STM32TRUSTEE-SM

Errata sheet

SMAK binary software errata

Introduction

This document applies to the binary of the Secure Manager access kit (SMAK), which is part of the STM32Trust TEE Secure Manager (STM32TRUSTEE-SM).

In this document, X-CUBE-SEC-M is used to refer to any SMAK binary reference. The X-CUBE-SEC-M references concerned by the errata in this document are summarized in Table 1.

Table 1. **Summary of impacted X-CUBE-SEC-M references**

X-CUBE-SEC-M reference[1]
X-CUBE-SEC-M-H5

1. Refer to each erratum for the references and versions considered.

1 General information

The SMAK binary runs on STM32 microcontrollers based on the Arm® Cortex® processor with Arm® TrustZone®.

This document describes the errata of the X-CUBE-SEC-M Secure Manager encrypted binary used for production purposes.

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

2 Summary of errata

The software errata are defined by their status:

- A = workaround available
- N = no workaround available
- P = partial workaround available
  An erratum workaround is deemed partial if
  - either it only reduces the rate of occurrence, or the consequences, or both
  - or if it is effective only for a subset of applicable references or versions
  - or it is a combination of both

2.1 Software errata

Table 2 gives a reference to the software errata and their status.

Table 2. **Summary of software errata**

Section	Erratum	Status
3.1.1	Low power management: the system cannot stay in low-power mode when the Secure Manager is installed	N
3.1.2	PSA firmware update: installation of images with dependency is not supported	P
3.1.3	Secure module with device specific license is not supported	N
3.1.4	STiRoT fails if a tamper event arises during the startup	N

3 Description of software errata

3.1 X-CUBE-SEC-M Secure Manager binary

3.1.1 Low power management: the system cannot stay in low-power mode when the Secure Manager is installed

3.1.1.1 *Applicability*

Table 3. **Applicability (low-power mode erratum)**

X-CUBE-SEC-M reference	X-CUBE-SEC-M profiles	X-CUBE-SEC-M versions
X-CUBE-SEC-M-H5	Large	Up to v1.1.2

3.1.1.2 *Erratum details*

3.1.1.2.1 Description

The Secure Manager is based on a 10 ms secure SysTick that cannot be disabled. This secure SysTick prevents the system from remaining in low-power mode.

3.1.1.2.2 Workaround

No workaround is available.

3.1.2 PSA firmware update: installation of images with dependency is not supported

3.1.2.1 *Applicability*

Table 4. **Applicability (PSA firmware update erratum)**

X-CUBE-SEC-M reference	X-CUBE-SEC-M profiles	X-CUBE-SEC-M versions
X-CUBE-SEC-M-H5	Large	Up to v1.1.2

3.1.2.2 *Erratum details*

3.1.2.2.1 Description

The PSA firmware update service supports image installation with image dependency verification. The `psa_fwu_install()` service verifies the image version dependency before installing the images. The Secure Manager does not accept the installation of an image with dependency if the dependent image is not already installed.

3.1.2.2.2 Workaround

- If an image A depends on an image B, the update agent (in the cloud) must install the image B before the image A.
- If the images A and B are interdependent, there is no workaround because the Secure Manager cannot ensure the installation of both images at the same time (same installation). This is the case if a reset occurs between the image A and image B installation requests.

3.1.3 Secure module with device specific license is not supported

3.1.3.1 Applicability

Table 5. Applicability (secure module erratum)

X-CUBE-SEC-M reference	X-CUBE-SEC-M profiles	X-CUBE-SEC-M versions
X-CUBE-SEC-M-H5	Large	From v1.0.0

3.1.3.2 Erratum details

3.1.3.2.1 Description

Secure modules with device specific licenses are not supported.

Note: Such secure module installation requires STM32HSM.

3.1.3.2.2 Workaround

No workaround is available.

3.1.4 STiRoT fails if a tamper event arises during the startup

3.1.4.1 Applicability

Table 6. Applicability (STiRoT failure erratum)

X-CUBE-SEC-M reference	X-CUBE-SEC-M profiles	X-CUBE-SEC-M versions
X-CUBE-SEC-M-H5	Large	Up to v1.2.1

3.1.4.2 Erratum details

3.1.4.2.1 Description

If a tamper event (on tamper 9 or tamper 15) arises during the startup, the execution remains in an infinite loop, failing to jump to the user application code.

In this situation, the only way to quit the infinite loop and restart the device is to remove all power supplies (also on the VBAT pin), then power the device back on.

3.1.4.2.2 Workaround

No workaround is available.

Warning: *STMicroelectronics advises users against using version v1.2.1 for any production purposes. Users must base their products on the X-CUBE-SEC-M v2.0.0.*

4 Acronyms

Table 7 defines the acronyms needed for a better understanding of this document.

Table 7. List of acronyms

Acronym	Description
SEC-M	Secure Manager
STM32HSM	STM32 hardware security module

Revision history

Table 8. **Document revision history**

Date	Revision	Changes
03-Nov-2023	1	Initial release.
30-Aug-2024	2	Updated versions in the applicability sections: *Section 3.1.1.1*, *Section 3.1.2.1*, and *Section 3.1.3.1*.
10-Apr-2025	3	STiRoT failure erratum for tamper events occurring during startup: • Added Section 3.1.4: STiRoT fails if a tamper event arises during the startup • Updated Table 2. Summary of software errata

Contents

List of tables

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. 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.

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, 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.