Security Target for GD32F503xx/F505xx Arm®-based 32-bit MCU

Version 1.3, dated 2026-08-12

Gigadevice

Based on [2] methodology, version "Public Release v1.2, July 2023"

Revision History

Version	Date	Changes
1.0	2026-05-07	Initial release
1.1	2026-05-19	1.Update Section “Cryptographic Operation”. 2.Update Section “Verification of Platform Identity”. 3.Add Section “Verification of Platform Instance Identity”.
1.2	2026-07-20	1.Update Section “Platform Functional Overview and Description”.
1.3	2026-08-12	1.Update Section “ST Reference” to identify the SESIP profile

1 Introduction

The Security Target describes the GD32F503xx/F505xx Arm®-based 32-bit MCU and the exact security properties of the platform that are evaluated against SESIP.

1.1 ST Reference

See title page. And the SESIP profile is GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs, Version 1.1[1].

1.2 Platform Reference

The Target of Evaluation (TOE) for this Security Target is:

Table 1. TOE reference

Reference	Value
Platform name	GD32F503xx/F505xx Arm®-based 32-bit MCU
Platform version	Rev 0.0
Platform identification	GD32F503xx, GD32F505xx
Platform Type	General purpose microprocessor device for IoT, industrial, or consumer applications

1.3 Conformance Statement

This Security Target conforms to the requirements of the GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs, version 1.1 [1]. The conformance is specified as follows:

Table 2. Conformance Statement

Conformance Item	Statement
Conformant Protection Profile	GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [1]
Security Package	Base SP, Package Security Services, Additional SFR (Verification of Platform Instance Identity)

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 3. Guidance Documents

Reference	Name	Version
[5]	GD32F50x User Manual	1.4
[6]	Device limitations of GD32F50x	1.1
[7]	AN270 GD32F50x Software Development Guide	1.2
[8]	AN278 GD32F50x Hardware Development Guide	1.0
[9]	GD32F50x Secure Installation and Acceptance Procedures	1.0

1.5 Platform Functional Overview and Description

The platform in the GD32F503xx/F505xx series is a high-performance device suitable for a wide range of interconnection and advanced applications, especially in areas such as industrial control, consumer and handheld equipment, embedded modules, human machine interface, security and alarm systems, graphic display, audio player, automotive navigation, drone, IoT and so on. GD32F503xx/F505xx operating at a maximum frequency of 280 MHz frequency with Flash security protection to prevent illegal code/data access. It provides up to 1024 KB main Flash memory, 192KB SRAM memory. An extensive range of enhanced I/Os and peripherals connected to two APB buses. The FMC supports functions required for on-chip flash memory, such as erase and program operations. The platform also supports an OTP (One-Time Programmable) memory area, hardware AES and HASH acceleration engines, and a TRNG (True Random Number Generator). It allows the debug port to be permanently disabled to support secure debugging.

1.5.1 Platform Type and Scope

GD32F503xx/F505xx is a general-purpose microprocessor with OTP memory, flash protect, security configuration, cryptographic accelerators, and true RNG. The platform does not contain any software or firmware.

1.5.2 Major Functions and Security Features Overview

GD32F503xx/F505xx is a general-purpose MCU designed with security feature for *IoT, industrial, or consumer applications*. Its major security features include:

- Verification of Platform Identity: The platform provides a unique identification of the platform.
- Residual information purging: when the SPC level is downgraded from a lower protection level to unprotected, the data in the flash is automatically erased.
- Secure debugging: the chip debugging function can be permanently disabled by configuring the OTP field or setting the SPC to a high protection level.

- Cryptographic operations, based on hardware cryptographic accelerators, include AES algorithm and HASH algorithm.
- Cryptographic Random Number Generation, based on True Random Number Generator (TRNG)

Regarding security features, note the following:

- Secure initialization: This platform is hardware only with no firmware.
- The secure update is not applicable to this platform because the platform does not include firmware, and the hardware part cannot be updated.

1.5.3 Platform Physical Scope

The physical scope of the TOE is the GD32F503xx/F505xx integrated circuit (IC) itself, that is, all silicon functional modules within the chip package. All elements outside the TOE package boundary (such as PCB, external Flash, sensors, communication modules, etc.) are not within the physical scope. The platform definition is identical across all devices in the series.

An overview of the GD32F503xx/F505xx microcontroller is shown in the block diagram below as shown in Figure 1.

The physical boundary of the TOE is the GD32F50x silicon die within the package. This includes all on-chip Flash memory, SRAM, OTP areas, cryptographic peripherals (CAU, HAU, TRNG), the Flash Memory Controller (FMC) with security protection logic, and the debug port (SWJ-DP).

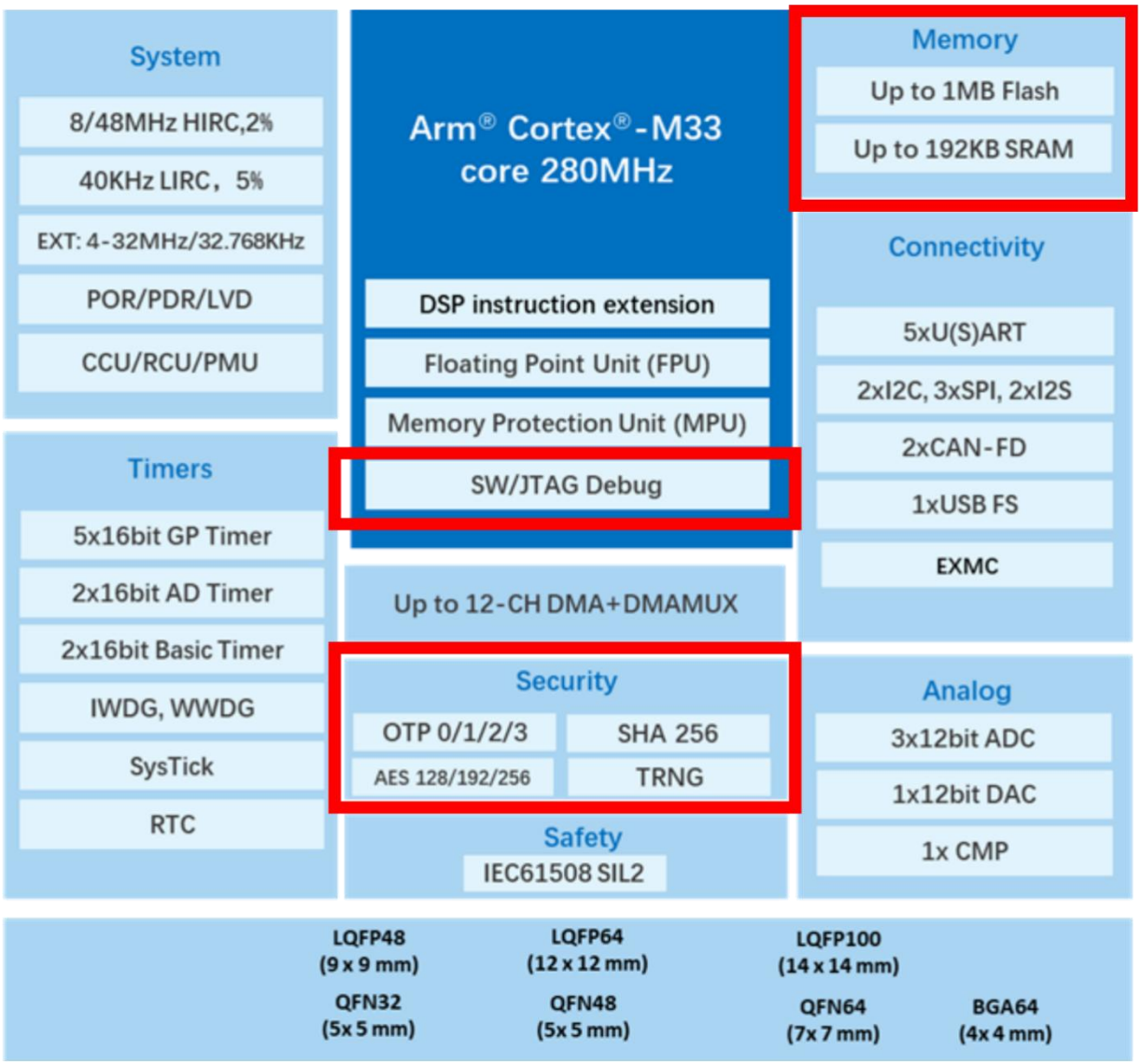

Figure 1. Platform physical scope

1.5.4 Platform Logical Scope

The TOE does not include any software components, and it only contains hardware security mechanisms. The logical scope consists of a security approach as depicted in Figure 2.

The core security services provided by the TOE include:

Platform identity based on OTP storage.

Booting from OTP1.

Hardware AES-ECB encryption/decryption (128/192/256 bits).

Hardware SHA-256 hash computation.

True Random Number Generation (TRNG).

Secure key storage based on OTP2, with read-hide capability.

Flash protection.

Debug protection.

Residual information clearing.

The following components are out of the evaluation scope:

Application software running on the MCU.

Non-secure hardware peripherals (USB, UART, SPI, I2C, Ethernet, etc.).

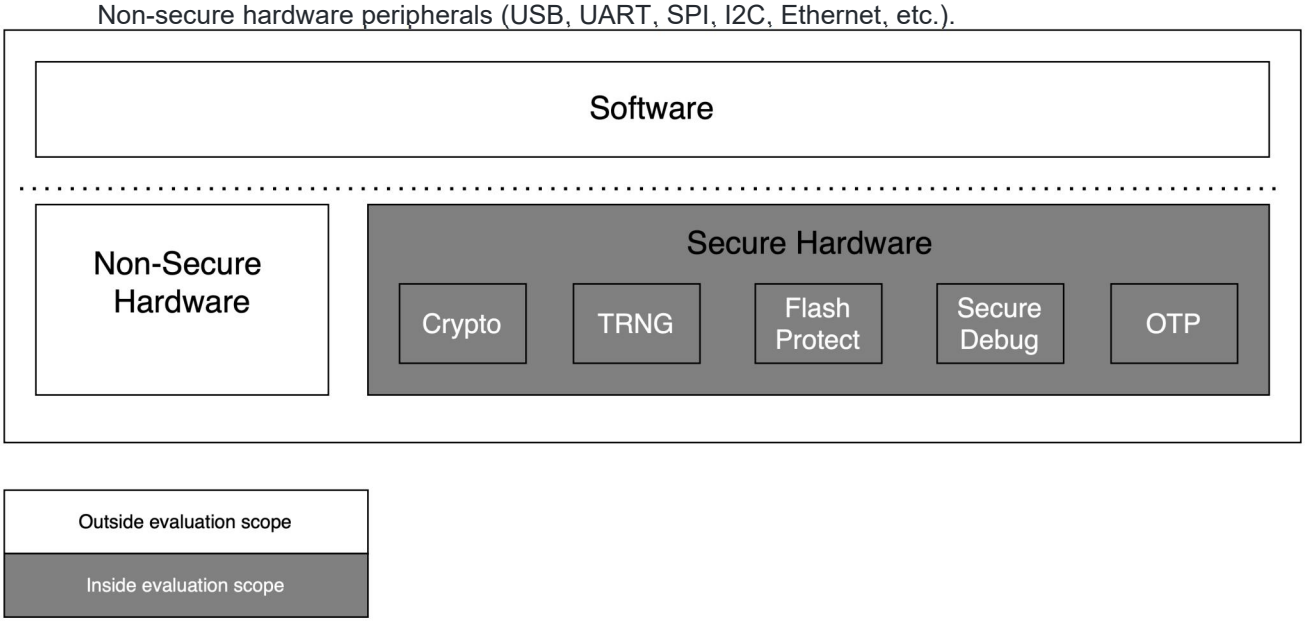

Figure 2. Platform logical scope

1.5.5 Non-TOE Hardware/Software/Firmware

If secure boot and an immutable platform root of trust are to be configured on this platform, the platform requires a secure boot firmware to perform, at a minimum, the following operations on the platform itself:

Verify non-volatile parameters configured according to the lifecycle state;

When transitioning from the first-stage immutable secure boot (code in OTP1) to the second-stage updatable firmware (code in main Flash), configure the OTP1REN[15:0] bits in the FMC_OTP1CFG register to activate protection for the OTP1 region, thereby preventing subsequent application code from accessing the immutable root of trust.

The secure boot firmware may also support additional security features, such as:

Verifying the authenticity and integrity of next-stage firmware and data;

Secure updates of next-stage firmware.

However, these additional features are not required by the Security Functional Requirements (SFRs) claimed by the platform.

1.5.6 Life Cycle

GD32F503xx/F505xx has 5 life cycle states, as shown in Table 4

Table 4. Life Cycle States

LC State	Description
Factory	IC manufacturing completed.
Provisioned	The integrator programs firmware, configuration parameters and keys.
Field	Set SPC to Level 1 or Level 2; debug interface locked or not.
Operational	Device operates normally in the end-user environment.
Decommissioned	Physical destruction.

1.5.7 Use case

The environmental conditions under which the TOE in certified configuration can be securely used are defined below:

- **[Trusted user only]** The product operates in a controlled environment (industrial or private domain), where physical attackers other than the legitimate device owner can be reasonably excluded.
- **[Trusted code only]** The platform only executes code that has been verified and authorized by the integrator; no unverified third-party code is executed.

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

For the platform to fulfill its security requirements, the operational environment (technical or procedural) shall fulfil the following objectives.

Table 5: Objectives for the Operational Environment

State Security Objective	Security Objective Description	Reference
Secure acceptance	The platform integrator is expected to verify the correct version of all platform components that it depends on.	section 1 of [9]
Security guidance application	The platform integrator shall follow all platform security guidelines provided in the platform documentation or provide a justification and a workaround ensuring an equivalent level of security.	[5][6][7][8]

Secure boot usage	This platform is hardware only with no firmware.	NA
Sensitive material secure handling	The development and operational environment shall implement protections of any material it handles and involved in the platform security at the same level of security as the platform.	No Sensitive material.
Secure environment	The operational environment must protect the TOE against physical access of attackers wherever needed.	Section 1.5.7
Trusted code	The operational environment must not allow the deployment of untrusted code. That means that all code running on the product is known to the product vendor and the product vendor can confirm that the code cannot harm the claimed security functionalities.	Section 1.5.7

3 Security Requirements and Implementation

This chapter details the Security Assurance Requirements (SARs) and Security Functional Requirements (SFRs) that the TOE must fulfill to meet its security objectives, along with an overview of the implementation of the SFRs.

3.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP2 as defined in [1].

3.1.1 Flaw Reporting Procedure (ALC_FLR.2)

The secure update is not applicable to this platform because the platform does not include firmware, and the hardware part cannot be updated. The SFR secure update of the platform is not applicable since the implemented hardware is not reprogrammable.

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to generate any needed update and distribute it. The developer has defined the procedure in https://www.gigadevice.com/solution/key-technologies/cybersecurity/gd-psirt. After submission, GigaDevice PSIRT will manage reported potential security vulnerabilities according to the following process:

- Receipt Confirmation: GigaDevice PSIRT will promptly respond to confirm receipt of your report.
- Assessment: GigaDevice PSIRT will evaluate the potential vulnerability, conduct analysis, and set priorities. We may contact you if the original report lacks certain information or requires clarification.
- Resolution: GigaDevice PSIRT will investigate solutions and mitigation measures to address valid issues.
- Disclosure: When appropriate, GigaDevice will publish security advisories according to Coordinated Vulnerability Disclosure (CVD) principles, provide remediation and mitigation measures, and acknowledge contributors in the advisory (if you agree).

3.2 Security Functional Requirements

3.2.1 Base SP Security Functional Requirements

As a base, the platform fulfils the following Security Functional Requirements:

3.2.1.1 Verification of Platform Identity

The platform provides a unique identification of the platform, including all its parts and their versions.

Conformance rationale:

The platform identification can be done through data stored in the Product ID register (FMC_PID). The data is one-time programmable at the time of chip fabrication.. A detailed information is described in clause 5.4.16 of

错误！未定义书签。. MCU hardware PID and revision, at 0x40022100 and 0x40022106 addresses. The PID is a halfword formed by concatenating the byte at address 0x40022103 with the byte at address 0x40022100. The version number is a halfword located at address 0x40022106.

PID: 0x6233, meaning GD32F503xx; PID: 0x6235, meaning GD32F505xx

Revision: 0xFFFF, meaning V0.0

3.2.1.2 Secure Initialization of Platform

~~The platform ensures its integrity and authenticity during platform initialization. If platform integrity or authenticity cannot be ensured, the platform will go to next controlled states.~~

Non-conformance rationale:
This platform is hardware only with no firmware.

3.2.1.3 Secure Update of Platform

~~The platform can be updated to a newer version in the field such that the confidentiality, integrity and authenticity of the platform is maintained.~~

Non-conformance rationale:
The secure update is not applicable to this platform because the platform does not include firmware, and the hardware part cannot be updated.

3.2.1.4 Residual Information Purging

The platform ensures that data stored in main flash, with the exception of none, is erased using the method specified in the rational below before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:
The protection level low performed when setting the option bytes block SPC byte to any value except 0xAA or 0xCC. The main flash can only be accessed by user code. In debug mode, boot from SRAM or boot from boot loader mode, all operations to main flash are forbidden. If a read operation is executed to main flash in debug mode, boot from SRAM or boot from boot loader mode, a bus error will be generated. If program back to no protection level by setting SPC byte to 0xAA, a mass erase for main flash will be performed. A detailed

information is described in clause 5.3.11 of [5]. The platform also provides the capability for page erase and mass erase, which are implemented through setting the PER and MER bits in the FMC_CTLx register.

3.2.1.5 Secure Debugging

The platform provides two debug interfaces: Serial Wire Debug (SWD) interface and JTAG interface.
The platform ensures that code and data stored in the Flash memory, with the exception of no data, is made unavailable.

Conformance rationale:

The Flash memory controller (FMC) provides a security protection function to prevent illegal code/data access on the Flash memory. There are 3 levels for protecting:

- No protection, the main flash and option bytes block are accessible by debug mode.
- Protection level low, in debug mode, all operations to main flash is forbidden. If a read operation is executed to main flash, a bus error will be generated. If a program/erase operation is executed to main flash, the WPERR bit in FMC_STATx register will be set.
- Protection level high, when this level is programmed, debug mode is disabled.

The debug mode is locked and cannot be turned on again when the data block corresponding to the 0 lock block of the OTP3 block is not all 1.
A detailed information is described in clause 5.3.10 and 5.3.11 of [5].

3.2.2 Package 'Security Services' Security Functional Requirements

3.2.2.1 Cryptographic Operation

The platform provides the application with list of cryptographic operations/algorithms/specifications/key lengths/modes specified in Table 6.

Table 6: Cryptographic Operation

Operations	Algorithm	Specification	Key lengths	Modes
Encryption and decryption	AES	Federal Information Processing Standards Publication 197 NIST SP 800-38A	128, 192, 256	ECB
Hash	SHA-256	Federal Information Processing Standards Publication 180-4	256	-

Conformance rationale:

The Cryptographic Acceleration Unit (CAU) and Hash Acceleration Unit (HAU) are supported in GD32F50x.

3.2.2.2 Cryptographic Random Number Generation

The platform provides the application with a way based on physical entropy source, seed check, clock check and post-processing to generate random numbers.

Conformance rationale:

The platform provides a physical true random number generator to generate random numbers which can pass AIS 31 statistical tests T0-T8 and NIST SP800-22 test.

3.2.3 Additional Security Functional Requirements

The platform fulfills the following additional security functional requirements defined in [2].

3.2.3.1 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform, including all its parts.

Conformance rationale:

The 96-bit unique device ID is stored in the information block of the Flash memory and is unique for any device. The value is factory programmed and can never be altered by user. A detailed information is described in clause 1.6 of [5].

4 Mapping and Sufficiency Rationales

This chapter argues how the TOE's security requirements address its security objectives and cover the environmental assumptions, and why the selected SARs provide sufficient assurance for the implementation of the SFRs.

4.1 SESIP2 Sufficiency

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in the Title, the platform reference is in the Section 1.2 the platform overview and description in the Section 1.5

	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the Operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section 3.2	All SFRs in this ST are taken from [1] and.[2]
	ASE_TSS.1 TOE Summary Specification	Section 3.2	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in Section 3.2 Since the scope only covers the hardware and does not include secure update or secure initialization.
ADV: Development	ADV_FSP.4 Complete functional specification	Materials provided to evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.4	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.4	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Materials provided to evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA_VAN.2	AVA_VAN.2 Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of	The platform evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the platform. Penetration testing is performed by the platform evaluator

		potential vulnerabilities.	assuming an attack potential of Basic.

5 References

[1] SESIP Profile for Secure MCUs and MPUs, Version 1.1

[2] GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP) Methodology, Version 1.2

[3] Common Criteria for Information Technology Security Evaluation, Parts 1, 2 and 3, Version 3.1 Revision 5

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5

[5] GD32F50x User Manual Rev1.4

[6] Device limitations of GD32F50x Rev1.1

[7] AN270 GD32F50x Software Development Guide Rev1.2

[8] AN278 GD32F50x Hardware Development Guide Rev1.0

[9] GD32F50x Secure Installation and Acceptance Procedures v1.0

6 Glossary

Term	Definition
TOE (Target of Evaluation)	The entity under evaluation, specifically GD32F50x in this document.
SESIP	Security Evaluation Standard for IoT Platforms.
SFR (Security Functional Requirement)	A statement describing a specific security behavior or function that must be provided.
SAR (Security Assurance Requirement)	A statement describing activities to gain confidence that the security functions are correctly implemented.

7 Abbreviations

Abbreviation	Full Term
MCU	Microcontroller Unit [1]
MPU	Microprocessor Unit / Memory Protection Unit [1]
RoT	Root of Trust [1]
SAR	Security Assurance Requirement [1]
SESIP	Security Evaluation Standard for IoT Platforms [1]
SFR	Security Functional Requirement [1]
SP	SESIP Profile [1]
ST	Security Target [1]
TOE	Target Of Evaluation (also Platform) [1]
TEE	Trusted Execution Environment [1]
SPC	security protection code [5]