STSAFE-A120 SPL05 generic sample profile description

Introduction

This application note provides an overview of the SPL05 personalization profile used to configure generic STSAFE-A120 samples. This profile provides a flexible STSAFE-A120 configuration for secure cryptographic operations and secure data storage, making it suitable for a wide range of applications.

The SPL05 generic profile includes the following STSAFE-A120 personalization options:

- Preprovisioned NIST-P256 private key (slot 0): Associated with a unique X.509 leaf certificate stored in user-nvm slot 0. The device leaf-certificate is compatible with Amazon™ JIT and Microsoft® Azure® and attested by the ST root Certificate Authority (CA).
- Four available private key slots, for asymmetric cryptography applicative use-case.
- Four provisionable public key slots designed for external entity authentication applicative use-case.
- Sixteen provisionable symmetric key slots: Usable for symmetric cryptography.
- A provisionable host key slot: Enabling secure communication between the host and the secure element.
- One-time programmable command access condition table allowing secure and controlled access to a specific device command set.
- 16 Kbytes of user NVM: Segmented into data and counter zones with configurable access conditions.

Note: Amazon is a trademark of Amazon in the United States and/or other countries.

Note: Microsoft and Azure are trademarks of the Microsoft group of companies.

For further information, refer to the STSAFE-A120 datasheet (DS13039).

1 STSAFE-A120 public key infrastructure (PKI)

The following figure illustrates the STSAFE-A120 SPL05 public key infrastructure (PKI).

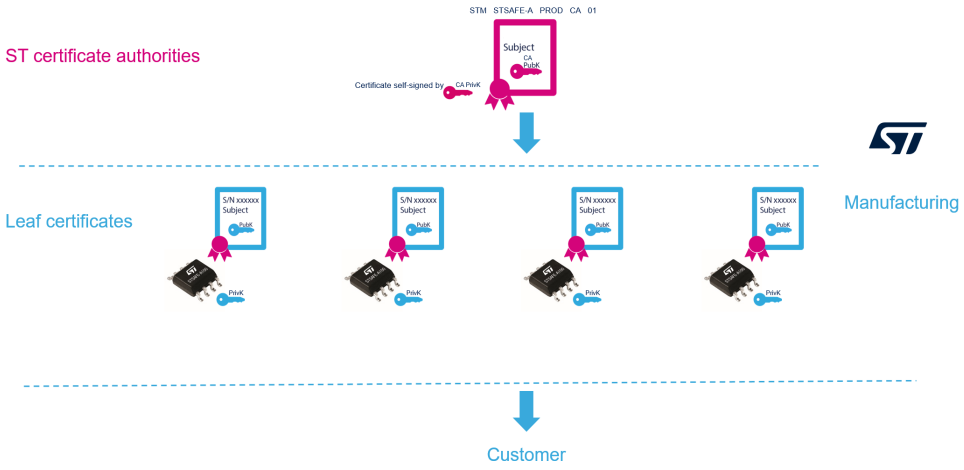
The first level of the PKI is a self-signed root certificate owned by the STMicroelectronics CA, with its dedicated key pair:

- A public key issued by a CA (CA PubK)
- A private key issued by a CA (CA PrivK)

This generic ST CA certificate is available on the STSAFE-A120 web page (tools and software tab) and in the Section 1.1: STM STSAFE-A PROD CA 01 certificate.

Each STSAFE-A120 SPL05 contains a specific private key (privk) and a leaf certificate containing a serial number and a public key (PubK) corresponding to the private key. This leaf certificate is signed by the private key (CA PrivK) of the generic ST CA certificate.

Figure 1. PKI two-level hierarchy



1.1 STM STSAFE-A PROD CA 01 certificate

The STM STSAFE-A PROD CA 01 key-pair is based on NIST P-256 elliptic curves.

STMicroelectronics uses the private key to sign the leaf certificate.

The content of the self-signed certificate is available below and on the STSAFE-A120 web page.

Table 1. Self-signed certificate value

Parameter		Value
Version		V3
Serial number		1
Signature algorithm		ECDSA-with-SHA256
Issuer	Country name	NL
	Organization name	STMicroelectronics nv
	Common name	STM STSAFE-A PROD CA 01
Validity	Not before	01 April 2024
	Not after	01 April 2054
Subject	Country name	NL
	Organization name	STMicroelectronics nv
	Common name	STM STSAFE-A PROD CA 01
Subject public key info	EC public key	NIST P-256
		Uncompressed encoding (both X and Y coordinates are present)

The following certificates are the DER encoded or PEM encoded self-signed X.509 certificates. They are available for download on the STSAFE-A120 web page.

DER encoded certificate

```
308201A0308201460A003020102020101300A06082A8648CE3D040302304F310B300906035504061302E4
C311E301C060355040A0C1553544D6963726F656C656374726F6E696373206E763120301E06035504030C
1753544D205354534146452D412050524F442043412030313031E170D313830373237303030303030305A170
D343830373237303030303030305A304F310B300906035504061302E4C311E301C060355040A0C1553544D
6963726F656C656374726F6E696373206E763120301E06035504030C1753544D205354534146452D41205
0524F442043412030313059301306072A8648CE3D020106082A8648CE3D030107034200048219 4F26CCA3
6E0E82195CE66658EC64A466922F58C9E64B5DE1A29E7F39863D042692E4C8AC79F96D2FED52774D52819
539F21F3ECD1938F83D70AEE09CCD8DA3133011300F0603551D130101FF040530030101FF300A06082A86
48CE3D0403020348003045022206EE5433247AC7234FC9D175AA51E83276901ADEC1F005E371F40734DE38
CC52E022100B1D9516AAD9A3E86D22B8E3B3BD0146FABB9B922F0452634FE927FF5D636CD90
(420 bytes)
```

PEM encoded certificate

```
-----BEGIN CERTIFICATE-----
MIIBoDCCAUagAwIBAgIBATAKBggqhkjOPQQDAjBPMQswCQYDVQQGEwJOTDEeMBwGA1UECgwVU1RNaWNyb2VsZ
WN0cm9uaWNzIG52MSAwHgYDVQQDDBdTVE0gU1RTQUZFLUEgUFJPRCBDQSAwMTAeFw0xODA3MjcwMDAwMDBaFw
00ODA3MjcwMDAwMDBaME8xCzAJBgNVBAYTAk5MMR4wHAYDVQQKDBVTVE1pY3JvZWxlY3Ryb25pY3MgbnYxIDA
eBgNVBAMMF1NUTSBTVFNBRkUtQSBQUk9EIENBIDAxMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEghlPJsyj
bg6CGVzmZljsZKRmki9YyeZLXeGinn85hj0EJpLkyKx5+W0v7VJ3TVKBlTnyHz7NGTj4PXCu4JzNjaMTMBEwD
wYDVR0TAQH/BAUwAwEB/zAKBggqhkjOPQQDAgNIADBFAiBu5UMyR6xyNPydF1qlHoMnaQGt7B8AXjcfQHNN44
zFLgIhALHZUWqtmj6G0iuOOzvQFG+rubki8EUmNP6Sf/XWNs2Q
-----END CERTIFICATE-----
```

1.2 Leaf certificate

The STSAFE-A leaf key pair is based on the NIST P-256 elliptic curves.

Each STSAFE-A120 SPL05 device is associated to a unique distinct leaf key pair.

The leaf certificate is signed by the STM STSAFE-A PROD CA 01 private key (see Section 1.1: STM STSAFE-A PROD CA 01 certificate). It is written during the personalization in zone 0 of the data partition as a DER-encoded X.509 certificate (see Table 4. Zone access conditions) with the following content:

Note: This leaf certificate is stored in a non-erasable partition of the user data memory. Customers who generate their own certificates can store them in another section of the data storage.

Table 2. DER-encoded X.509 certificate value

Parameter		Value
Version		V3
An unique serial number as is read from the chip		11 bytes with the following format `0x0209` (constant) An unique number (7 bytes), different for every chip Trailer (2 bytes) Product ID (same as read from chip)
Signature algorithm		ECDSA-with-SHA256 (OID = 1.2.840.10045.4.3.2)
Issuer (same order and format as in STM STSAFE-A PROD CA 01 self-signed certificate)	Country name	NL
	Organization name (1)	STMicroelectronics nv
	Common name	STM STSAFE-A PROD CA 01
Validity	Not before	date/time at generation of the leaf certificate
	Not after	Not before + 30 years
Subject	Country name	FR
	Organization name	STMicroelectronics (1)
	Common name	eval5 – Unique serial number, for example “eval5-0209A0949081D4C16B0139”
Subject public key info	EC public key	NIST-P-256
		Uncompressed encoding (both X- and Y-coordinates are present)

1. *Refer to the warning below.*

Warning: *The SPL05 is a generic configuration profile designed for evaluating the STSAFE-A120. All SPL05 devices are provisioned with identical leaf certificate subject organization names ("STMicroelectronics") and are issued by the same Certificate Authority ("STM STSAFE-A PROD CA 01").*

For customers intending to use the SPL05 in end-device production, it is recommended to prepare and store a custom leaf certificate, signed by their own Certificate Authority, in an available slot within the SPL05 product. This custom leaf certificate can retain the same public key information as the original certificate provided by STMicroelectronics.

STMicroelectronics also offers pre-provisioning services, including leaf certificate customization and allocation of a dedicated Certificate Authority. These services are available through STMicroelectronics secure factory and are subject to a minimum order quantity of 5,000 units for DFN8 package format or 2,500 units for SO8N package format.

2 SPL05 private key table

Each STSAFE-A120 SPL05 chip has a private key table that contains five static slots (slots 0, 1, 2, 3 and 4) and one ephemeral slot (slot 255).

Each slot is capable of storing a private key with any of the domain parameters that are supported by the STSAFE-A120.

The SPL05 STSAFE-A120 chips are delivered with slot 0 populated, and slots 1 to 4 empty and ready for use.

The provisioning of the key slots 1 to 4 is left up to the customers. Zones 1 to 4 in the data partition are configured to support storage of the corresponding certificates, if relevant.

Table 3. STSAFE-A120 SPL05 Private key table summary

Slot	Change Right	Curve ID	Generate Key	Signature generation (GENERATE SIGNATURE)	Signature generation (SIGNATURE SESSION)	Key establishment
0x00	Forbidden	NIST-P256	Forbidden	Allowed	Forbidden	Forbidden
0x01	Allowed (once)	-	-	-	-	-
0x02	Allowed (once)	-	-	-	-	-
0x03	Allowed (once)	-	-	-	-	-
0x04	Allowed (once)	-	-	-	-	-
0xFF	Allowed (once)	-	Allowed	Forbidden	Forbidden	Allowed

2.1 Static slot 0 configuration

The private key of the leaf key pair (see Section 1.2: Leaf certificate) is written in slot 0, which is not erasable.

This private key is configured as follows:

- **Curve ID: NIST P-256**
- **Change right**: The authorization flags update is **forbidden**.

The authorization flags are:

- **GENERATE KEY**: **forbidden**
- **Signature generation** on receipt of a message digest using the **GENERATE SIGNATURE** command: **allowed**.
- **Signature generation** over a sequence of **commands and responses**: **forbidden**.
- **Key establishment** using the *ESTABLISH KEY* command: **forbidden**.

Note: The public key, also called PubK, associated with PrivK is stored inside the leaf certificate stored in zone 0.

2.2 Static slot 1 to 4 configuration

These private key slots 1 to 4 are configured as follows:

- The **curve ID** for those key pairs can be either:
  - NIST P-256
  - NIST P-384
  - NIST P-521
  - BRAINPOOL P-256
  - BRAINPOOL P-384
  - BRAINPOOL P-512
  - EdDSA25519
  - X25519
- **Change right**: The authorization flags update is **allowed** once with PUT ATTRIBUTE [PRIVATE KEY SLOT].

The authorization flags are:

- **GENERATE KEY**: **Allowed** for this slot and does not require authentication.
- **Signature generation** on receipt of a message digest using the **GENERATE SIGNATURE** command: **allowed**.
- **Signature generation** over a sequence of **commands and responses**: **forbidden**.
- **Key establishment** using the **ESTABLISH KEY** command: **forbidden**.
- EdDSA flags (only relevant for Edwards25519 private keys):
  - Ephemeral private key generation method: set to non-Edwards25519 key
  - EdDSA variant: set to non-Edwards25519 key

Note: When a new key pair is generated in slot 1 to 4, the STSAFE-A120 responds only with the public key part of the key pair. One can build a certificate over this key pair, and then store it to the STSAFE-A120 data partition zone 1 or any other zone, depending on the certificate size. Once signed by the right certificate authorities, the obtained certificate provides another way to authenticate the device, thus allowing the renewal of the leaf certificate stored in zone 0.

2.3 Ephemeral slot 255 configuration

This private key in slot 255 is configured as follows:

- The **curve ID** for this key pair can be either:
  - NIST P-256
  - NIST P-384
  - NIST P-521
  - BRAINPOOL P-256
  - BRAINPOOL P-384
  - BRAINPOOL P-512
  - Edwards25519
  - Curve25519
- **Change right**: the authorization flags update is **allowed once** with PUT ATTRIBUTE [PRIVATE KEY SLOT]

The authorization flags are:

- **GENERATE KEY**: **Allowed** for this slot and does not require authentication
- **Signature generation** on receipt of a message digest using the **GENERATE SIGNATURE** command: **forbidden**
- **Signature generation** over a sequence of **commands and responses**: **forbidden**
- **Key establishment** using the *ESTABLISH KEY* command: **allowed**
- EdDSA flags (only relevant for Edwards25519 private keys):
  - Ephemeral private key generation method: set to non-Edwards25519 key
  - EdDSA variant: set to non-Edwards25519 key

3 Host secure channel

The host secure channel is based on the host keys slot. The host keys slot provisioning is to be handled by the customer.

3.1 Host keys slot configuration

The host keys slot is configured as follows:

- **Change right**: The provisioning control fields update is **allowed once** with PUT ATTRIBUTE[HOST KEY SLOT, PROVISIONING CONTROL FIELDS] command.

The provisioning control fields are:

- **Reprovision**: writing new keys when the slot already contains the keys is **forbidden**
- **Plaintext**: Writing host keys in plaintext is **allowed**
- **Wrapped or Diffie-Hellman derived - anonymous**: Writing wrapped host keys (with *WRITE HOST KEY V2* command) or establishing host keys (with *ESTABLISH HOST KEY V2* command) without a valid host signature (with *START VOLATILE KEK* command) are **forbidden**
- **Wrapped or Diffie-Hellman derived - authentication key**: Writing wrapped host keys (with *WRITE HOST KEY V2* command) or establishing host keys (with *ESTABLISH HOST KEY V2* command) without a valid host signature (with *START VOLATILE KEK* command) are **forbidden**

4 SPL05 symmetric key functionality

Sixteen (16) symmetric slots are defined during the configuration process.

No key is written in the table. All 16 slots are kept open for provisioning by the customers.

The provisioning control fields for the symmetric key slots are configured for each slot, as defined below:

- **Change right**: the provisioning control fields update is **allowed once** with the *PUT ATTRIBUTE* command
- Control fields:
  - **Derived**: The slot provisioning with a key derived with the *DERIVE KEYS command* is **forbidden**
  - **Plaintext**: The slot provisioning with a key derived with *WRITE SYMMETRIC KEY PLAINTEXT* command is **forbidden**
  - **Wrapped anonymous**: *WRITE SYMMETRIC KEY* without a valid host signature in *START VOLATILE KEK SESSION* is **forbidden**
  - **ECDHE anonymous**: *ESTABLISH SYMMETRIC KEYS* without a valid host signature in *START VOLATILE KEK SESSION* is **forbidden**
  - **Wrapped - authentication key**: provisioning with *WRITE SYMMETRIC KEY* with a valid host signature in *START VOLATILE KEK SESSION* is **forbidden**
  - **ECDHE - authentication key**: provisioning with *CONFIRM SYMMETRIC KEYS* when the corresponding ESTABLISH SYMMETRIC KEYS included a valid host signature in *START VOLATILE KEK SESSION* is **forbidden**

5 Generic public key table configuration

Up to three public key slots can be used for authentication of the host (to verify signatures in *START VOLATILE KEK SESSION* and *ESTABLISH SYMMETRIC KEYS* commands), for key establishment or entity authentication.

These three generic public key slots are left empty. It is up to the customers to configure and provision the public key slots.

The slots configuration flags are defined below:

- **Change right**: The configuration flags update is **allowed**
- **ESTABLISH HOST KEY V2 flag**: using the public key to authenticate a host key by verifying that the signature in an ESTABLISH KEY V2 command is **forbidden**
- **ENTITY AUTHENTICATION flag**: using the public key to authenticate an off-chip entity by verifying that the signature in the VERIFY ENTITY SIGNATURE command is **forbidden**
- **START VOLATILE KEK SESSION flag**: using the public key to verify signatures in S*TART VOLATILE KEK SESSION* command is **forbidden**
- **ESTABLISH SYMMETRIC KEYS flag**: using the public key to verify signatures in *ESTABLISH SYMMETRIC KEYS* command is **forbidden**

6 SPL05 data partition configuration

The NVM of the STSAFE-A120 contains zones, which have been configured with read and write access conditions, as detailed in the table below.

The table below describes these zones and their access conditions.

For more information on this principle and on the use of these zones, read the STSAFE-A120 user manual.

Table 4. Zone access conditions

Zone index	One-way decreasing counter presence code and initial value	Data segment length in bytes	Read AC change right (1)	Read AC	Update AC change right (1)	Update AC	Content
0	False -	1000	False	Always	False (2)	Never	The data segment includes the leaf certificate associated with the private key in slot 0
1	False -	1000	True	Always	True	Always	The data segment is empty - it can be used to store data or a certificate associated with a key pair
2	False -	1000	True	Always	True	Always	The data segment is empty - it can be used to store data or a certificate associated with a key pair
3	False -	1000	True	Always	True	Always	The data segment is empty - it can be used to store data or a certificate associated with a key pair
4	False -	1000	True	Always	True	Always	The data segment is empty - it can be used to store data or a certificate associated with a key pair
5	True (2), counter initial value: $2^{32} - 1$	64	True	Always	True	Always	The data segment is empty - it can be used to store data associated with the counter
6	True (2), counter initial value: $2^{32} - 1$	64	True	Always	True	Always	The data segment is empty - it can be used to store data associated with the counter
7	True (2), counter initial value: $2^{32} - 1$	64	True	Always	True	Always	The data segment is empty - it can be used to store data associated with the counter

Zone index	One-way decreasing counter presence code and initial value	Data segment length in bytes	Read AC change right (1)	Read AC	Update AC change right (1)	Update AC	Content
8	True (2), counter initial value: $2^{32} - 1$	64	True	Always	True	Always	The data segment is empty - it can be used to store data associated with the counter
9	False -	5120	True	Always	True	Always	The data segment is empty - it can be used to store data
10	False -	3072	True	Always	True	Always	The data segment is empty - it can be used to store data
11	False -	2944	True	Always	True	Always	The data segment is empty - it can be used to store data

1. *True means that it is possible to switch the access condition from always to false for the defined zone. False means that it is not possible to change the access condition for the defined zone.*
2. *$2^{32} - 1$ is the maximum supported value. If the customer needs a lower initial value, a decrement to reach the initial desired value can be done on the first power-up of the device.*

7 Command authorization configuration

The following figure describes the command authorization configuration.

Table 5. Command authorization configuration

The customers can configure the authorization configuration of the commands differently with a one-time put attribute [PRIVATE KEY SLOT] command (one command for ACs and one for encryption flags).

Command	Command access condition (AC)	Encryption of command data	Encryption of response data
Echo	Free	No	No
Generate MAC	Free	No	No
Verify MAC	Free	No	No
Wrap local envelope	Free	No	No
Unwrap local envelope	Free	No	No
Generate signature	Free	No	No
Establish the key	Free	No	No
Encrypt	Free	No	No
Decrypt	Free	No	No
Generate random	Free	No	No
Decrement	As defined for the addressed counter zone (see Table 4. Zone access conditions)	No	No
Read	As defined for the addressed counter zone (see Table 4. Zone access conditions)	No	No
Update	As defined for the addressed counter zone (see Table 4. Zone access conditions)	No	No
Generate key	Depends on slot configuration (see Section 2.2: Static slot 1 to 4 configuration)	No	No
Get a signature	Free	No	No
Verify signature	Free	No	No
Start hash	Free	No	No
Process hash	Free	No	No
Finish hash	Free	No	No
Start a volatile KEK session	Free	No	No
Establish symmetric keys	Free	No	No
Confirm symmetric keys	Free	No	No
Stop volatile KEK session	Free	No	No
Write host key in plaintext	Free	No	No
Write host key wrapped	Free	No	No
Write a symmetric key	Free	No	No
Write a public key	Free	No	No
Generate ECDHE key	Free	No	No
Generate challenge	Free	No	No
Verify entity signature	Free	No	No

Command	Command access condition (AC)	Encryption of command data	Encryption of response data
Derive keys	Free	No	No
Start encrypt	Free	No	No
Process encrypts	Free	No	No
Finish encrypt	Free	No	No
Start decrypt	Free	No	No
Process decrypts	Free	No	No
Finish decrypt	Free	No	No
Write symmetric key plaintext	Free	No	No
Establish host key V2	Free	No	No
Erase symmetric key slot	Free	No	No

8 SPL05 configuration parameters

The following table describes the configuration of the keys and I²C parameters of the STSAFE-A120SPL05 .

Table 6. STSAFE-A120 configuration data

Attribute	STSAFE-A120 configuration
I²C parameters	I²C address: 0100000b (0x20) and low-power mode is standby
Host key slot	Empty
Private key table	5 static slots and 1 ephemeral slot
Local envelope key slots(1)	Empty

1. *Two slots available and each slot can store either an AES 128 bit key or AES 256 bit key which can be used for wrapping and unwrapping of envelopes*

9 MAC sequence counter

A host key can be specified in the host key slot (see Section 8: SPL05 configuration parameters) for the purpose of securing communication. It allows *C-MAC* verification on commands and *R-MAC* generation on responses.

A counter is assigned to the use of this key. It is incremented with every C-MAC verification.

The counter has a maximum value of $2^{24} - 1$ or $2^{32} - 1$ depending on the configuration, which means that a maximum of $2^{24} - 1$ or $2^{32} - 1$ MAC operations are allowed with the STSAFE-A120.

Revision history

Table 7. **Document revision history**

Date	Revision	Changes
15-Sep-2025	1	Initial release.

Glossary

AC Access condition

AES Advanced encryption standard

CA Certification Authority

CCM Counter with CBC-MAC (counter with cipher-block chaining message authentication code)

CCM as described in Annex B of [IEEE 802.15.4], IEEE, part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks, 2006

C-MAC Command message authentication code

DER Distinguished encoding rules

EC Elliptic curve

ECB FIPS SP800-38A electronics code book

[FIPS SP800-38A], Recommendation for Block Cipher Modes of Operation, December 2001

ECC Elliptic curve cryptography

ECDSA Elliptic curve digital signature algorithm

EEPROM Electrically erasable programmable read-only memory

ID Identity

MAC Message authentication code

NIST National Institute of Standards and Technology

OID Object identifier

PEM Privacy enhanced mail

PKI Public-key infrastructure

RAM Random access memory

R-MAC Response message authentication code

SO8N Eight-lead small outline package – narrow

ST STMicroelectronics

UFDFPN Ultra-thin profile, fine-pitch, dual-flat package

Contents

1 **STSAFE-A120 public key infrastructure (PKI) 2**
1.1 STM STSAFE-A PROD CA 01 certificate 3
1.2 Leaf certificate 4
2 **SPL05 private key table 5**
2.1 Static slot 0 configuration 5
2.2 Static slot 1 to 4 configuration 5
2.3 Ephemeral slot 255 configuration 6
3 **Host secure channel 7**
3.1 Host keys slot configuration 7
4 **SPL05 symmetric key functionality 8**
5 **Generic public key table configuration 9**
6 **SPL05 data partition configuration 10**
7 **Command authorization configuration 12**
8 **SPL05 configuration parameters 14**
9 **MAC sequence counter 15**
Revision history 16
List of tables 19

List of tables

Table 1. Self-signed certificate value . . . 3
Table 2. DER-encoded X.509 certificate value . . . 4
Table 3. STSAFE-A120 SPL05 Private key table summary . . . 5
Table 4. Zone access conditions . . . 10
Table 5. Command authorization configuration . . . 12
Table 6. STSAFE-A120 configuration data . . . 14
Table 7. Document revision history . . . 16

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.

© 2025 STMicroelectronics – All rights reserved