How to enable security features when using X-CUBE-IOTA1

Introduction

Distributed Ledger Technology (DLT) is built on a network of multiple nodes which do not trust each other. The network maintains a distributed ledger, namely a cryptographically secured, distributed database, that stores a set of transactions. Nodes agree on issuing transactions through a consensus protocol.

IOTA is a Distributed Ledger Technology specifically designed for use in IoT.

The IOTA distributed ledger is called tangle and is formed by the transactions issued by the nodes in the IOTA network, which includes full nodes and light nodes.

A full node is connected to peers in the network and stores a copy of the ledger. A light node is a device that has a private key called seed, which can be used to create addresses and signatures. A light node creates and signs transactions and sends them to a full node so that the network can validate and store them. Withdrawal transactions must contain a valid signature.

When implementing an IOTA light node using the X-CUBE-IOTA1 expansion software package for STM32Cube, some practical security features can be enabled on the target STM32 microcontroller.

RELATED LINKS

https://www.iota.org/get-started/what-is-iota

https://docs.iota.org/docs/getting-started/0.1/introduction/what-is-iota

1 Security features

Some security features for the STM32F746ZG microcontroller are:

- Readout Protection (RDP)
- Memory Protection Unit (MPU)
- True Random Number Generator (TRNG)

For a detailed description of the security features of all STM32 series 32-bit Arm Cortex MCUs, refer to AN5156: "Introduction to STM32 microcontrollers security" freely available at www.st.com.

1.1 Readout Protection

Readout Protection (RDP) is a static protection feature that allows embedded firmware code to be protected against copy, reverse engineering, dumping, using debug tools or code injection in SRAM.

RDP can be set to level 0,1, or 2.

1.1.1 Level 0

Level 0 is the Readout Protection default level.

All read or write operations on the Flash memory or the backup SRAM are possible in all boot configurations. Option bytes are changeable.

Note: As this level does not provide any protection to the device, it should be used only for development and debug.

1.1.2 Level 1

In this security protection level, Flash memory accesses (read, erase, program) or SRAM2 accesses via debug features (such as Serial Wire or JTAG) are forbidden, even while booting from SRAM or system memory bootloader.

In these cases, any read request to the protected region generates a bus error.

However, when booting from Flash memory, accesses to the Flash memory and the SRAM2 (from user code) are allowed.

Note: Option bytes can still be modified at this level by re-programming RDP option byte from level 1 to 0 but causing the Flash memory and the backup SRAM to be mass-erased.

1.1.3 Level 2

This level provides the same protection as RDP level 1 but in a permanent way.

Option bytes can no longer be modified. In particular, level regression is not possible.

RDP level 2 guarantees full protection of the microcontroller from external attackers: debug interfaces are disabled, therefore access to internal Flash and SRAM memories are forbidden.

However, modifications by an internal application are still possible. In particular, RDP level 2 allows a Secure Firmware Update (SFU) application to update the internal code when the device is on the field.

Note: Setting RDP level 2 is an irreversible operation and cannot be undone. Therefore, this level must only be considered in the final product, when the development stage is completed.

1.2 Memory Protection Unit

Memory Protection Unit (MPU) is a dynamic protection feature that allows defining specific access rights for any memory-mapped resource of the device (Flash memory, SRAM and peripheral registers).

Access rights can be set as Executable, Not executable (XN), Read-Write (RW), Read Only (RO), or No Access.

Two execution modes are defined, allowing a process to run in either privileged or unprivileged mode.

The MPU protection is dynamically managed at runtime. It splits the memory map into several regions, each with its own access attribute.

For each region, the access attribute can be set independently for each mode. At reset, the privilege mode is the default one for any process.

1.3 True Random Number Generator

True Random Number Generator (TRNG) is a hardware-based peripheral providing a physical noise source. It can be used to generate strong session keys.

2 Secure configuration

2.1 Initial configuration

After the binary code is loaded into the embedded Flash memory, RDP should be set to level 2.

Note: As this operation is irreversible, the code should be tested adequately before running it.

A sector of the Flash memory should be reserved for the seed. At the first boot the seed can be securely generated using the device embedded TRNG. Alternatively, the seed is transferred to the device in a secure environment.

2.2 MPU configuration

You should set the access attributes of memory regions as follows:

- Region storing the seed: Read Only for privileged processes, No Access for any other process
- Region defining MPU configuration: Read Only for privileged processes, No Access for any other process
- Flash interface: Read-Write for privileged processes, No Access for any other process
- Direct Memory Access (DMA) controller: Read-Write for privileged processes, No Access for any other process

Processes to be set as privileged are: address generation, signature computation, and processes implemented in Secure Firmware Update.

Note: For Secure Boot and Secure Firmware Update, refer to UM2262 “Getting started with the X-CUBE-SBSFU STM32Cube Expansion Package” freely available at X-CUBE-SBSFU.

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
18-Jun-2019	1	Initial release

Contents

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2019 STMicroelectronics – All rights reserved