STM32U385xx SESIP security guidance

Introduction

This document describes the preparative procedures and operational user guidance of STM32U3 microcontrollers to make a secure system solution according to SESIP level 3 certification scheme.

The security guidance described in this document applies to any boards based on the devices listed in the table below.

Table 1. Applicable products

Reference	Products
STM32U3	STM32U385xx

1 General information

This document applies to STM32U385xx Arm®-based MCUs with the Arm® TrustZone® technology.

arm

Note: Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere.

The Arm word and logo are trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved.

Table 2. Specific acronyms

Acronym	Description
HUK	Hardware unique key
CLI	Command line interface
HDP	Secure hide protection
HW	Hardware
IoT	Internet of things
MCU	Microcontroller
TOE	Target of evaluation
RDP	Readout protection
RMA	Return material for analysis
SESIP	Security evaluation standard for IoT platforms
SFR	Security-functional requirement
WRP	Write protection

2 Reference documents

Table 3. List of reference documents

Reference	Document title and revision
[ST]	Technical note *STM32U385xx SESIP Security Target* (TN1546), Rev 1
[RM]	Reference manual *STM32U3 Series Arm®-based 32-bit MCUs* (RM0487), Rev 3
[UM2237]	User manual *STM32CubeProgrammer software description* (UM2237), Rev 29
[UM2609]	User manual *STM32CubeIDE user guide* (UM2609), Rev 17
[IEEE1149]	EEE 1149.1–2013
[IHI0031]	Arm® Debug Interface Architecture Specification ADIv5.0 to ADIv5.2
[SM]	PSA Certified *Platform Security Model 1.1* (JSADEN014)
[PM0264]	Programming manual *STM32 Cortex®-M33 MCUs and MPUs* (PM0264), Rev 7
[AN6205]	Application note *Introduction to the use of PKA key wrapping with coupling and chaining bridge on STM32 MCUs*, Rev 1

3 TOE preparative procedures

This section provides useful information for ensuring that the target of evaluation (TOE) has been received and installed in a secure manner as intended by the developer.

- Secure acceptance: procedures to check the product to be prepared.
- Secure preparation of the operational environment: procedures to set up the environment needed to manage and prepare the final product.
- Secure installation: procedure to program and configure the product to be prepared.

3.1 Secure acceptance

Secure acceptance is the process in which the user securely receives the TOE and verifies its genuineness (the integrity and authenticity of all its components). The TOE is distributed as an MCU device.

To ensure that the MCU is not manipulated during TOE delivery, the integrator must verify:

- The integrity of the quality assurance (QA) sealed tape closing the inner box (picture 1 & 2).
- The integrity of the sealed dry bag (vacuum closed) including the final product (picture 3).
- That the user flash is virgin (reading 0xFF everywhere with STM32CubeProgrammer). For more details on STM32CubeProgrammer, refer to [UM2237].

Figure 1. QA sealed tape closing the inner box (1)



Figure 2. QA sealed tape closing the inner box (2)



Figure 3. **Sealed dry bag (vacuum closed) including the final product**



During the secure acceptance process, it is the responsibility of the integrator to obtain the correct software package as described in Section 3.2.2: Software setup procedure.

The integrator accepts a microcontroller part of the STM32U3 series by reading, with STM32CubeProgrammer, the DBGMCU_IDCODE register value as defined in [RM] below. Supported part numbers are listed in Table 4.

Table 4. **Applicable products**

Field	Address	Halfword value	Comments
Device identifier (DEV_ID)	0xE004 4000	0x454	STM32U385xx version 1.3 (rev X)
Revision identifier (REV_ID)	0xE004 4002	0x1007	

As part of the acceptance process the integrator also reads the product configuration information as defined in the Table 5. The integrator should not accept a TOE without the correct product configuration for STM32U3 series.

Table 5. **Product configuration**

Field	Address	Halfword value	Comments
Product configuration for STM32U3 series	0x0BFA 0500	Bits 10, 13 and 15 set	PKA, CCB, and SAES enable

3.2 Secure installation and preparation (AGD_PRE.1.2C)

This section preparative procedures describes all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in [ST].

3.2.1 Hardware setup procedure

To set up the hardware environment, the development board must be connected to a personal computer via a USB cable. This connection with the PC allows the user to:

- Configuring the platform non-volatile memory (flash)
- Debugging when the protections are disabled.
- Optionally interacting with the board via a UART console (see Terminal emulator)

The ST-LINK firmware programmed on the development board must be the V3J15M6 version or newer.

3.2.2 Software setup procedure

This section lists the minimum requirements for the developer to set up the SDK on a Windows 10® host, run the sample scenario and customize applications delivered in the corresponding STM32Cube MCU package.

3.2.2.1 STM32Cube firmware package

The STM32Cube firmware package includes necessary drivers, middleware, template projects, example applications and compiler toolchain for software development on the target STM32 microcontroller.

Download and install the latest STM32CubeU3 MCU package release for the STM32U3 series of devices from:

- https://www.st.com/en/embedded-software/stm32cubeu3.html

3.2.2.2 Software tools for programming STM32 microcontrollers

STM32CubeProgrammer (STM32CubeProg) is an all-in-one multi-OS software tool for programming STM32 microcontrollers. It provides an easy-to-use and efficient environment for reading, writing, and verifying device memory through both the debug interface (JTAG and SWD) and the bootloader interface (UART and USB).

STM32CubeProgrammer offers a wide range of features to program STM32 microcontroller internal memories (such as flash memory, RAM, and option bytes) as well as external memories. STM32CubeProgrammer also allows option programming and upload, programming content verification, and microcontroller programming automation through scripting.

STM32CubeProgrammer is delivered in GUI (graphical user interface) and CLI (command-line interface) versions.

For more details about STM32CubeProgrammer, refer to [UM2237].

Note: Always use the latest release of the STM32CubeProgrammer software package.

3.3 Secure installation

The product preparation for microcontrollers that are part of the STM32U3 series is done in two steps, to get a complete installation with fully activated security configuration. All the steps must be performed successfully to have the product in its certified configuration.

3.3.1 Step 1: Software programming

- Program the non-platform required secure boot firmware and root parameters in the HDP securable memory at address according to the integrator mapping.
- All the other parts of the application code not belonging to the secure boot firmware are programmed outside of the HDP securable memory area at the destination address according to the integrator mapping.

3.3.2 Step 2: Static security protection programming

- Program FLASH_OPTR.TZEN=1 (TrustZone),
- Set the unique boot entry:
  - FLASH_OPTR.SWAP_BANK=0 (no swap)
  - Program FLASH_SBOOT0R.ADD = the secure boot memory address modulo 128 bytes
  - Set FLASH_SBOOT0R.BOOT_LOCK = 1.
- Program the platform's secure area (SECWM), so that at least the non-platform required secure firmware and root parameters are in the secure area:
  - Program FLASH_SECWMxR1.SECWMx_STRT[6:0] = First page of the secure area
  - Program FLASH_SECWMxR1.SECWMx_END[6:0] = Last page of the secure area. With x value can be 1 or/and 2.
- Program the platform's hide protection area (HDP) located in the secure area, so that the non-platform required secure firmware and root parameters matches the hide protection area:
  - Program FLASH_SECWMxR2.HDPxEN[7:0] = value different than 0xB4
  - Program FLASH_SECWMxR2.HDPx_END[6:0] = last page of the hide protection area. Must be in the secure area. With x value can be 1 or/and 2.

- Program a write-protected memory area (WRP) on the immutable area. This area must include the HDP area.
  - Program FLASH_WRPxAR.STRT = first page of WRP area A in bank x
  - Program FLASH_WRPxAR.END = last page of WRP area A in bank x. Must be equal to the last page of the hide protection area.
  - Program FLASH_WRPxAR.UNLOCK = 0, so WRP area A in bank x is locked. With x value set to 1 or 2, depending on integrator mapping
- Program the Read Protection (RDP):
  - Program FLASH_OPTR.RDP = 0xCC (RDP level2)

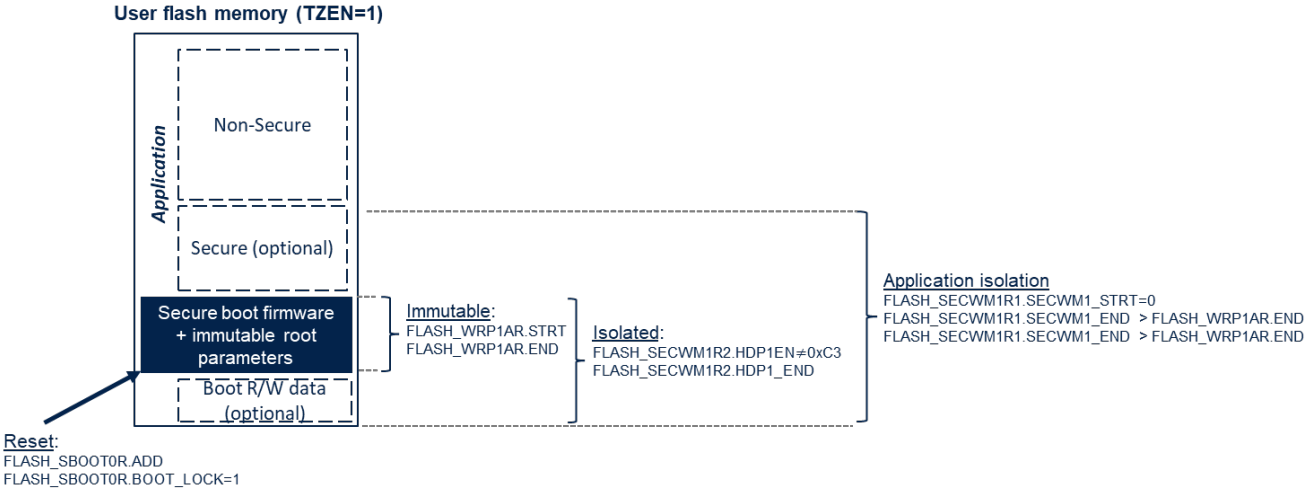
Some secure boot code examples are available in the STM32Cube firmware package defined in Section 3.2.2: Software setup procedure.

3.3.3 Certified configuration

After achieving the two secure installation steps, the platform is in its secured configuration.

Figure 4 illustrates the configuration of the secure boot firmware and the root parameters in bank1.

Figure 4. TOE certified configuration



4 Operational user guidance

4.1 User roles

The user role integrator is the only role involved in the preparative TOE procedure. The integrator is responsible for:

- Receiving the TOE.
- Performing the preparative procedures as described in TOE preparative procedures.
- Integrating the TOE into a final product.

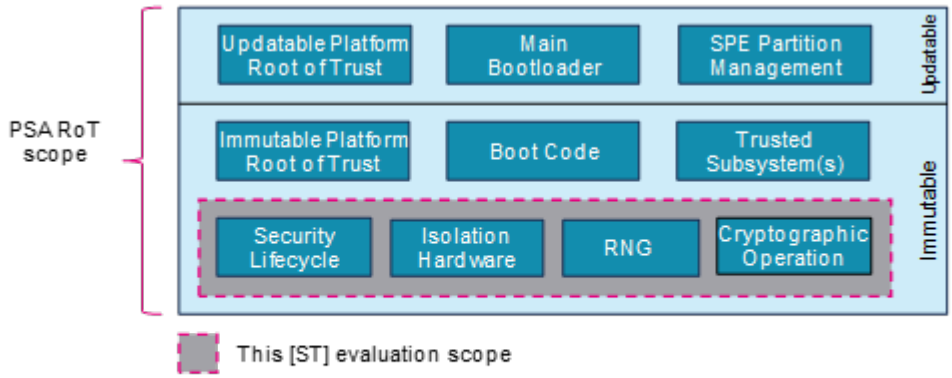
The integrator has full access to the TOE security features, as the MCU devices of the STM32U3 series are delivered in RDP0 state without any features activated for NVM protection. The integrator also has full access to the tools needed to program the TOE.

4.2 Operational guidance for the integrator roles

4.2.1 User-accessible functions and privileges (AGD_OPE.1.1C)

The main task of the Integrator is to integrate the TOE into a final product. To this end, the system integrator has access to interfaces that are unavailable to other users, as described in Section 4.2.2: Available interfaces and methods of use (AGD_OPE.1.2C and AGD_OPE.1.3C). The Integrator cannot change any parts inside the TOE but must configure the TOE to make it functional in the final secure state. The Integrator can change parts outside the TOE without compromising the security of the TOE as shown in Figure 5.

Figure 5. Figure 2. TOE perimeter



Follow the procedures described in Section 3.1: Secure acceptance to check if the TOE is acceptable for the secure configuration. The secure configuration of the TOE may be impacted when changing some parts of the TOE but may also be impacted when changing some parts located outside the TOE scope. This section describes the changes that the integrator can make and highlights what is covered in the evaluation scope and what might impact the secure configuration of the TOE.

4.2.1.1 Product firmware

The integrator must first load the product firmware prior to setting up the security configuration of the final product.

The integrator must split the product firmware into two separated areas:

- Securable memory area that includes an HDP area in which the integrator can locate its protected assets. This HDP section contains an immutable area safeguarded by write protection (WRP). This area might contain, for example, a first-stage secure boot code with root parameters composed of private and immutable personalization data or cryptographic elements depending on the integrator's product security requirements.
- A non-HDP memory area where the integrator can locate the next boot stages plus the application firmware.

Recommended security protection programming is described in Section 3.2.2: Software setup procedure.

4.2.1.2 *RDP configuration*

In its certified configuration the platform is deployed in RDP level 2.

The RDP value in FLASH_OPTR indicates the protection level of the product, as explained in section 3.10.1 of [RM].

For the platform, in the scope of this certification, the OEM2KEY shall not be provisioned.

4.2.1.3 *HDP securable memory area*

The platform is certified with the HDP securable memory enabled. The integrator shall link the immutable Root of Trust of the product firmware inside the securable memory area and configure the associated options bytes as follows:

- FLASH_SECWMxR2.HDPxEN = value different than 0xB4
- FLASH_SECWMxR2.HDPx_END: index of the last page of the HDP1 securable memory area.
- With x value can be 1 or/and 2, depending on the integrator mapping

Additionally, for STM32U3 series, the product firmware shall activate the hide protection just before jumping out of the securable memory area by setting the HDPx_ACCDIS to a value different than 0xA3 in the FLASH_SECHDPCR register. Refer to section 3.6.1 in [RM] for more details on HDP.

4.2.1.4 *Boot configuration*

In its certified configuration the platform starts by executing code from the secure address defined by option byte FLASH_SBOOT0R.ADD, because the option byte BOOT_LOCK is set. This address must be located in a secure, write protected, and HDP protected area, as described in Section 3.2.2: Software setup procedure.

4.2.1.5 *Fault injection attacks countermeasures*

The platform claims resistance against physical attacker, to fully leverage it, the Integrator must enable the following protections.

The Integrator must implement the following software countermeasures within its application when performing sensitive operations (including cryptographic ones):

- Redundancy:
  For example:
  - Perform sensitive operation twice and verify that results are equal.
  - Implement the inverse of the cryptographic operation: encrypt then decrypt or decrypt then encrypt.
- In case of verification error:
  - Implement security response, such as platform reset.
- Random timing jitter:
  - For example, apply random loop (using RNG peripheral) before sensitive operation.
- Execution control flow:
  For example:
  - Use a finite state machine in which transitions are verified to be legit.
  - Use a scattered known computation with a verified result at the end.
- In case of control flow error:
  - Implement security response, for example platform reset.

In addition to the above protection, the integrator should implement anti-tampering protection:

- Enable system and cryptographic internal tampers detection (TAMP peripheral):
- When a tamper flag raises (tampering detected), the Integrator must implement a security response, for example platform reset. Refer to the section 3.7.3 “Tamper detection and response” in [RM].

4.2.1.6 *True random number generator*

For the device to generate random numbers as specified in NIST SP800-90B, the integrator must use the TRNG peripheral with the configuration A. Refer to the subsection “validation conditions” of the RNG section in the [RM] for details.

4.2.1.7 *Hardware-accelerated cryptography*

In its configuration with additional cryptography (see Section 3.1: Secure acceptance) the platform is certified with hardware-accelerated cryptography that is protected against SCA, fault injection, and timing analysis attacks.

To achieve the required resistance against hardware attacks, the integrator must use the following hardware-accelerated cryptographic function, detailed in the corresponding sections of the [RM].

- SAES peripheral:
  - AES-128 and AES-256:
    - Encryption/decryption
    - Authenticated encryption or decryption
    - Cipher-based message authentication code computation
- PKA peripheral:
  - RSA, decryption using protected modular exponentiation (MODE=0x3).
  - ECC, protected scalar multiplication (MODE=0x20) and signature (MODE=0x24).

Note: SAES and PKA cannot operate if the RNG peripheral is not properly initialized, with its AHB clock running.

As any software dealing with sensitive data, the software driving hardware cryptography accelerators should follow the guidelines described in section “Section 4.2.1.5: Fault injection attacks countermeasures” (for instance, timing randomization, and control flow). The software handling crypto operations should comply with the recommendations provided in the corresponding specification, as indicated in Table 7 of the [ST].

4.2.1.8 *Cryptographic key storage*

The integrator can use the SAES peripheral to protect the confidentiality of AES 128 or 256-bit keys in its KeyStore, using the key wrapping/ unwrapping method described in the subsection “*SAES operation with wrapped keys*” of the SAES section in [RM].

As any software dealing with sensitive data, the software driving SAES peripheral should follow the guidelines described in section “Section 4.2.1.5: Fault injection attacks countermeasures” (for instance, timing randomization and control flow).

The integrator can use the CCB to protect the confidentiality of the RSA and ECC private Keys in its keystore using the special coupling and chaining operations method as described in the subsection “*CCB coupling and chaining operations”* of the CCB in [RM] and in [AN6205].

Note: The wrapping/unwrapping function is not usable while an active tamper event is not cleared. See next section.

4.2.1.9 *Anti-tamper peripheral*

The platform resets with internal and external tamper sources deactivated in the TAMP peripheral. The integrator must configure TAMP peripheral with anti-tamper methods available (internal tampers) in the device when managing following functions:

- Nonvolatile derived hardware unique key (DHUK) usage.
- Crypto functions in hardware engines (SAES, AES, HASH, PKA, and CCB).

For TAMP peripheral configuration, refer its dedicated section in [RM].

4.2.2 Available interfaces and methods of use (AGD_OPE.1.2C and AGD_OPE.1.3C)

To exercise the functions and privileges described in Section 4.2.1: User-accessible functions and privileges (AGD_OPE.1.1C), the integrator interacts with the TOE interfaces described in this section:

- Physical chip interface
- Flash option bytes, Flash registers and flash memory interface
- True Random Number Generation
- Cryptographic functions interface
- TAMP peripheral
- DBGMCU
- RCC peripheral
- CPU

4.2.2.1 *Physical chip interface*

After providing power supply and clocks and de-asserting the reset signal (Refer to RCC and PWR sections in [RM] for details on power-on and reset procedures), the platform firmware starts at a unique boot address stored in FLASH_SBOOT0R.ADD

Method of use:

- Activate power supplies and clocks of the platform.
- Reset the device.

Parameters:

- Not applicable

Actions:

- The Cortex-M33 processor first executes in secure mode the code located in an internal flash area HDP and write protected.

Errors:

- The platform firmware does not start properly if its vector table of the integrator firmware is not located at the boot address in the user flash. The Cortex-M33 goes to error states if its vector table points toward a non-secure area (see Section 2.3.2 in [RM] for details).

4.2.2.2 *Flash option bytes*

The integrator in the secure boot shall read the flash option bytes to confirm that the platform is set in the certified configuration defined in Section 3.2.2: Software setup procedure.

Method of use:

- The CM-33 processor in secure mode performs read access in the flash registers.

Parameters:

- The list of flash option bytes and their configuration are presented in step 2: static security protection programming of Section 3.3: Secure installation.

Actions:

- Verify the value of each enumerated configuration byte.

Errors:

- The action fails if the content read from option bytes differs from the programmed values. In that case, the integrator firmware must cancel the boot operation, by resetting the platform or looping infinitely.

4.2.2.3 *Flash registers*

When the secure boot firmware ends its execution it must jump to a code located in a non-HDP area. The jump procedure must activate the TOE HDP area protection, making it inaccessible by any read or write operation until the next reset.

Method of use:

- Set HDP1_ACCDIS to a value different than 0xA3 in FLASH_SECHDPCR register (refer to [RM] section 7.10)

Parameters:

- In FLASH_SECHDPCR the HDP1_ACCDIS bits

Actions:

- Set HDP1_ACCDIS to a value different than 0xA3
- Verify TOE HDP activation by reading anywhere in the TOE HDP area a 32-bit word that was programmed with a non-zero value. The read value must be zero.

Errors:

- If the verification value is not zero the TOE HDP area protection is not properly activated. In that case, the product firmware must be restarted.

4.2.2.4 *Flash memory*

To verify the platform identity, the integrator has to verify the platform configuration by reading at the address 0x0BFA0500.

Method of use:

- The CM-33 processor reads at address 0x0BFA0500 and check that the bits 10, 13 and 15 are set. These bits indicate whether the PKA, CCB and SAES IP are enabled or not.

Parameters:

- Address of the platform configuration

Actions:

- The CM-33 processor reads at address 0x0BFA0500.
- Verify that the bits 10, 13 and 15 are set.

Errors:

- If one of the bits 10, 13 and 15 are not set, then the platform configuration is not correct, and the integrator must not accept the TOE.

4.2.2.5 *True random number generation*

When the platform is not executing the application can use the RNG peripheral to generate true random numbers.

Method of use:

- The firmware interacts with the hardware TRGN through a bank of memory-mapped registers.

Parameters:

- Refer to [RM] section 30.7 RNG registers.

Actions:

- Refer to [RM] section 30.3.4 RNG initialization.
- Refer to [RM] section 30.3.5 RNG operation.
- Refer to [RM] section 30.3.8 RNG low-power use.
- Refer to [RM] section 30.4 RNG interrupts.

Errors:

- Refer to [RM] section 30.3.7 Error management.

4.2.2.6 *Cryptographic functions interface*

The platform provides to the application a set of hardware IP registers to access cryptographic operations and cryptographic key store resources. Some of those cryptographic operations are protected against side-channel attacks (AES, modular exponentiation, signature, ECC scalar multiplication).

Method of use:

- The firmware interacts with the hardware SAES, PKA and CCB through a bank of memory mapped registers, and the embedded RAM in the PKA peripheral.

Parameters:

- Refer to [RM] section 32.8 SAES registers.
- Refer to [RM] section 34.7 PKA registers.
- Refer to [RM] section 34.4 PKA RAM parameters.
- Refer to [RM] section 29.7 CCB registers.

Actions:

- Refer to SAES [RM] sections 32.4, 32.5, and 32.6
- Refer to PKA [RM] sections 34.3, and 34.6
- Refer to CCB [RM] sections 29.4, and 29.6

Errors:

- Refer to [RM] Section 32.4.19 SAES error management.
- Refer to [RM] Section 34.3.8 PKA error management.
- Refer to [RM] Section 29.5.5 CCB error

4.2.2.7 *TAMP peripheral*

The TAMP peripheral is used to protect sensitive data from external attacks

Method of use:

- The integrator needs to activate and configure the system and cryptographic internal tampers detection in the TAMP peripheral when managing following functions:
- Non-volatile derived hardware unique key (DHUK) usage.
- Crypto functions in hardware engines (SAES, AES, HASH, PKA and CCB).

Parameters:

- Refer to [RM] section 44.6 TAMP registers

Actions:

- The tamper detection can be configured for the following purposes:
- Erase the backup registers and other device secrets stored in SRAMs or peripherals listed in [RM] *Table 446: TAMP interconnection*. The list of resources protected by tamper is configurable thanks to TAMP_RPCFGR.
- Block the read/write access to the backup registers and other device secrets stored in SRAMs or peripherals listed in [RM] *Table 446: TAMP interconnection*. The list of resources protected by tamper is configurable thanks to TAMP_RPCFGR.
- Generate an interrupt, capable to wake up from low-power modes.
- Generate a hardware trigger for the low-power timers, or an RTC timestamp event.
- Refer to TAMP [RM] Section 44.3.12 Tamper detection configuration and initialization

Errors:

- To avoid false detection, it is possible to configure each tamper source in potential mode, so that the erase is not launched by hardware on tamper detection. The erase can then be launched by software after software checks. Refer to section Tamper detection in section 44.33.9 to [RM].

4.2.2.8 *DBGMCU*

The device and revision identifier (REV_ID, DEV_ID) of the platform are stored in DBGMCU registers (DBGMCU_IDCODE).

Method of use:

- The integrator needs to interact with DBGMCU registers to retrieve the device and revision identifier of the platform (REV_ID, DEV_ID).

Parameters:

- REV_ID and DEV_ID are stored in DBGMCU_IDCODE register.

Actions:

- The integrator accepts a microcontroller part of the STM32U3 series by reading, with STM32CubeProgrammer, the DBGMCU_IDCODE register value as defined in [RM] below

Errors:

- RDP level remains set to level 2, if the wrong password is provided or the sequence is not respected.
- If the DBGMCU_IDCODE value does not correspond to STM32U385xx version 1.3 (revX), the integrator should not accept this microcontroller.

4.2.2.9 *Reset and Clock Control (RCC) peripheral*

The application can use the RCC to manage the different kinds of reset and generates all clocks for the bus and peripherals. At startup the MSIS is used as system clock source after startup from reset, configured at 12MHz. The application can use different clock sources to drive the system clock and configure additional clock sources.

Method of use:

- The firmware interacts with the RCC through a bank of memory-mapped registers.

Parameters:

- Refer to [RM] section 10.5 RCC registers.

Actions:

- Refer to [RM] section 10.2.2 RCC reset functional description
- Refer to [RM] section 10.2.3 RCC clock functional description
- Refer to [RM] section 10.3 RCC in low-power modes
- Refer to [RM] section 10.4 RCC interrupts.

Errors:

- If a clock source that is not yet ready is selected, the switch occurs when the clock source becomes ready. Status bits in the *RCC clock control register (RCC_CR)* indicate which clocks are ready and which clock is currently used as a system clock. Refer to [RM] section 10.2.3 RCC clock functional description.

4.2.2.10 *CPU*

The CPU executes application code by fetching instructions from memory, processing data, and storing results back into memory. It uses system registers to manage control and configuration tasks, ensuring proper operation and interaction with peripherals.

Method of use:

- The CPU fetches instructions from memory to execute.
- The CPU reads data from memory or peripheral registers.
- The CPU writes data to memory or peripheral registers.

Parameters:

- Program Counter (PC), memory address, data size, data value
- Refer to [PM0264] section 2.1.3 Core registers
- Refer to [PM0264] section 3.1 Instruction set summary

Actions:

- fetch instructions from the specified memory address.
- Read and write data from the specified memory address or peripheral register.
- Refer to [PM0264] section 2.3 memory model

Errors:

- Faults can occur on instruction fetches, instruction execution, and data accesses. Refer to [PM0264] section 2.6 Fault handling

4.2.3 Security-relevant events (AGD_OPE.1.4C)

Once configured according to Section 3.2: Secure installation and preparation (AGD_PRE.1.2C), the platform detects any unauthorized access and any unexpected configuration:

- Erroneous values found in the option bytes of the security configuration at boot time:
- Cancel the boot sequence by resetting or blocking the platform (integrator-defined implementation)
- Illegal access in the HDP securable memory area:
- Read returns zero.
- Write causes a bus error. The integrator firmware can implement an error handler.
- Attempt to reprogram the security option bytes in RDP level 2:
- Status FLASH_SR.OPTWERR raised with a possible interrupt by a user implementation defined error handler.
- Closed JTAG/SWD access violation:
- The connection request is not transmitted to the access port and debug port. The request is ignored.
- generation of internal tamper (tamp_itamp6 input)
- Attempts to compromise RNG entropy properties by disturbing physical RNG interfaces:
- The RNG hardware raises alarms on clock and noise source defects with a possible interrupt toward a user implementation-defined error handler.
- Detection of attacks to RNG, SAES, CCB, and PKA by an attacker with physical access
- Peripheral goes to locked mode + generation of internal tamper (tamp_itamp9 input), disabled by default.

4.2.4 Security measures (AGD_OPE.1.6C)

This section describes, as the user role of the integrator, the security measures to be followed to fulfil the security objectives for the operational environment as described in [ST] section 2.1.

To achieve TRUSTED_INTEGRATOR and LIFECYCLE., the following measures must be taken:

- Verify the genuineness of the TOE as described in Section 3.1: Secure acceptance.
- Follow all guidelines described and referenced in section 3.2 Secure installation and secure preparation of the operational environment (AGD_PRE.1.2C).
- Follow all guidelines described in section 4.2.1 User-accessible functions and privileges (AGD_OPE.1.1C) and section 4.2.2 Available interfaces and methods of use (AGD_OPE.1.2C and AGD_OPE.1.3C) regarding the implementation of the non-platform required firmware described in [ST] section 1.4.5.
- In manufacturing phase, the integrator must securely provision the TOE immutable data specific to the integrator or specific to the product as stated in the product firmware HDP securable memory area of section 4.2.1 User-accessible functions and privileges (AGD_OPE.1.1C).
- Once the integrator finishes the production of a final user application, they must set the MCU hardware static protections as stated in section 3.3 Secure installation. To protect the complete product including the user application, the final product state must be RDP2.

To achieve UNIQUE_ID and KEY_MANAGEMENT, the following measures must be taken:

- The integrator must protect the integrity of the Immutable Root of Trust of the non-platform required firmware ([ST] section 1.4.5) until it is programmed and properly protected inside the securable memory area for each device.
- The persons responsible for the application of the procedures described in section 3 Section 3: TOE Preparative procedures, and the persons involved in the delivery and protection of the product must have the required skills and must be aware of the security issues.
- In the case that any part of the preparative procedures of the platform or a party other than the integrator integrates any part of the preparative procedures of the integrated platform, the integrator must guarantee sufficient guidance is provided to this party.
- The integrator can define any type of immutable data unique per product that might allow product identification after its field deployment. It is recommended that the integrator puts in place a data management process, possibly based on database solution, ensuring new unique data generation.
- The integrator must protect the integrity of all the data protected in the HDP securable memory area until they are provisioned and properly protected inside the platform of each device. Moreover, the integrator must protect the confidentiality of the secret data that are stored in the HDP securable memory area.
- Once immutable data of the non-platform required firmware are generated for a new product, the integrator must program them in the defined format at the correct location corresponding to the securable memory area and must protect them as described in section 3.3 Secure installation.
- The integrator must protect the integrity and confidentiality of the cryptographic secret keys encapsulated in the root parameters as defined in section 4.2.1.

4.2.5 Modes of operation (AGD_OPE.1.5C)

This section identifies all possible modes of operation of the platform (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

4.2.5.1 Normal boot mode

After reset, the platform is forced to boot into the non-platform required secure firmware. The security configuration, dictated by Section 3.2: Secure installation and preparation (AGD_PRE.1.2C), unauthorizes all the other alternative boot modes.

Revision history

Table 6. **Revision history table**

Date	Revision	Changes
09-Sep-2026	1	Initial release

Contents

1 General information 2
2 Reference documents 3
3 TOE preparative procedures 4
3.1 Secure acceptance 4
3.2 Secure installation and preparation (AGD_PRE.1.2C) 5
3.2.1 Hardware setup procedure 5
3.2.2 Software setup procedure 6
3.3 Secure installation 6
3.3.1 Step 1: Software programming 6
3.3.2 Step 2: Static security protection programming 6
3.3.3 Certified configuration 7
4 Operational user guidance 8
4.1 User roles 8
4.2 Operational guidance for the integrator roles 8
4.2.1 User-accessible functions and privileges (AGD_OPE.1.1C) 8
4.2.2 Available interfaces and methods of use (AGD_OPE.1.2C and AGD_OPE.1.3C) 10
4.2.3 Security-relevant events (AGD_OPE.1.4C) 14
4.2.4 Security measures (AGD_OPE.1.6C) 15
4.2.5 Modes of operation (AGD_OPE.1.5C) 16
Revision history 17
List of tables 19
List of figures 20

List of tables

Table 1. Applicable products . . . 1
Table 2. Specific acronyms . . . 2
Table 3. List of reference documents . . . 3
Table 4. Applicable products . . . 5
Table 5. Product configuration . . . 5
Table 6. Revision history table . . . 17

List of figures

Figure 1. QA sealed tape closing the inner box (1) 4
Figure 2. QA sealed tape closing the inner box (2) 4
Figure 3. Sealed dry bag (vacuum closed) including the final product 5
Figure 4. TOE certified configuration 7
Figure 5. Figure 2. TOE perimeter 8

IMPORTANT NOTICE – 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.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The 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 acknowledgment.

The 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 the 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.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, 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.

© 2026 STMicroelectronics – All rights reserved