Customer training workshop: Cryptography_TRNG_Demonstration for KIT_T2G-B-H_EVK

TRAVEO™ T2G CYT4BF series Microcontroller Training
V1.0.0 2022-06

Please read the **Important Notice and Warnings** at the end of this document

Scope of work

- This code example demonstrates how to generate a one-time password (OTP) of eight characters in length with the true random number generation (TRNG) feature using the cryptography hardware block in MCU. The generated random number consists of alphanumeric and special characters of the ASCII code. The generated OTP is then displayed on a UART terminal emulator.

- Device
  - The TRAVEO^{TM} T2G CYT4BFBCH device is used in this code example.

- Board
  - The TRAVEO^{TM} T2G KIT_T2G-B-H_EVK board is used for testing.

Introduction

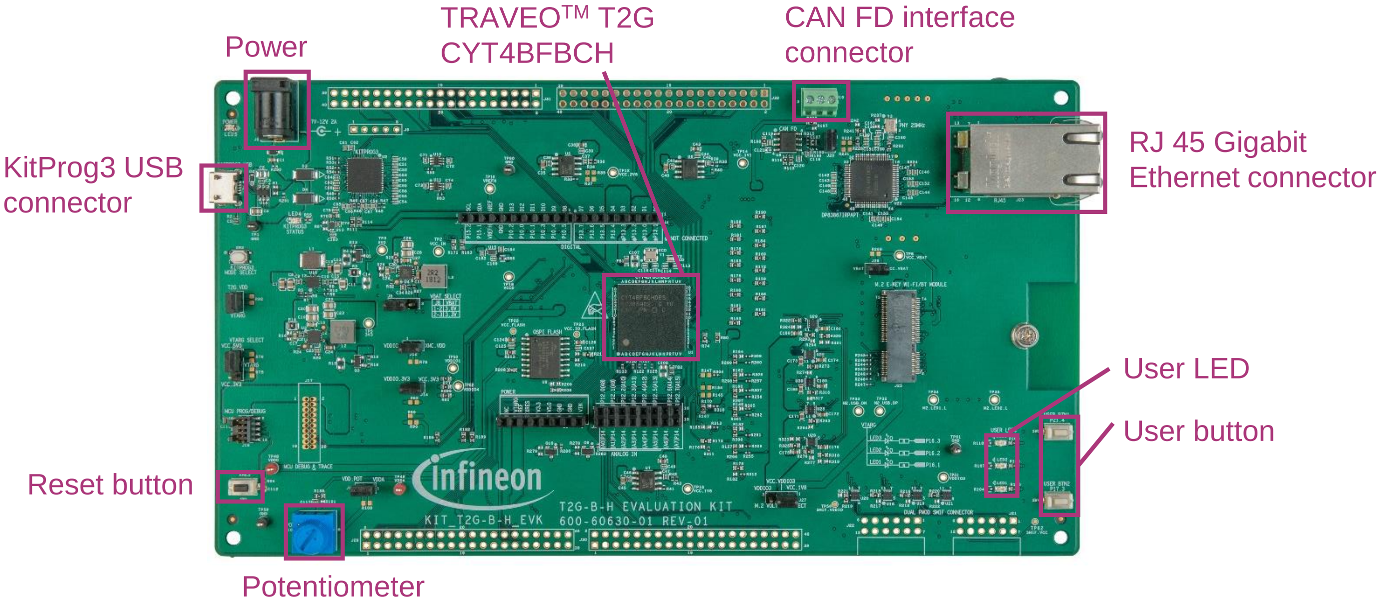
- **The cryptography block has the following features**
  - Advanced Encryption Standard (AES) functionality according to FIPS 197:
    The AES component can be used to encrypt/decrypt data blocks of 128-bit length and supports programmable key length (128/192/256-bit key).
  - CHACHA20 functionality according to RFC 7539:
    CHACHA20 is a stream cipher, which produces output consisting of 512-bit random-looking bits. These random-bits can be XORed with plain-text to produce cipher-text.
  - Triple Data Encryption Standard (TDES):
    The TDES component can be used to encrypt/decrypt data blocks of 64-bit length using a 64-bit key.
  - Secure Hash Algorithm (SHA) functionality according to FIPS 180-4/FIPS-202:
    This component can be used to produce a fixed-length hash (also called “message digest”) of up to 512 bits from a variable-length input data (called “message”). SHA1, SHA2, SHA3 hashes are supported.
  - Cyclic Redundancy Check (CRC) functionality:
    This component performs a cyclic redundancy check with a programmable polynomial of up to 32-bits.
  - String (STR) functionality:
    This component can be used to efficiently copy, set, and compare memory data.

Introduction (contd.)

- Pseudo Random Number Generator (PRNG):
  This component generates pseudo random numbers in a fixed range. This generator is based on three Linear Feedback Shift Registers (LFSRs).
- True Random Number Generator (TRNG):
  This component generates true random numbers of up to 32 bits using ring oscillators.
- Vector unit (VU):
  This component act as coprocessors to offload asymmetric key operations from the main processor.
- AHB master-interface:
  This allows to fetch operands directly from the system memory.
- Device key functionality:
  The device key usage is restricted to specific functionality; it cannot be accessed by the software that implements that functionality.
  Two independent device keys are supported.

Hardware setup

- This code example has been developed for the KIT-T2G-B-H-EVK board.
- Connect your PC to the board using the provided USB cable through the KitProg3 USB connector.



Implementation

- In this example, an OTP of eight characters in length is generated. The generated OTP is then displayed on an UART terminal emulator. The firmware generates a new OTP instantly when the user presses the Enter key.

Follow these steps to configure this code example:

- Configure the STDIN / STDOUT
- Display the initial message to the terminal and check the key operation
- Generate password

Configure the STDIN / STDOUT

- Initialization of the GPIO for UART is done in the ***cy_retarget_io_init()*** function
  - Initialize P13.1 as UART TX, P13.0 as UART RX (these pins are connected to the KitProg3 COM port)
  - The serial port parameter changes to 8N1 and 115200 baud

Implementation

Display the initial message to the terminal and check key operation

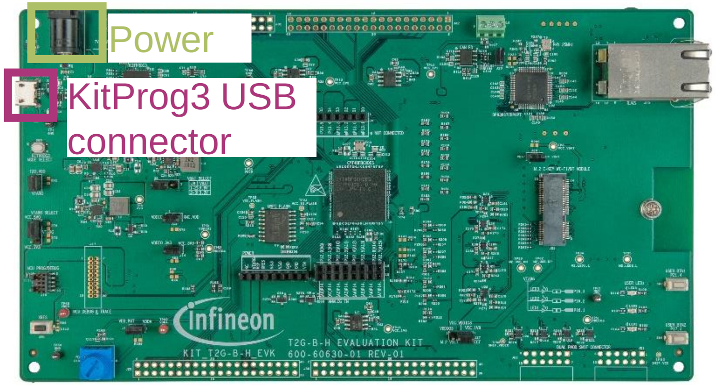
- The terminal can be displayed by ***printf()***
  - The display data is specified as ***CLEAR_SCREEN*** and ***SCREEN_HEADER***
- The checking of key operation is done in the ***cyhal_uart_getc()*** function
  - In this sample, it checks if the “Enter” key was pressed

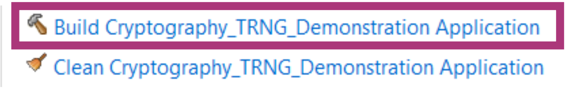
Generate password

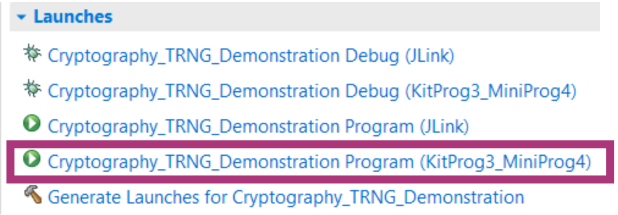
- OTP generation of 8 characters is done in the ***generate_password()*** function. This function runs the following:
  - Initialization of the cryptography TRNG block is done in the ***cyhal_trng_init()*** function
  - Generates a random number using the ***cyhal_trng_generate()*** function
    - The generated 32-bit random number is converted to an 8-character ASCII code.
    - The OTP is displayed on the terminal by ***printf()***
  - The random number generator block is released by the ***cyhal_trng_free()*** function
  - The OTP length can be changed by modifying the ***PASSWORD_LENGTH*** value

Compiling and programming

1. Connect to power and USB cable
2. Use Eclipse IDE for ModusToolbox™ software for compiling and programming
3. Compile
   a) Select the target application project in Project Explorer
   b) In the Quick Panel, scroll down, and click “Build Cryptography_TRNG_Demonstration Application” in the Cryptography_TRNG_Demonstration kit (KIT-T2G-B-H-EVK)
4. Open a terminal program and select the KitProg3 COM port. Set the serial port parameters to 8N1 and 115200 baud.
5. Programming
   a) Select the target application project in the Project Explorer
   b) In the Quick Panel, scroll down, and click “Cryptography_TRNG_Demonstration Program (KitProg3_MiniProg4)” under Launches

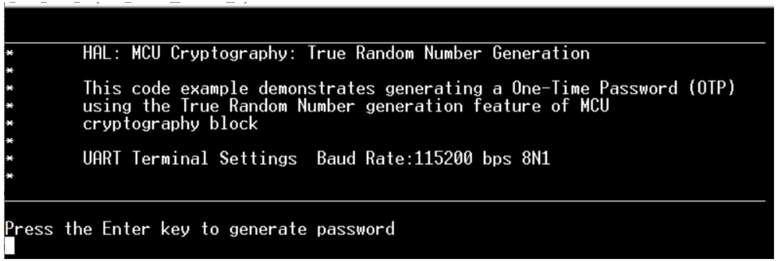



Build Cryptography_TRNG_Demonstration Application
Clean Cryptography_TRNG_Demonstration Application


Launches
Cryptography_TRNG_Demonstration Debug (JLink)
Cryptography_TRNG_Demonstration Debug (KitProg3_MiniProg4)
Cryptography_TRNG_Demonstration Program (JLink)
Cryptography_TRNG_Demonstration Program (KitProg3_MiniProg4)
Generate Launches for Cryptography_TRNG_Demonstration

Run and test

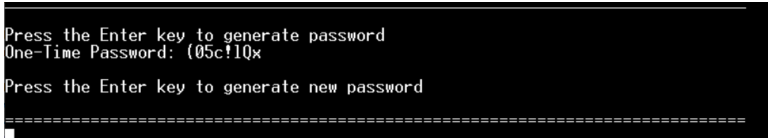
1. After successful programming, observe the following message:



```
*       HAL: MCU Cryptography: True Random Number Generation
*
*       This code example demonstrates generating a One-Time Password (OTP)
*       using the True Random Number generation feature of MCU
*       cryptography block
*
*       UART Terminal Settings  Baud Rate:115200 bps 8N1
*

Press the Enter key to generate password
```

2. When you press the “Enter” key, an OTP is generated and displayed:

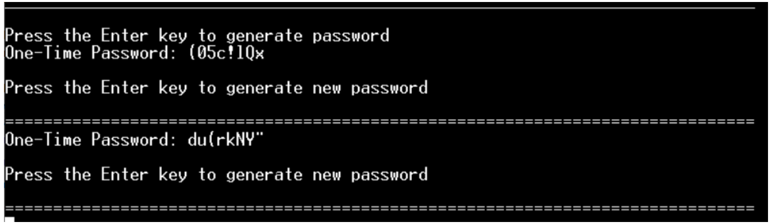


```
Press the Enter key to generate password
One-Time Password: (05c!1Qx

Press the Enter key to generate new password

===============================================================================
```

3. When you press the “Enter” key again, another OTP is generated and displayed.



```
Press the Enter key to generate password
One-Time Password: (05c!1Qx

Press the Enter key to generate new password

===============================================================================
One-Time Password: du(rkNY"

Press the Enter key to generate new password

===============================================================================
```

References

Datasheet

- CYT4BF datasheet 32-bit Arm® Cortex®-M7 microcontroller TRAVEO™ T2G family

Architecture technical reference manual

- TRAVEO™ T2G automotive body controller high family architecture technical reference manual

Registers Technical reference manual

- TRAVEO™ T2G Automotive body controller high registers technical reference manual

PDL/HAL

- PDL
- HAL

Training

- TRAVEO™ T2G Training

Revision History

Revision	ECN	Submission Date	Description of Change
**	7782086	2022/07/05	Initial release

Important notice and warnings

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

Edition 2022-06
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?
Go to: www.infineon.com/support

Document reference
002-35561 Rev. **

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.