Join End Customer PKI Domain

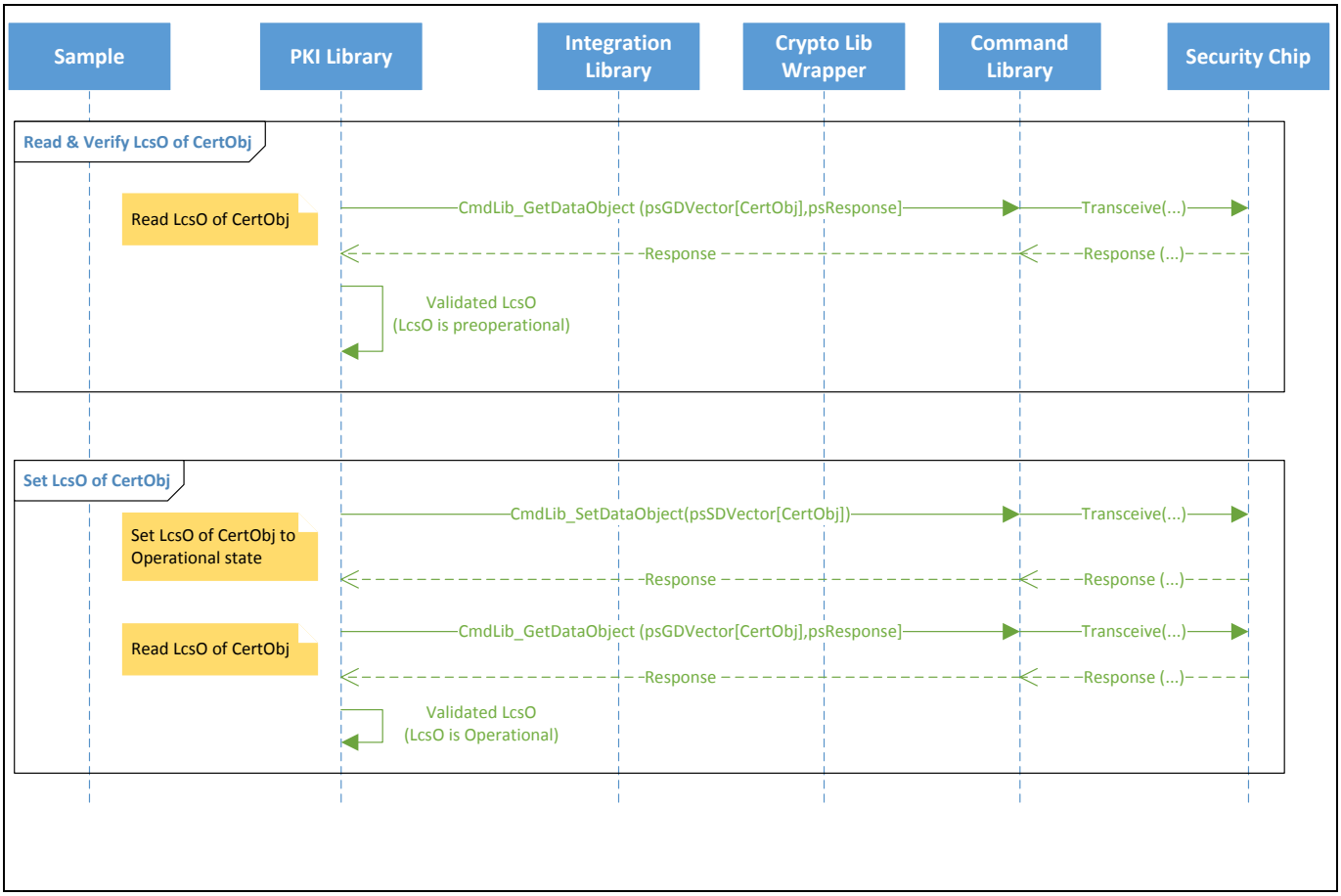

Figure 9 Set and Read & Verify LcsO of object

6.6 Transceive Command over Transparent Channel

This sequence explains how a command is exchanged with the OPTIGA™ Trust X1 over transparent channel.

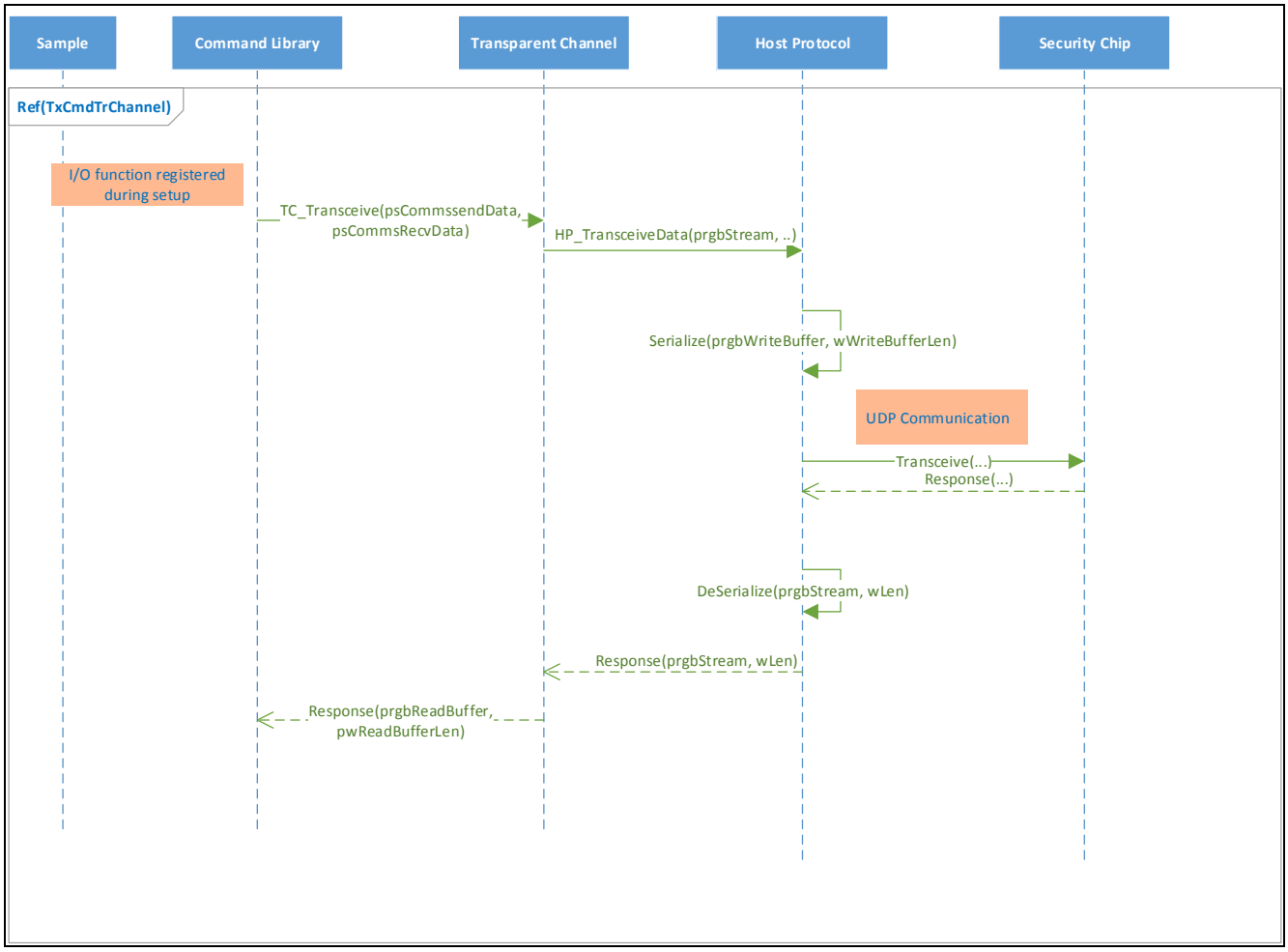

Figure 10 Transceive Command (Transparent Channel)

7 Porting to a Different Platform

7.1 Platform Independent

The following modules are platform independent and do not require porting:

1. Integration Library
2. Command Library
3. Transparent Channel
4. Crypto Lib Wrapper

7.2 Platform Dependent

The following modules are platform dependent and require porting:

1. PKI Library
   1. Timestamp generation for file name which is used by store Key Pair and store certificate.
   2. File operations including writing to file and writing of standard console
   3. Store Key Pair which verifies for removable drive connected to PC
2. Crypto Library
   1. The Crypto Library must be built for the intended platform
   2. The default endianness is little-endian. To change to big-endian, define “WORDS_BIGENDIAN” and build the code

7.3 Endianness

The Authentication and PKI Library is tested on little endian platform

7.4 Feature Selection

By default, all the features such as One Way Authentication, Cryptographic ToolBox and Read/Write General Purpose Data are enabled at compile time.To enable the user to choose specific feature set, the following compile time switches are provided (Refer AuthLibSettings.h in Source\Include\ Common):

1. FEATURE_ONEWAY_AUTH : One Way Authentication and Read/Write General Purpose Data are enabled.
2. FEATURE_TOOLBOX : Cryptographic Toolbox feature is enabled.

Note: Refer AuthLibSettings.h in Source\Include\Common for the feature selection switches.

Revision History

Major changes since the last revision

Version	Description of change	Sections Modified
Revision 1.0, 2016-12-05	Initial Version	All
Revision 1.1, 2017-02-27	CmdLib_CalcHash API added Updated the Join End Customer PKI Domain sequence diagrams.	Section 5.2, 6.5
Revision 1.2, 2017-05-06	Updated the Join End Customer PKI Domain sequence diagrams.	Section 6.5
Revision 1.21, 2017-05-06	CmdLib_VerifySign API added	Section 5.2
Revision 1.22, 2017-05-19	CmdLib_GenerateKeyPair added CmdLib_CalculateSignature added	Section 5.2.9, Section 5.2.10
Revision 1.23, 2017-06-01	CmdLib_DeriveKey CmdLib_CalculateSharedSecret	Section 5.2.11, Section 5.2.12
Revision 1.24, 2017-06-08	Updated CmdLib_GetRandom Updated Intlib_Authenticate	Section 5.2.5, Section 6.1

Edition 2017-06-08
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 contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. 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) with respect to any and all information given in this application note.

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.