ST0047

Security target

STM32WBA6xxx SESIP

Document information

This document is based on the GlobalPlatform® Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (mid 2024), GP_FST_070.

1 Introduction

This security target describes the STM32WBA6xxx platform and the exact security properties of the platform that are evaluated against the GlobalPlatform® Security Evaluation Standard for IoT Platforms [SESIP].
The Protection Profile reference and conformance claims for this security target are described below.

Table 1. SESIP profile reference and conformance claims

Reference	Value
Protection profile name	SESIP Profile for PSA Certified™ Level 3 iSE/SE and RoT Component [PP]
Protection profile version	2.0 REL 01
Package claim	Verification of Platform Identity, Isolation of Platform, Physical Attacker, Resistance Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic KeyStore
Optional and Additional SFRs	Field return of platform, Secure encrypted storage
Assurance claim	See Section 3.1

1.1 Security target reference

This document: ST0047 STM32WBA6xxx SESIP (July 2025), STMicroelectronics.

1.2 Platform reference

Table 2. Platform reference: STM32WBA6xxx product series

Reference	Value
Platform name	STM32WBA6xxx series Arm®-based 32-bit MCUs
Platform version	1.1
Platform identification	0x4B0
Platform type	BLE & 802.15.4 wireless microcontroller series for IoT, industrial, or consumer applications.

1.3 Included guidance documents

The following documents are included with the platform:

Table 3. Guidance documents

Category	Name	Reference
User manual	SG0048 STM32WBA6xxx security guidance for SESIP level 3 certification	[SG]
Product reference manual	RM0515 STM32WBA6xxx series Arm®-based 32-bit MCUs	[RM]
Product errata	ES0644 STM32WBA6xxx device errata sheet	[ES]

1.4 Platform functional overview and description

1.4.1 Platform type

The platform is a general-purpose microcontroller certified for Bluetooth® Low Energy. It enables seamless integration of wireless communication into the final product in a cost-effective way.

The platform consists of an Arm® Cortex®-M33-based microcontroller with internal flash memories, RAMs, and peripherals. It provides the necessary hardware building blocks for the platform integrator to implement a secure boot with a protected Root of Trust.

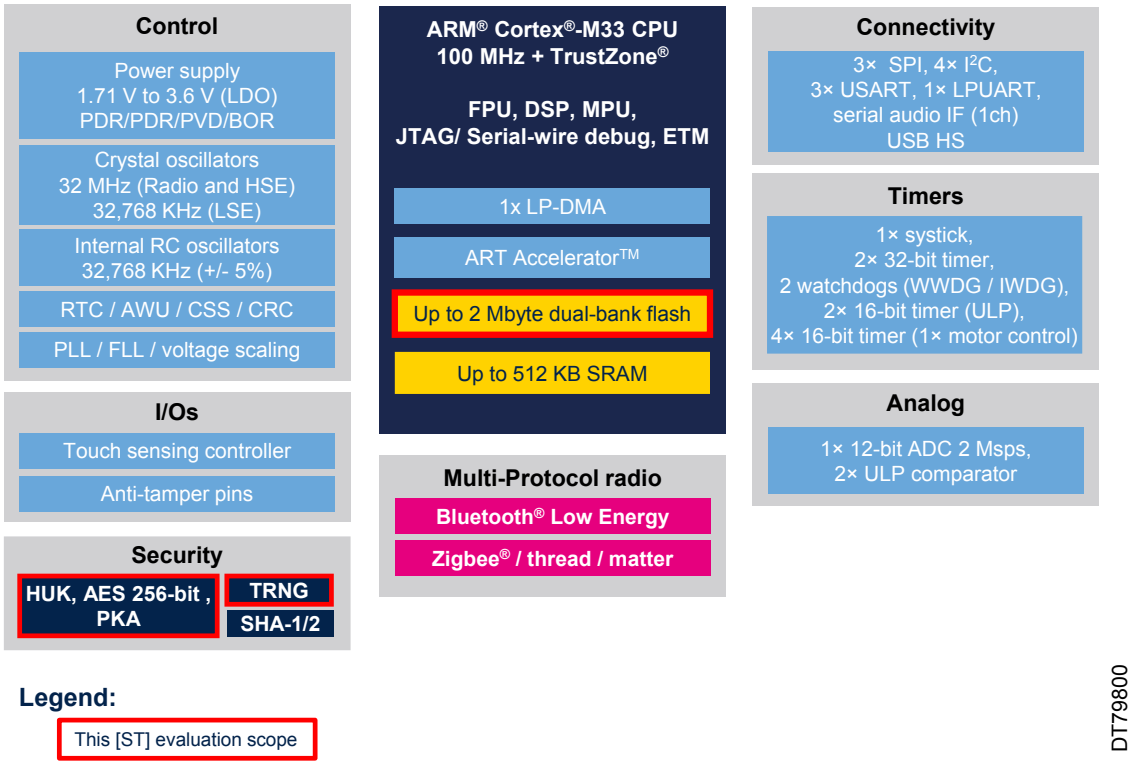
The platform is mainly envisioned to be the lower-level platform part for further composition evaluation activities.

1.4.2 Physical scope

The physical scope of the platform is implemented in the STM32WBA6xxx series of MCU products described in the [RM] reference manual. The block diagram in Figure 1 provides an overview of the major features supported by this MCU. The features in the scope of the platform are highlighted in red.

The platform definition is identical across all devices in the STM32WBA6xxx series.

Figure 1. Platform physical scope



The platform perimeter resides in the components and interfaces listed in Table 4. They are described in the [RM] reference manual, and in [ES] errata sheet.

Table 4. Hardware components and interfaces of the TOE

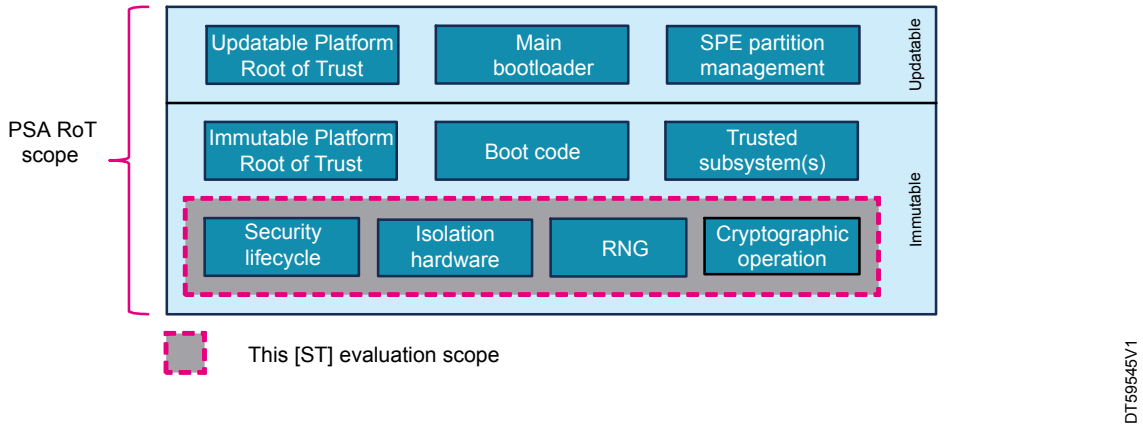
Component/Interface	Description	Identification
CPU	*Not applicable*	Hardware revision(1)
Debug ports	DBGMCU, JTAG/SWD	
Memories	FLASH	
Cryptography	SAES, PKA, RNG	

1. *Refer to the platform version in Table 2 of Section 1.2*

1.4.3 Logical scope

The block diagram in Figure 2 extracted from [PSA-PP] Section 2.4.3 recaps the PSA Root of Trust expectations that are specified in the PSA security model [PSA-SM] document.

Figure 2. Platform logical scope



The logical scope of the platform includes:

- The security lifecycle resources
- The hardware isolation resources
- The cryptographic random number generation
- The cryptographic operations

The logical scope of the platform does not include:

- The immutable platform Root of Trust, for example, the boot code and any root parameters, and the management and enforcement of the isolation and security lifecycle hardware resources.
- The updateable platform Root of Trust, for example, the main bootloader code, the code that implements the SPE partition management function, and the code that implements the PSA-defined services such as attestation, secure storage, and cryptography.
- The trusted subsystem components that the PSA Root of Trust relies on for the protection of its assets or implements some of its services, for example, a subscriber identification module or a secure element.

1.4.4 Usage and major security features

The platform supports the following major security features:

- The RDP level manages the product state in the life cycle. In RDP level 0, the product is fully open for development, debugging, prototyping, and programming of both user flash and user nonvolatile options known as option bytes. In RDP level 1, the product is still open but with limited debug and execution capabilities. In RDP level 2, the product is closed. The nonvolatile configuration cannot be changed and the debug link is locked. The unique boot entry address is necessarily in user flash.
- The securable memory area HDP mechanism manages the flash memory region protection. The main purpose of the securable memory area is to protect a specific part of flash memory against undesired access. After the system reset, the code in the securable memory area can be executed before the securable area becomes inaccessible until the next system reset. This allows the implementation of software security services such as isolation or a secure initialization. The base securable memory area is defined by option byte at manufacturing time and cannot be modified in an RDP level not equal to zero. The code executed in the securable memory area can optionally extend the securable memory area, which is then locked for any later access.
- The RNG peripheral is a NIST-compliant true random number generator that provides full entropy outputs to the application. It is composed of multiple analog noise sources and an internal conditioning component.
- The secure AES peripheral provides encryption, decryption, and authenticated encryption with associated data (AEAD) computation supporting ECB, CBC, CTR, GCM, GMAC, and CCM modes of operation.
- The PKA peripheral provides RSA and ECC cryptography (ECDSA/ECDH/ECIES)

- Platform instance unique key of key length 128-bit and 256-bit, with a value that differs according to the execution context.

Life cycle

The platform life cycle is based on the device RDP mechanism detailed in [RM] Section 3.11.1.

The platform supports the SFR field return of platform as described in Section 3.5.1.

Use case

The platform is intended to be used by an integrator wishing to implement a secure boot with the expected Root of Trust services.

The environmental conditions under which the platform can be securely used are defined below:

- [**Any user**] The product may be physically accessed by an unknown or untrusted user, in an environment where access to the product cannot be sufficiently controlled or even in a more hostile environment.
- **[Any code]** It cannot be excluded that the product executes code that is unknown to the product developer.

1.4.5 Required hardware/software/firmware

As defined in Section 1.4.3 the platform does not include any software component in the evaluation perimeter.

Required nonplatform hardware/software/firmware (ASE_INT.1.6C)

The platform aims to host a secure boot and an immutable platform Root of Trust in a subsequently composed platform as shown in Figure 2 of the platform logical scope.

Consequently, the platform requires a secure boot firmware to achieve at least the following operation on the platform itself:

- Verification of the nonvolatile parameters configured for the state of the life cycle.
- Activation of the HDP securable memory area when switching from the first stage immutable secure boot to the second stage updatable firmware. The HDP activation makes the immutable Root of Trust inaccessible for later application code.

The required nonplatform secure boot firmware expectations are exhaustively described in [SG] Section 4.2.2.

The secure boot firmware might support other security features, such as integrity, verification, or update of the next stage firmware. However, those additional features are not mandatory for the SFRs claimed by the platform.

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) must fulfill the following objectives.

Table 5. Security objectives for the operational environment

ID	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures	[SG], Section 4.2.4 Security measures
TRUSTED_INTEGRATOR	The integrator builds/personalizes the platform and uses the security functionalities needed by the user application following the security guidance documentation. The integrator is trusted and does not attempt to thwart the security functionalities or bypass them	
UNIQUE_ID	The integrator must provide the integrity and uniqueness of the unique identification of the platform during the personalization stage.	
LIFECYCLE	The integrator is expected to configure the nonvolatile product state according to the stage of product development and deployment	

2.2 Inherited objectives for the operational environment

This is inapplicable as the platform is not composite.

3 Security requirements and implementation

3.1 Security assurance requirements

The claimed assurance requirements package is **SESIP Assurance Level 3 (SESIP3)**, as defined in Section 4 of the GlobalPlatform® Technology Security Evaluation Standard for IoT Platforms [SESIP].

3.2 Flaw Reporting Procedure (ALC_FLR.2)

Due to the TOE type, meaning *component of a system on chip hardware*, the SFR secure update of the platform is inapplicable 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 described in [PSIRT].

3.3 Base PP security functional requirements

The platform fulfills the following security functional requirements:

3.3.1 Verification of platform identity

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

Conformance rationale:

The platform referred to in Section 1.2: Platform reference provides the following identifiers:

Field	Address	Halfword value	Comments
Device identifier (DEV_ID)	0xE004 4000	0x4B0	STM32WBA6xxx version 1.1 (rev Z)
Revision identifier (REV_ID)	0xE004 4002	0x1001	

3.3.2 Secure update of the platform

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

Nonconformance rationale:

The platform does not include any firmware component. The implemented hardware is not reprogrammable.

3.3.3 Physical attacker resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

Conformance rationale:

The platform provides the following hardware countermeasures against physical attacks:

- Redundancy checks to prevent RDP and HDP deconfiguration by physical tampering or perturbation.
- Detection of transient perturbation attacks in cryptographic functions (SAES, PKA private operations).
- Prevention of leakage of information via side channels when using the AES algorithm (in SAES) or private key cryptography (in PKA).

3.4 SFRs for PSA-RoT component

The platform fulfills the following security functional requirements:

3.4.1 Software attacker resistance: Isolation of platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

Conformance rationale:

The HDP mechanism prevents any firmware code executed outside the region defined by HDP boundaries from performing any access inside the HDP region. This region can be freely used by the integrator to protect any data or code ensuring the secure initialization of a composite platform.

When TrustZone® configuration is activated via option bytes, the boot region is isolated from NSPE and SPE code when located in the HDP area.

3.4.2 Cryptographic random number generation

The platform provides the application with a way based on an *analog live entropy source* to generate random numbers as specified in [SP 800-90B].

Conformance rationale:

The TOE includes an RNG peripheral compliant with NIST SP800-90B recommendations. The application must use this peripheral to generate true random numbers.

Refer to [RM] Section 25 for details.

3.4.3 Cryptographic operation

The platform provides the *operations* in Table 6 functionality with the *algorithms* in Table 6 as specified in *specifications* in Table 6 for *key lengths* and *modes* described in Table 6.

Table 6. Platform cryptographic operations

Operations	Algorithms	Specifications	Key lengths	Modes
Encryption, decryption	AES(1)	FIPS PUB 197 NIST SP800-38A	128, 256 bits	ECB, CBC, CTR
Authenticated encryption or decryption		NIST SP800-38C NIST SP800-38D		GCM, CCM
Cipher-based message authentication code		NIST SP800-38D		GMAC
Protected modular exponentiation (signature, decryption, key agreement...)	RSA(2)	IETF RFC 8017 NIST SP800-56B FIPS PUB 186-4	Up to 4096 bits	RSA 2048, 3072, 4096
Signature	ECDSA(2)	ANSI X9.62 IETF RFC 7027 FIPS PUB 186-4 SEC 1, SEC 2(3)	Up to 640 bits	Nist: P256, P384, P521 Brainpool: bp256r1, bp384r1, bp512r1 SEC 2(3): secp256k1, secp256r1, secp384r1, secp521r1
ECC scalar multiplication (public key generation, key agreement, shared secret generation...)	ECDH ECIES	ANSI X9.42 ANSI X9.63 FIPS PUB 186-4 SEC 1, SEC 2(3)		

1. *Running in side-channel attack-resistant SAES peripheral.*
2. *Other PKA operations not written in this table (like RSA CRT exponentiation or ECDSA signature verification) are not protected against side-channel attacks.*
3. *Standards for Efficient Cryptography: SEC1, SEC2*

Conformance rationale:

Refer to [RM]:

- Section 27 Secure AES coprocessor (SAES)
- Section 29 Public Key Accelerator (PKA)

3.4.4 Cryptographic KeyStore

The platform provides a way to store cryptographic keys such that not even the application can compromise the confidentiality of this data. This data can be used for the cryptographic operations listed in Section 3.4.3: Table 7, algorithm AES.

Conformance rationale:

The platform provides hardware mechanisms to protect the confidentiality of AES 128 or 256-bit keys. When the user encrypts those keys in the SAES peripheral using the derived hardware unique key (DHUK), they can only be decrypted in this specific device, and the decrypted keys are only available in the SAES write-only key registers. Note that if the application tries to overwrite part of the key, the whole key is erased.

The DHUK is never disclosed to any application code or debugger and is only usable in the side-channel protected SAES peripheral. Refer to *SAES operation with wrapped keys* in [RM] Section 27, for details.

3.5 Additional security functional requirements

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

3.5.1 Field return of platform

The platform can be returned to the vendor without user data.

Conformance rationale:

In the certified configuration, the Integrator allows the platform to regress to RDP Level 1 when the TOE secret OEM2KEY is successfully provisioned, and the OEM2LOCK option bit is set. The detailed sequence “OEM2 unlock sequence B, starting at RDP Level 2” is described Section 3.11.1 of [RM].

When RDP is set to Level 1, flash and protected memories cannot be accessed via the JTAG interface, but it is still possible to do an RDP regression to Level 0 to go to the product's virgin state (flash and protected memories are first erased before reopening the JTAG interface with full debug capabilities).

Note: If the Integrator sets RDP to Level 2 without programming the OEM2KEY the product is locked, and it is not possible to change the RDP level.

3.6 Optional security functional requirements

The platform fulfills the following optional security functional requirements:

3.6.1 Secure encrypted storage

The platform ensures that all data stored by the application, except for the data stored outside the region encrypted by SAES using DHUK, is encrypted as specified in Table 7 with a platform instance unique key of the key length described in Table 7.

Table 7. Secure encrypted storage cryptographic operations

Operations	Algorithms	Specifications	Key lengths	Modes
Authenticated encryption or decryption	AES(1)	NIST SP800-38C NIST SP800-38D	128, 256 bits	GCM, CCM

1. *AES algorithm running in SAES peripheral (with side-channel resistance).*

Conformance rationale:

As described in the conformance rationale of Section 3.4.4, any data encrypted with the DHUK can only be decrypted in this specific device, DHUK is never disclosed to any application code or debugger and is only usable in side-channel protected SAES peripheral.

Refer to *SAES key registers* in [RM] Section 27, for details on selecting DHUK for any supported AES operation.

4 Mapping and sufficiency rationales

4.1 SESIP3 Sufficiency

Table 8. SESIP3 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 TOE reference in the “Platform Reference”, the TOE overview and description in “Platform Functional Overview and Description”.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in “Security Objectives for the Operational Environment” refer to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section 3.3 to Section 3.6	All SFRs in this ST are taken from [SESIP]. “Verification of Platform Identity” is included. “Secure Update of Platform” is not included with justification in ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in “Security Functional Requirements”.
ADV: Development	ADV_FSP.4 Complete functional specification	Section 1.3, and material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Material provided to the 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 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_CMS.1 TOE CM Coverage	Section 5, and material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_FLR.2 Flaw reporting procedures	Section 3.2	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA_VAN.3	AVA_VAN.3 Focused Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities.	The platform evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the platform evaluator assuming an attack potential of Enhanced-Basic.

5 Documentation references

Table 9. **References**

Reference	Definition
Evaluation documents	
[SESIP]	Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (June 2023), GlobalPlatform, GP_FST_070
[PP]	SESIP Profile for PSA Certified™ Level 3 iSE/SE and RoT Component, version 2.0 REL 02, JSADEN018
[PSA-PP]	SESIP Profile for PSA Certified Level 3, version 1.0 REL 02, JSADEN011
[SP 800-90B]	NIST Special Publication (SP) 800-90B (Draft), Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018
[PSA-SM]	Platform Security Model 1.1, (01/12/2021), JSADEN014
Developers documents	
[SG]	SG0048 STM32WBA6xxx security guidance for SESIP level 3 certification, STMicroelectronics, rev 1
[RM]	RM0515 STM32WBA6xxx series Arm®-based 32-bit MCUs, STMicroelectronics, rev 2
[ES]	ES0644 STM32WBA6xxx device errata sheet, STMicroelectronics, rev 1
[PSIRT]	DM00882158, PSIRT ST PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT) MANAGEMENT, rev 1.0

6 Glossary

Table 10. **Glossary**

Term	Definition
Application	Used in SESIP to refer to the components that are out of the scope of the evaluation.
Hardware Unique Key	Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust. It is a critical security parameter.
Platform	Used in SESIP to refer to the components that are in the scope of the evaluation. It is a synonym for connected platform.
Product	Used by SESIP as a synonym for connected product
PSA Root of Trust	PSA-defined combination of the immutable platform Root of Trust and the updateable platform Root of Trust. It is the most trusted security component on the device. See [PSA-SM].

7 Abbreviations

Table 11. **Abbreviations**

Term	Definition
DHUK	Derived hardware unique key
HDP	Hide data protection
HUK	Hardware unique key
NSPE	Non-Secure processing environment
PRoT	Platform Root of Trust
PSA	Platform security architecture
RDP	Read data protection
RoT	Root of Trust
RNG	Random number generator
SFR	Security functional requirement
SPE	Secure processing environment
TOE	Target of evaluation

Revision history

Table 12. **Document revision history**

Date	Revision	Changes
24-Jul-2025	1	Initial release.

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.

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.