OPTIGA™ Trust B SLE95250

Evaluation Kit User Guide

About this document

Scope and purpose

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

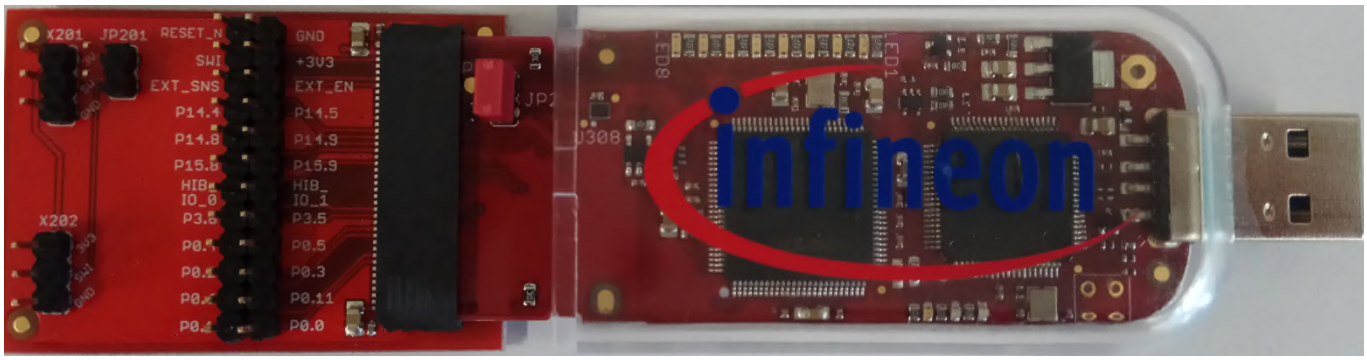
Intended audience

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

Table of Contents

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.

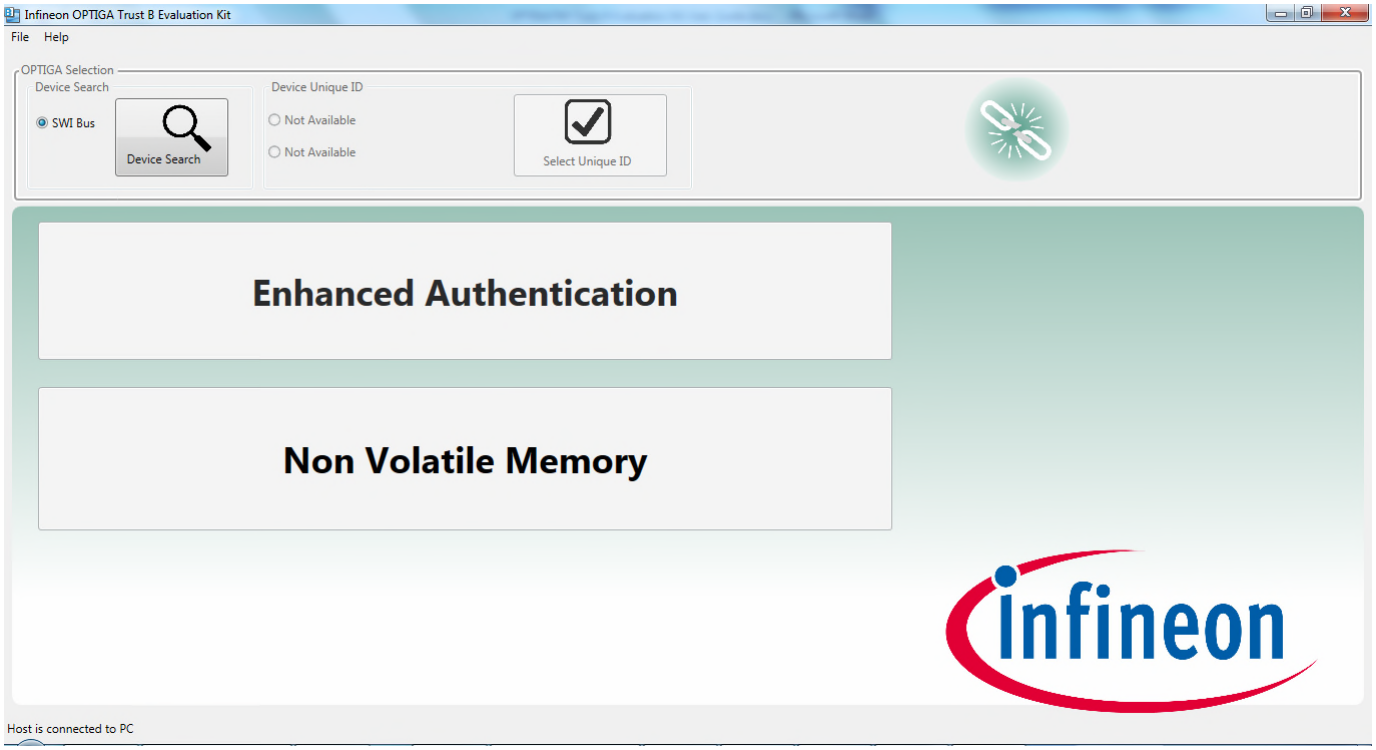


On the main board, JP2 is used to enable OPTIGA™ Trust B device on the main board. On the daughter board, JP201 is used to enable OPTIGA™ Trust B device on the daughter board. There are two sets of pin header X201 and X202 on the daughter board, which can be used to either connect external OPTIGA™ Trust 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

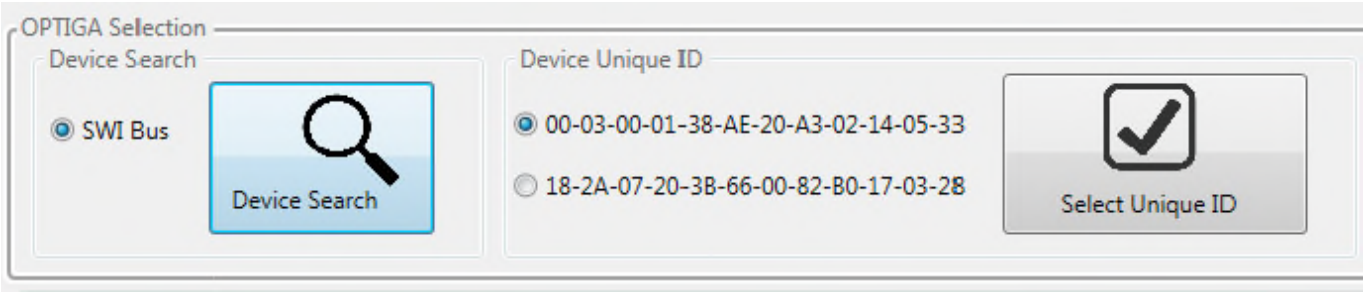
PC GUI can be downloaded from www.infineon.com/optiga (OPTIGA™ Trust B Evaluation Kit). Upon running the executable file (OPTIGA Trust B.exe), below GUI should be shown on the desktop.



2.1 Search devices on SWI bus

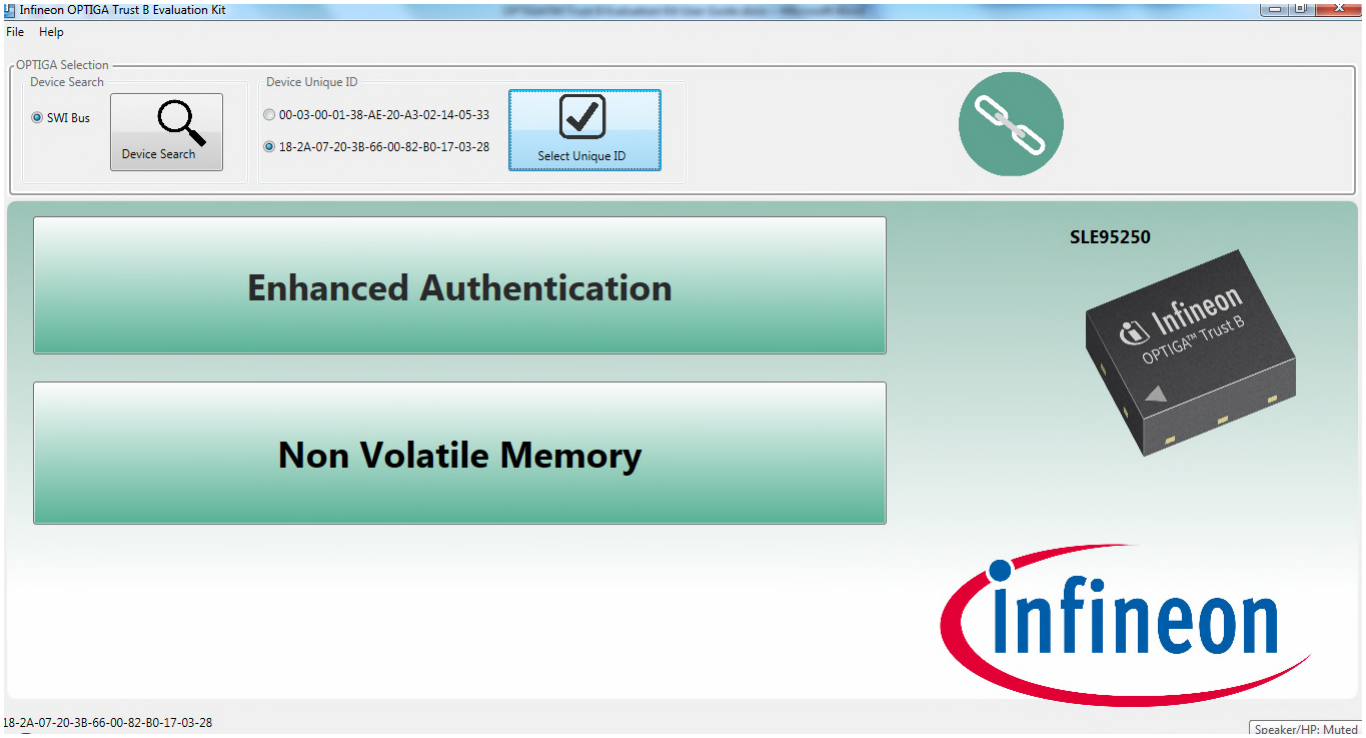
The first step before running authentication or NVM operations is to identify the devices connected to the SWI bus, and then select the device to communicate. This can be achieved by clicking the button “Device Search”. After clicking the button, at least one device unique ID should be displayed. The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

Here is the example of two device unique IDs



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.

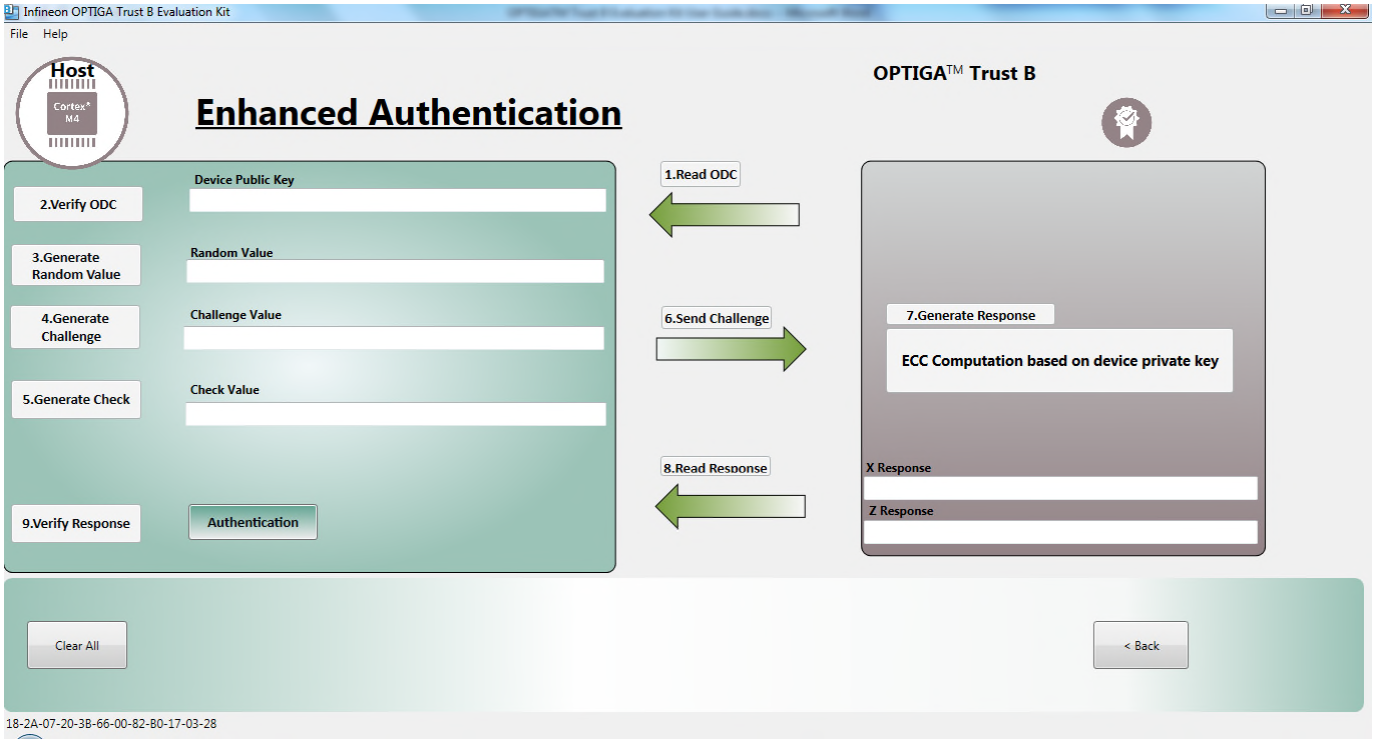
PC GUI



Now you are ready to start authentication and NVM operations.

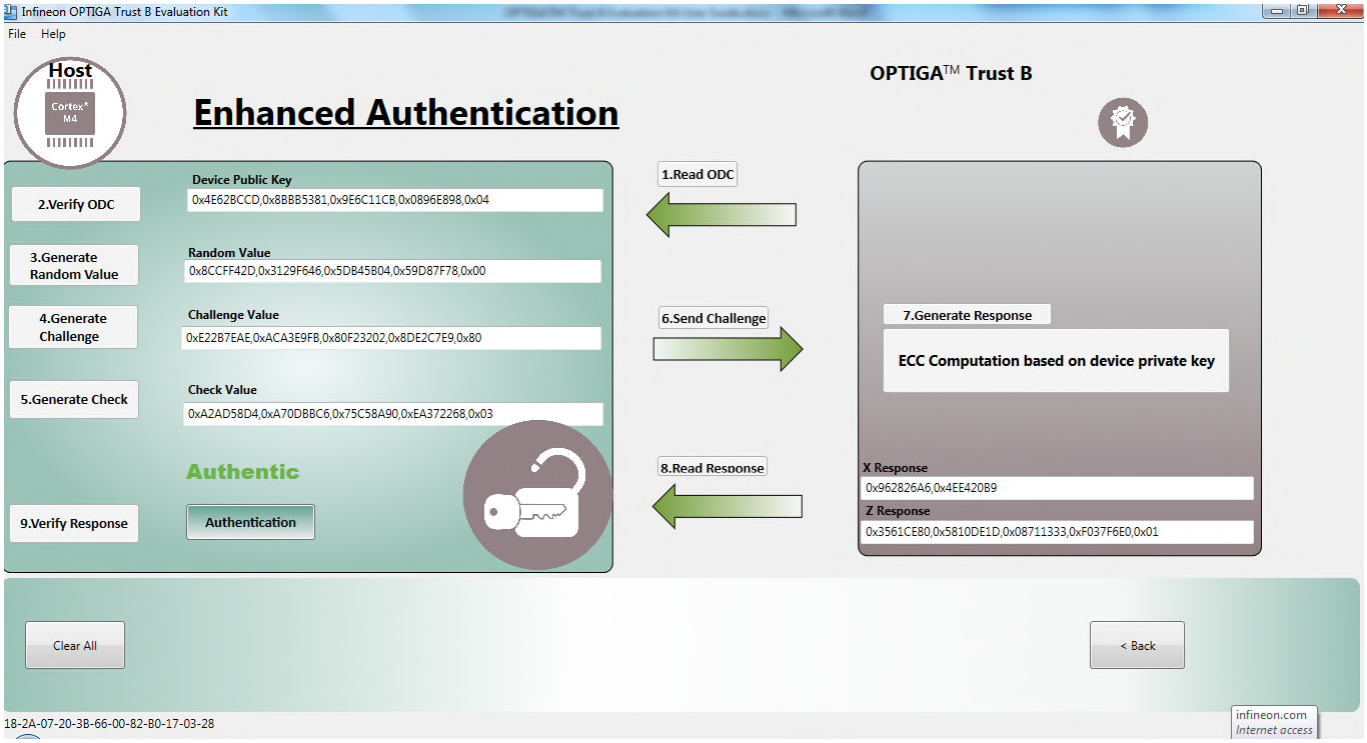
2.2 Authentication

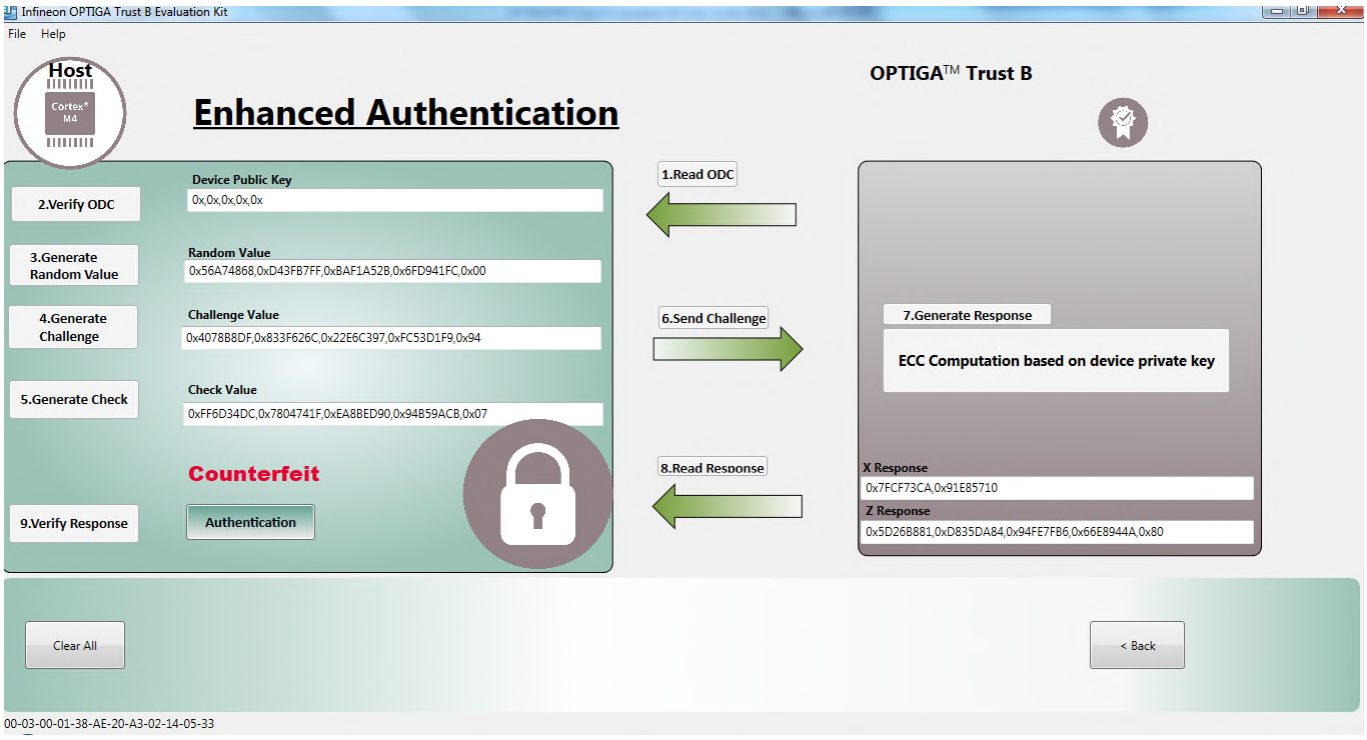
Click “Enhanced Authenticatin button, this brings you to the authentication GUI tab.



PC GUI

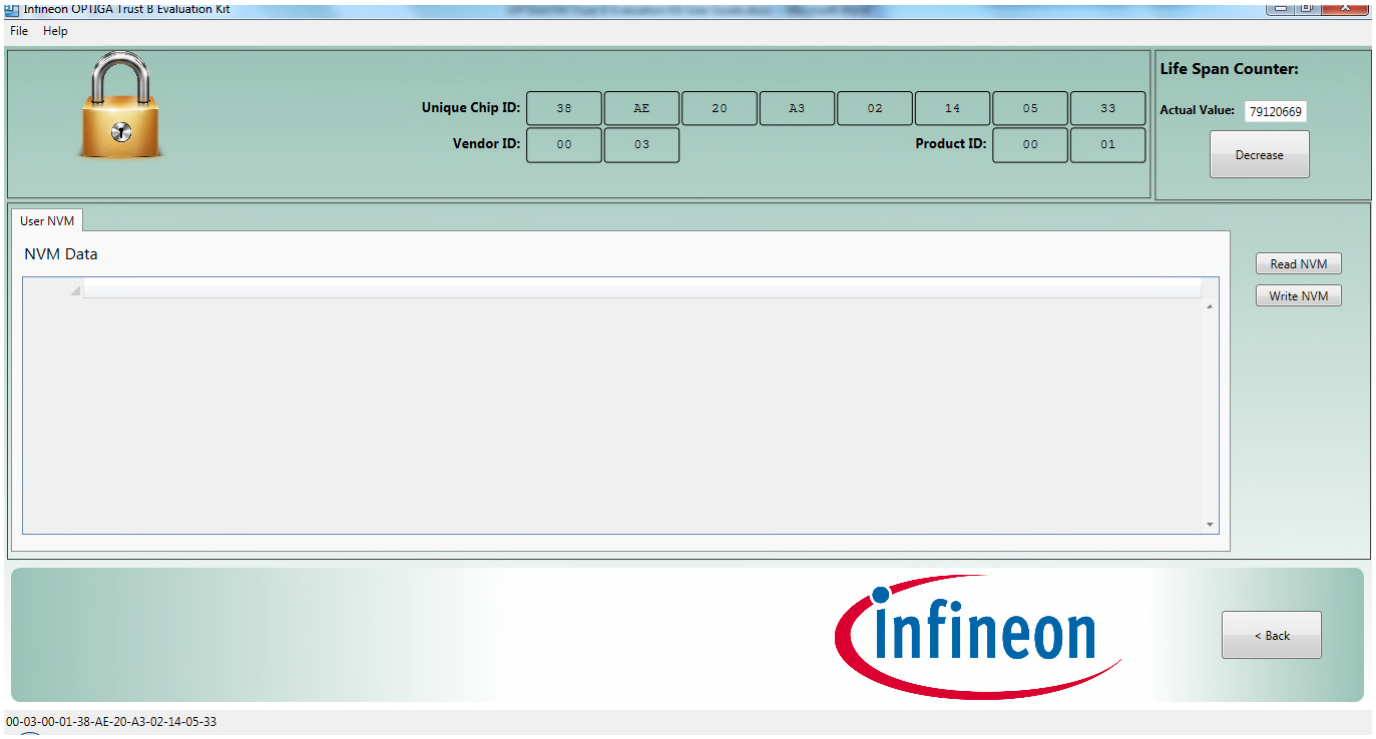
Simply click “Authentication” button on the left bottom of the GUI, the complete authentication sequence will be executed and displayed. Actual value of all the algorithm flow can be viewed in the edit box. If the authentication passes, “Authentic” will be printed, otherwise “Couterfeit” will be printed.



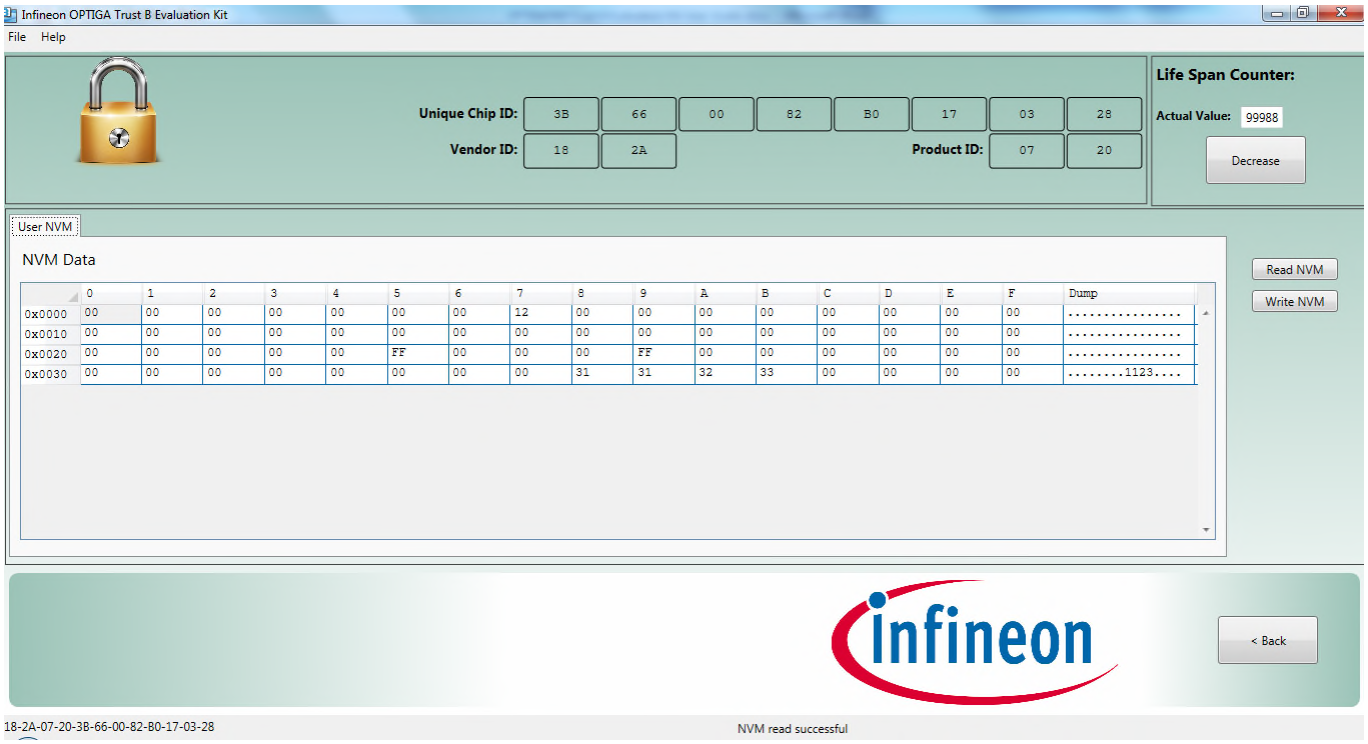


2.3 Non-Volatile Memory

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.



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

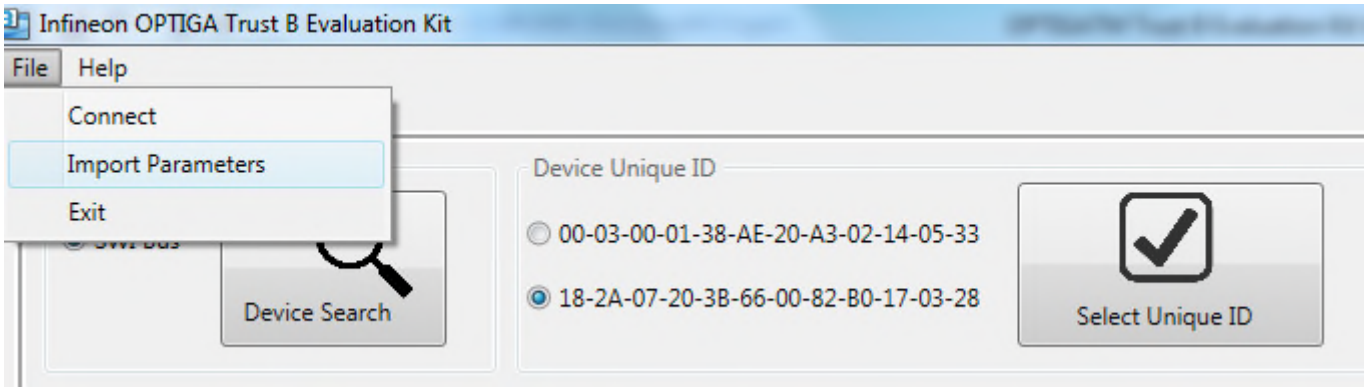


3 Test external devices

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

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

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 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.