

OPTIGA[™] Trust B SLE95250

Evaluation Kit User Guide

About this document

Scope and purpose

This is the User Guide for $OPTIGA^{TM}$ Trust B evaluation kit. It gives the detailed guideline of how to use $OPTIGA^{TM}$ Trust B evaluation kit for demonstration and evaluation purpose.

Intended audience

This document is intended for the engineers who want to evaluate $OPTIGA^{TM}$ Trust B. It can also be used to verify the customer system with $OPTIGA^{TM}$ Trust B integrated.

Table of Contents

About t	his document	1
Table of	f Contents	1
	Hardware board	
2	PC GUI	3
2.1	Search devices on SWI bus	4
2.2	Authentication	
2.3	Non-Volatile Memory	
3	Test external devices	8
Revisio	n History	9



Hardware board

1 Hardware board

OPTIGA[™] Trust B evaluation kit comes with two boards in the kit. The main board with USB interface and a daughter board for external connection. The below picture is when the main board and daughter board is connected.

x201_JP201	RESET_N SHI EXT_SNS P14.4 P14.8 P15.8 HIB IO_0 P3.8		Terrar	
2 3	P0.0		P0.5	
- Cono	PØJE		P0.11	
•	P0.4	1 Martin	P0.0	

On the main board, JP2 is used to enable OPTIGA[™] Trust B device on the main board. On the daughter board, JP201 is used to enable OPTIGA[™] Trust B device on the daughter board. There are two sets of pin header X201 and X202 on the daughter board, which can be used to either connect external OPTIGA[™] Trust B devices or to probe the signal. The rest of the pin headers on the board are mapped to some of the commonly used external signals on the XMC controller.

When the main board is plugged into the USB interface of the computer, a green LED should light up followed by running orange LEDs. That means the firmware in XMC controller is executed properly. If both LEDs cannot be observed, please plug out and plug in the main board to reset the firmare.



2 PC GUI

PC GUI can be downloaded from www.infineon.com/optiga (OPTIGA™ Trust B Evaluation Kit). Upon running the executable file (OPTIGA Trust B.exe), below GUI should be shown on the desktop.

Infineon OPTIGA Trust B Evaluation	Kit	
File Help		
Device Search	Device Unique ID	
SWI Bus Device Search	Not Available Not Available Select Unique I	
Device Search	Select Unique I	
	Enhanced Authenticat	ion
	Non Volatile Memor	y and a second sec
		infineon
Host is connected to PC		



2.1 Search devices on SWI bus

The first step before running authentication or NVM operations is to identify the devices connected to the SWI bus, and then select the device to communicate. This can be achieved by clicking the button "Device Search". After clicking the button, at least one device unique ID should be displayed. The GUI supports maximum of two device unique ID to be displayed.

PTIGA Selection Device Search		Device Unique ID	
SWI Bus	Q	18-2A-07-20-3B-66-00-82-B0-17-03-28	
	Device Search		Select Unique ID

Here is the example of two device unique IDs

Device Search		Device Unique ID	
SWI Bus	Q	00-03-00-01-38-AE-20-A3-02-14-05-33	
	Device Search	© 18-2A-07-20-3B-66-00-82-B0-17-03-28	Select Unique ID

In order to select the device to communicate, simply check the radio button of the corresponding Device Unique ID and click button "Select Unique ID". After this, you should see SLE95250 displayed and "Enhanced Authentication" and "Non-Volatile Memory" button enabled as below picture.



Infineon OPTIGA Trust B Evaluation I	Kit	
File Help		
OPTIGA Selection Device Search SWI Bus Device Search	Device Unique ID © 00-03-00-01-38-AE-20-A3-02-14-05-33 © 18-2A-07-20-38-66-00-82-80-17-03-28 Select Unique ID	
	Enhanced Authentication	SLE95250
	Non Volatile Memory	
		infineon
18-2A-07-20-3B-66-00-82-B0-17-03-28 		Speaker/HP: Mute

Now you are ready to start authentication and NVM operations.

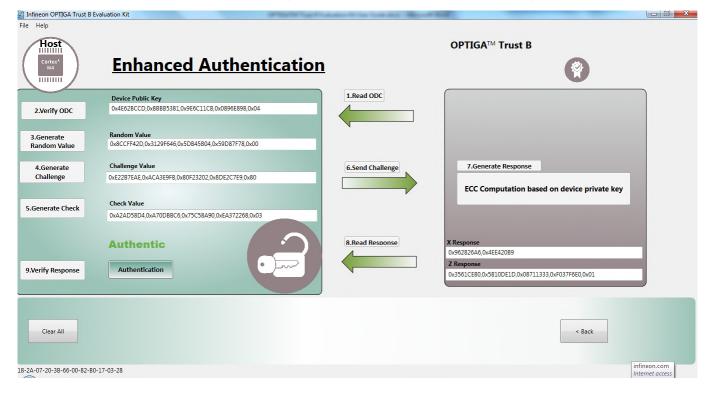
2.2 Authentication

Click "Enhanced Authenticatin button, this brings you to the authentication GUI tab.

Infineon OPTIGA Trust B Ev	aluation Kit	station 10 for Lobolton Manual B		
File Help	Enhanced Authentication		OPTIGA™ Trust B	
2.Verify ODC 3.Generate Random Value	Device Public Key Random Value	1.Read ODC		
4.Generate Challenge	Challenge Value Check Value	6.Send Challenge	7.Generate Response ECC Computation based on device private key	
5.Generate Check 9.Verify Response	Authentication	8.Read Response	X Response Z Response	
Clear Ali 18-2A-07-20-3B-66-00-82-80-	17-03-28		< Back	



Simply click "Authentication" button on the left bottom of the GUI, the complete authentication sequence will be executed and displayed. Actual value of all the algorithm flow can be viewed in the edit box. If the authentication passes, "Authentic" will be printed, otherwise "Couterfeit" will be printed.



Infineon OPTIGA Trust B Evaluation Kit

Host Cortex*	Enhanced Authentication		OPTIGA™ Trust B
	Device Public Key	1.Read ODC	
2.Verify ODC	0x,0x,0x,0x,0x		
3.Generate Random Value	Random Value 0x56A74868,0xD43FB7FF,0x8AF1A528,0x6FD941FC,0x00		
4.Generate	Challenge Value	6.Send Challenge	7.Generate Response
Challenge	0x4078B8DF,0x833F626C,0x22E6C397,0xFC53D1F9,0x94		
5.Generate Check	Check Value 0xFF6D34DC,0x7804741F,0xEA8BED90,0x94B59ACB,0x07	8.Read Response	ECC Computation based on device private key
9.Verify Response	Counterfeit Authentication	8.Read Response	A Response 0x7EC773CA,0x91E85710 Z Response 0x5D266881,0xD835DA84,0x94FE7F86,0x66E8944A,0x80
Clear All			< Back
00-03-00-01-38-AE-20-A3-02	2-14-05-33		



2.3 Non-Volatile Memory

Click Non-Volatile Memory brings you to NVM operation tab. The Unique ID (UID) is displayed with vendor ID and product ID decoded. Current value of life span counter is shown as well. The value of the counter can be decremented once at a time by clicking "Decrease" button.

Infineon OPTIGA Trust B Evaluation Kit		Sector Sector	Contraction 10							
File Help										
\square										Life Span Counter:
	Unique Chip ID:	38	AE	20	A3	02	14	05	33	Actual Value: 79120669
	Vendor ID:	00	03				Product ID:	00	01	Decrease
User NVM										
NVM Data										Read NVM
A										Write NVM
										-
							nfin			
						(Ir	ntin	60	n	< Back
						\ ''				
								-		
00-03-00-01-38-AE-20-A3-02-14-05-33										

NVM read and write operation can be verified by "Read NVM" and "Write NVM" button.

Infineon C	OPTIGA T	rust B Evalu	ation Kit																
le Help																			
	ſ	Ì																Life Span	Counter:
		<u> </u>				U	Inique Chip	ID:	3B	66	00	8:	2	BO	17	03	28	Actual Value	99988
	9	6					Vendor	ID:	18	2A					Product ID:	07	20		Decrease
User NVM]																		
NVM D	ata																		Read NVM
	0	1	2	3	4	5	6	7	8	9	A	в	с	D	Е	F	Dump		
0x0000	00	00	00	00	00	00	00	12	00	00	00	00	00	00	00	00		*	Write NVM
0x0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0x0020	00	00	00	00	00	FF	00	00	00	FF	00	00	00	00	00	00			
0x0030	00	00	00	00	00	00	00	00	31	31	32	33	00	00	00	00	11	.23	
																		Ŧ	
													(in	fin	ec	n	[< Back

NVM read successful



Test external devices

3 Test external devices

External devices can be connected to X201 or X202 on the daughter board. JP201 needs to be shorted and JP2 is recommended to be left open to avoid confusion.

By connecting to X201 or X202, the customer device can be searched by the GUI, proper Unique ID can be displayed, and NVM operation can be verified as well. However authentication test might fail due to mismatch of the key.

In order to test authentication, a proper customer key and curve parameter needs to be loaded. This can be achieved by importing a configuration xml file. The default configuration xml file is located in the GUI folder, named config.xml. Edit the file so that proper customer specific curve parameter and public key is loaded. After editing, under file menu, select "Import Parameters" and select Config.xml in the GUI software folder to load the parameters.





Revision History

Major changes since the last revision

Page or Reference	Description of change
	Initial revision

Trademarks of Infineon Technologies AG

µHVIC™, µIPM™, µPFC™, AU-ConvertIR™, AURIX™, C166™, CanPAK™, CIPOS™, CIPURSE™, CoolDP™, CoolGaN™, COOLIR™, CoolMOS™, CoolSET™, CoolSiC™, DAVE™, DI-POL™, DirectFET™, DrBlade™, EasyPIM™, EconoBRIDGE™, EconoDUAL™, EconoPACK™, EconoPIM™, EiceDRIVER™, eupec™, FCOS™, GaNpowIR™, HEXFET™, HITFET™, HybridPACK™, iMOTION™, IRAM™, ISOFACE™, IsoPACK™, LEDrivIR™, LITIX™, MIPAQ™, ModSTACK™, my-d™, NovalithIC™, OPTIGA™, OptiMOS™, ORIGA™, PowIRaudio™, PowIRStage™, PrimePACK™, PrimeSTACK™, PROFET™, PRO-SIL™, RASIC™, REAL3™, SmartLEWIS™, SOLID FLASH™, SPOC™, StrongIRFET™, SupIRBuck™, TEMPFET™, TRENCHSTOP™, TriCore™, UHVIC™, XHP™, XMC™

Trademarks updated November 2015

Other Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition <2017-01-01> Published by Infineon Technologies AG 81726 Munich, Germany

© 2017 Infineon Technologies AG. All Rights Reserved.

Do you have a question about this document?

Email: erratum@infineon.com

Document reference AppNote Number

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 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.