TLE9893_2QTW62S_SECURE_BOOT

About this document

Scope and purpose

The aim of this guide is to present the scope, the implementation, the algorithm and a demonstration of the **TLE9893_2QTW62S_SECURE_BOOT** example code for the TLE989x Infineon Embedded Power ICs based on Arm® Cortex® M3. This example code can be found in the Keil µVision Pack Installer.

The full functionalities and characteristics of the embedded power devices are described in the datasheets and user's manual. Please refer to these documents for more detailed information. Furthermore, a low level (line-by-line) description of the code is not the aim of this document, although occasionally some codeblocks might be reported if necessary to the comprehension.

Note: *The following information is given as a hint for the implementation of the system only and shall not be regarded as a description or warranty of a certain functionality, condition or quality of the referred devices or presented software example.*

Intended audience

Design engineers, system engineers, embedded power designers

Table of contents

1 Introduction

Figure 1 shows the basic implementation for secure boot mechanism. The user must trigger the first reset to write the CMAC of user BSL into the first page. Upon successful write, the user must trigger Power-on Reset to initialize the secureboot mechanism. If the secure boot check is passed, the led pin P0.1 is set to high.

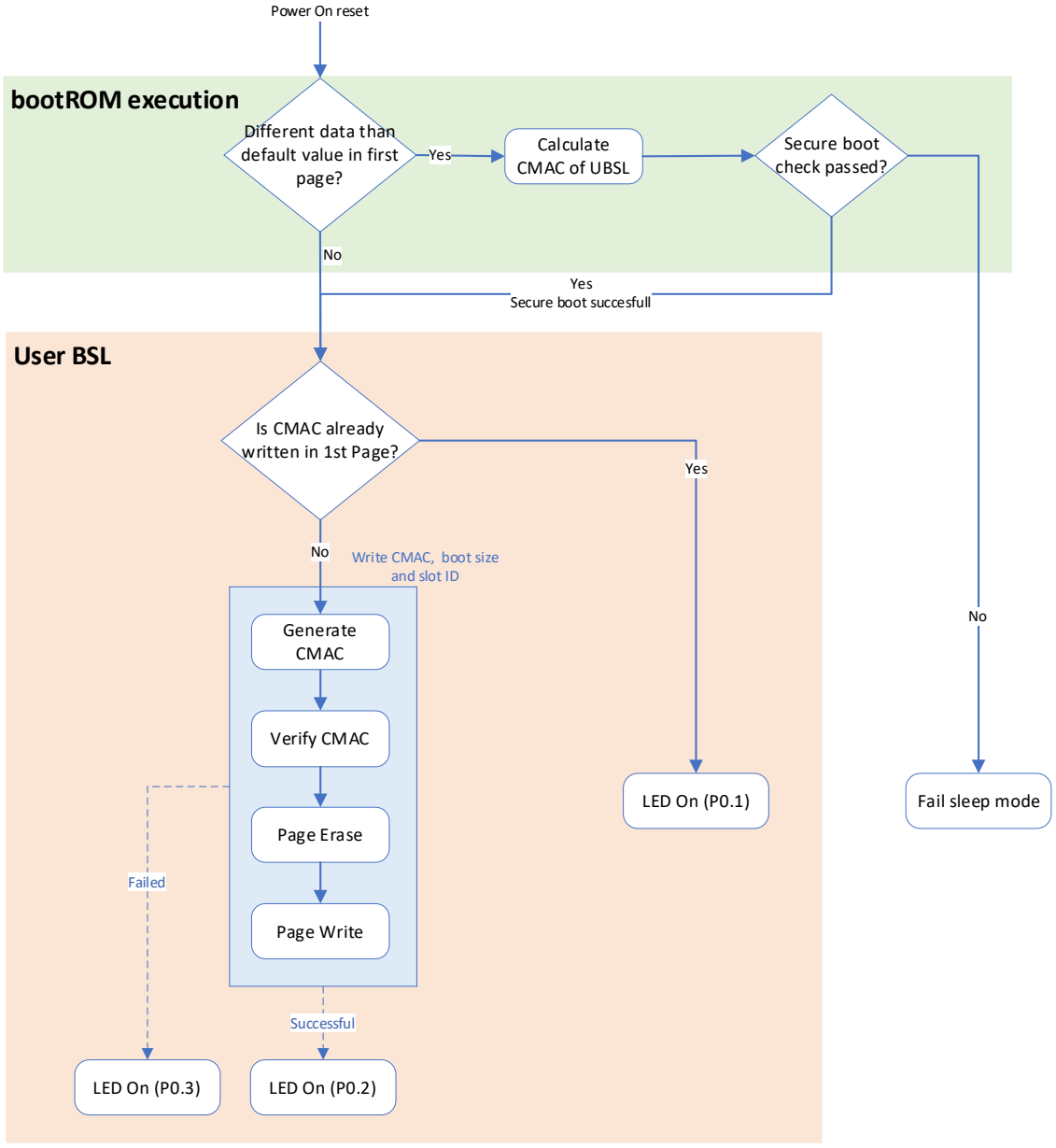

Figure 1 Application example flow chart for secure boot check

2 Hardware

This chapter shows how to run the TLE9893_2QTW62S_SECURE_BOOT example with the TLE988x/TLE989x evaluation board. For this the project must be opened and compiled.

Figure 2 shows the TLE988x/TLE989x evaluation board. The application code must be loaded via a debugger (e.g. ULINK or J-Link) to the board. The board must be powered with 12V (red and black connections).

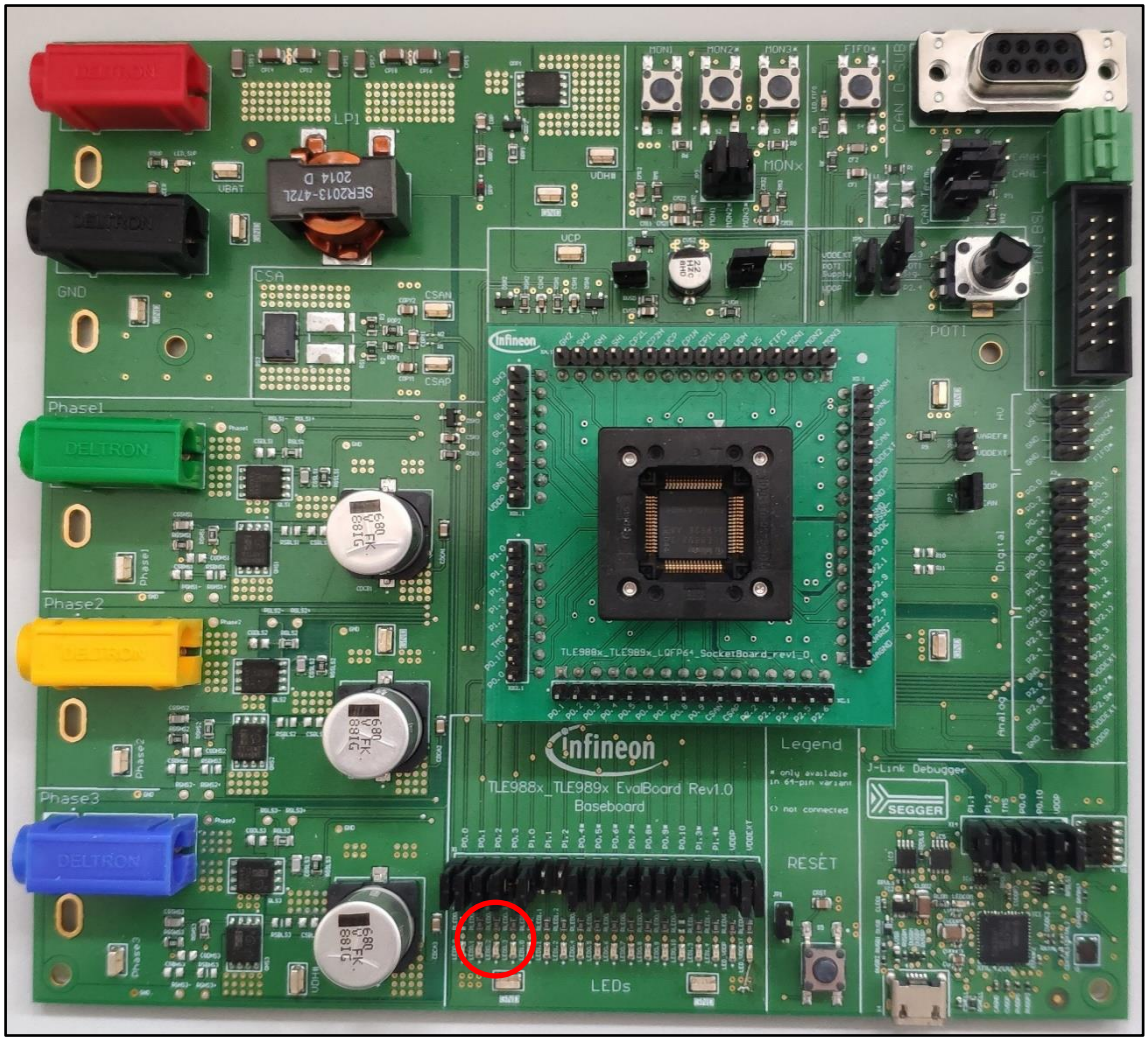

Figure 2 TLE988x/TLE989X evaluation board

3 Implementation

This chapter shows the process to follow to get a working secure access simple example.

3.1 Get the example via the Pack Installer for Keil

Open the Pack Installer within the Keil IDE.

Choose the appropriate device (here TLE9893_2QTW62S) on the left-hand side. On the right-hand side, select the tab Examples, where you can access the TLE98932QTW62S_SECURE_BOOT example.

Clicking on “Copy” will copy the example on your computer and open it.

3.2 Configuration

Figure 3 shows the GPIO configuration in the Config Wizard.

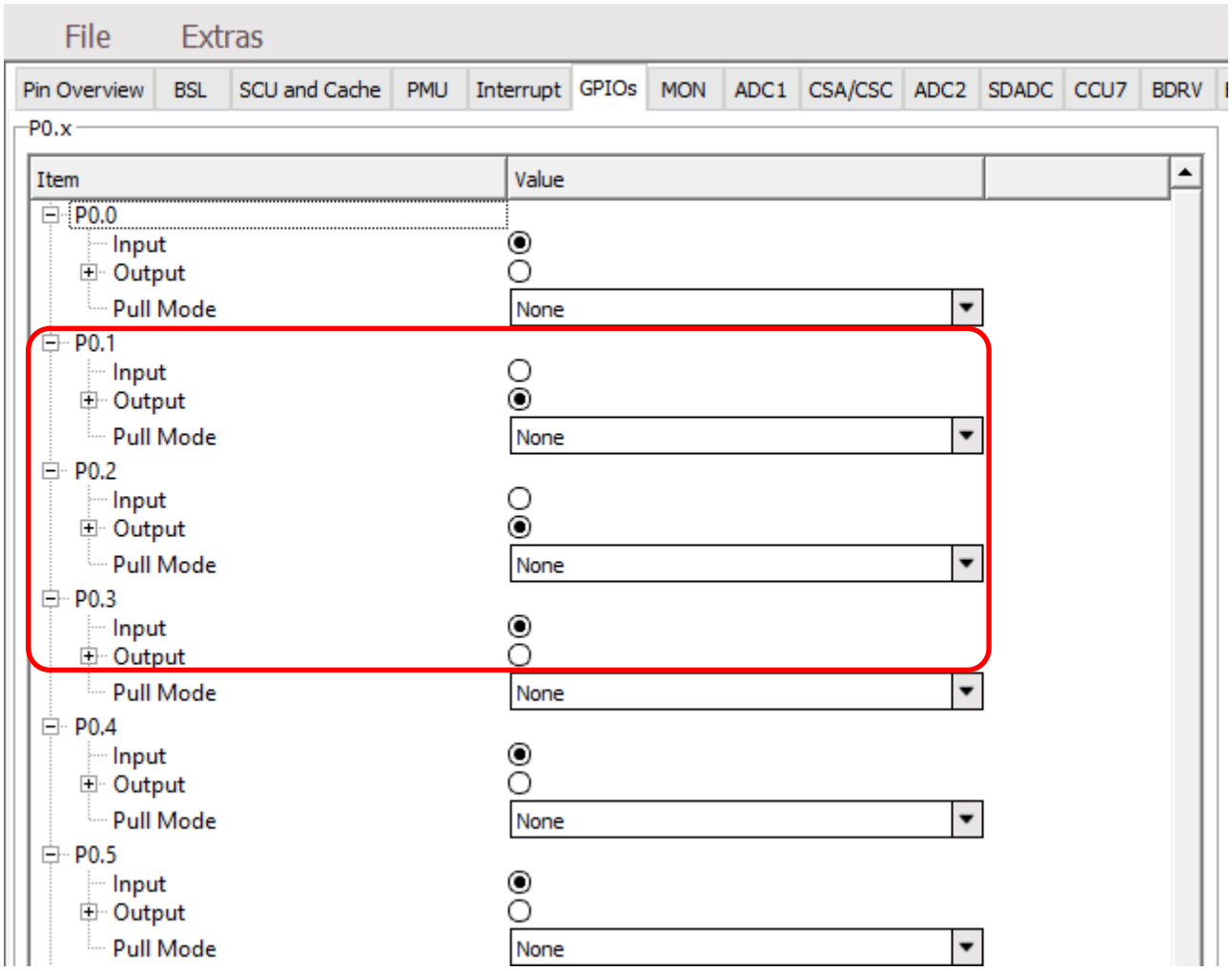

Figure 3 Config Wizard configuration

Finally, save your configuration to take these changes into account (File -> Save).

3.3 Sample code for CMAC write for Secure Boot Feature

Step 1: call `user_crypto_aes_cmac_generate_start` function which initializes the CMAC generation with the specified AES key ID.

Step 2: call `user_crypto_aes_cmac_generate_update` function which updates an ongoing CMAC generation with the specified buffer.

Step 3: call `user_crypto_aes_cmac_generate_finish` function which finalizes an ongoing CMAC verification with the specified input/output buffer.

Step 4: call `user_crypto_aes_cmac_verify_start` function which initializes the CMAC verification with the specified AES key ID.

Step 5: call `user_crypto_aes_cmac_verify_update` function which updates an ongoing CMAC verification with the specified buffer.

Step 6: call `user_crypto_aes_cmac_verify_finish` function which finalizes an ongoing CMAC verification with the specified MAC.

Step 7: update the CMAC and secure boot length into the flash0Data buffer.

Step 8: call `user_nvm_page_erase` function which erases a specified NVM page in user NVM.

Step 9: call `user_nvm_page_write` function which writes to the user NVM.

Step 10: Once the CMAC is written into the first page, user must trigger Power On reset. The device will perfrom secure boot verification. If the verification is successful, the led is set to high.

References

See the code examples at **www.infineon.com**

Revision history

Document version	Date of release	Description of changes
1.0	2021-10-15	Initial version
1.1	2022-10-13	Editorial changes

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

Edition 2022-10-13

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.