STSAFE-L010 : SPL01/SPL02 generic sample profile description

Introduction

This application note describes the SPL01 and SPL02 personalization profiles used to configure generic STSAFE-L010 samples.

These profiles provide developers and end device makers with a reference configuration of STSAFE-L010 for:

- **End device authentication** (ED25519 key pair and X.509 leaf certificate)
- **Secure data storage and life cycle management** (user NVM zones and counters with access conditions)

The STSAFE-L010 devices with SPL01 / SPL02 generic profiles offer the following features:

- **Pre-provisioned ED25519 key pair (leaf key pair)**
  - Private key stored in a secure key slot inside the STSAFE-L010.
  - Associated with a unique X.509 leaf certificate stored in user NVM zone 0.
  - Leaf certificate signed by the **STM_STSAFE-L_CA0001 root certificate** authority (CA) operated by STMicroelectronics.
- **32 Kbytes of user NVM**
  - Partitioned into data zones and counter zones.
  - Each zone has specific read / write / update access conditions.
- **Communication protocol**
  - **SPL01**: I²C @ 100 kHz (7-bit address: 0x0C)
  - **SPL02**: ST1Wire @ 100 kHz

The **SPL01** and **SPL02** profiles differ only by the **selected physical communication interface**.

1 STSAFE-L010 SPL01 / SPL02 public key infrastructure (PKI)

The SPL01 / SPL02 profiles are integrated in a public key infrastructure (PKI) operated by STMicroelectronics.

At the root of this PKI, there is a self-signed STM_STSAFE-L_CA0001 certificate (root CA) with its own ED25519 key pair:

- **CA public key (CA_Kpub)** – published by ST and used to verify leaf device certificates.
- **CA private key (CA_Kpri)** – securely managed by ST and used only to sign STSAFE-L010 leaf certificates.

This **root CA certificate** is publicly available:

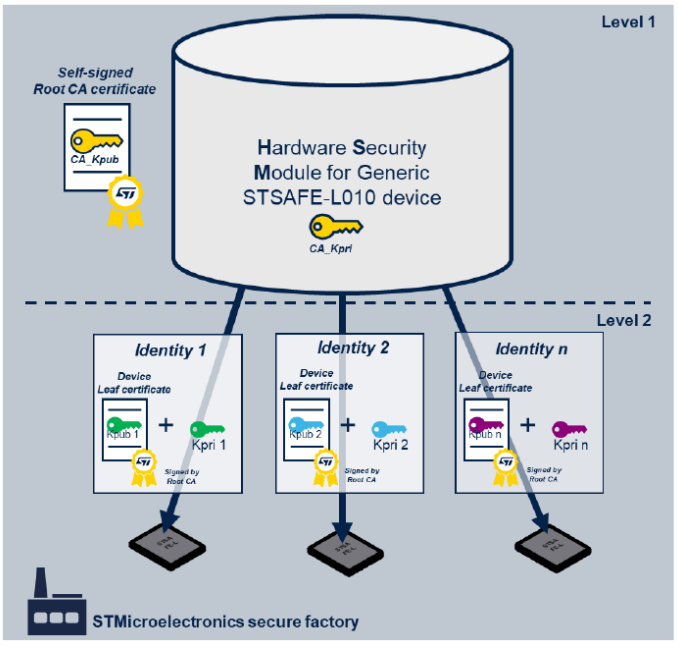
- On the STSAFE-L010 web page (Documentation tab).
- In Section 1.1 of this document (certificate content description).

Each STSAFE-L010 SPL01 / SPL02 device is personalized with:

- A **unique ED25519 private key** (leaf private key: KPri) stored in a private key secure slot inside the device.
- A corresponding **X.509 leaf certificate** stored in user **NVM zone 0**, including:
  - Device unique **serial number**
  - Device **public key (Kpub)** matching the private key
  - Certificate validity period
  - Identity information (Issuer / Subject)

This leaf certificate is **signed by the STM_STSAFE-L_CA0001 private key**, which allows the device identity to be authenticated by verifying the certificate chain up to the ST root CA.

Figure 1. Generic STSAFE-L010 device



1.1 STM_STSAFE-L_CA0001 certificate

The STM_STSAFE-L_CA0001 is the root CA used by STMicroelectronics to sign SPL01 / SPL02 device leaf certificates.

- Key pair type: **ED25519** (RFC8032)
- Purpose: Sign device X.509 leaf certificates for generic SPL01 / SPL02 profiles

The root certificate content is summarized below.

Table 1. STM STM_STSAFE-L_CA0001 certificate fields

Field	Value
Version	V3
Serial number	1
Issuer	
Country name Organization name Common name	NL STMicroelectronics nv STM_STSAFE-L_CA0001
Validity	
Not before Not after	June 7th 2024 ‘Not before’ + 30 years
Subject	
Country name Organization name Common name	NL STMicroelectronics nv STM_STSAFE-L_CA0001
Subject public key info	
Algorithm Subject public key	Ed25519 (OID 1.3.101.112) [RFC8032]-encoded STM_STSAFE-L_CA0001 public key value
Extensions	
Basic constrains Key usage	ca = TRUE, pathLenConstraint = 0 keyCertSign = 1b

The root CA certificate is distributed in both DER and PEM formats:

- DER-encoded self-signed X.509 certificate

```
3082016730820119a003020102020101300506032b6570304b310b300906035504061302 4e4c311e30
1c060355040a0c1553544d6963726f656c656374726f6e696373206e76311c301a06035504030c1353
544d5f5354534146452d4c5f434130303031302017 0d3234303630373030303030305a180f32303534
303630373030303030305a304b310b300906035504061302 4e4c311e301c060355040a0c1553544d69
63726f656c656374726f6e696373206e76311c301a06035504030c1353544d5f5354534146452d4c5f
434130303031302a300506032b65700321008447f2c098be15f605c698d5fac57b560f1ccf1f379fe9
88aa2feaa293b5ded1a320301e300f0603551d13040830060101ff020100300b0603551d0f04040302
0204300506032b65700341002931a86fed6fd7548a032072845d778797e2364b5265eac1bf7b393605
755b5d7619fd329cfd909317f953b4b821df9ce20da7cd745b9ef1abf7949f4ab0fb05
(363 bytes)
```

- PEM-encoded self-signed X.509 certificate

```
-----BEGIN CERTIFICATE-----
MIIBZzCCARmgAwIBAgIBATAFBgMrZXAwSzELMAkGA1UEBhMCTkwxHjAcBgNVBAoM
FVNUTWljcm9lbGVjdHJvbmljcyBudjEcMBoGA1UEAwwTU1RNX1NUU0FGRS1MX0NB
MDAwMTAgFw0yNDA2MDcwMDAwMDBaGA8yMDU0MDYwNzAwMDAwMFowSzELMAkGA1UE
BhMCTkwxHjAcBgNVBAoMFVNUTWljcm9lbGVjdHJvbmljcyBudjEcMBoGA1UEAwwT
U1RNX1NUU0FGRS1MX0NBMDAwMTAqMAUGAytlcAMhAIRH8sCYvhX2BcaY1frFe1YP
HM8fN5/piKov6qKTtd7RoyAwHjAPBgNVHRMECDAGAQH/AgEAMAsGA1UdDwQEAwIC
BDAFBgMrZXADQQApMahv7W/XVIoDIHKEXXeHl+I2S1Jl6sG/ezk2BXVbXXYZ/TKc
/ZCTF/lTtLgh35ziDafNdFue8av3lJ9KsPsF
-----END CERTIFICATE-----
```

Both formats are available for download from the STSAFE-L010 product web page.

1.2 Device Leaf-certificate format

Each STSAFE-L010 SPL01 / SPL02 device is associated with a **unique ED25519 leaf key pair**:

- The **private key (Kpriv)** is securely stored inside the STSAFE-L010.
- The **public key (Kpub)** is embedded in an **X.509 leaf certificate**, signed by the STSAFE-L PROD CA 0001.

This device leaf certificate is:

- Generated and signed by ST during **device personalization**.
- Stored in **data zone 0** of the user NVM as a **DER-encoded X.509 certificate**.
- Located in a **non-erasable** memory partition (see Section 2 for zone details).

*Note: Customers who wish to use their own PKI can store **additional or alternative certificates** in other user NVM zones.*

Table 2. Device Leaf Certificate fields

Field	Value
Version	V3
Serial number	9-Bytes unique serial number
Issuer	
Country name	NL
Organization name	STMicroelectronics nv
Common name	STM_STSAFE-L_CA0001 (UFT-8 string)
Validity	
Not before	Date & time of generation of this certificate
Not after	'Not before' + 30 years
Subject	
Country name	According to the country where the perso factory stands (printable string)
Organization name	STMicroelectronics nv
Common name	STSAFE-L010-GEN<Serial number defined above> (UFT-8 string)
Subject public key info	
Algorithm	Ed25519 (OID 1.3.101.112)
Subject public key	[RFC8032]-encoded device public key value

Warning:	The SPL01and SPL02 are generic configuration profile designed for evaluating the STSAFE-L010. All SPL01 and SPL02 devices are provisioned with identical leaf certificate subject organization names ("STMicroelectronics") and are issued by the same Certificate Authority ("STM_STSAFE-L_CA0001"). Refer to STSAFE-L010 SPL01 / SPL02 security consideration and customization for using these devices in production environment.

2 STSAFE-L010 SPL01 / SPL02 data partition configuration

The SPL01 / SPL02 devices non-volatile memory (NVM) offers 32KB of data storage organized into **zones**.

Each zone is configured with **data length**, **counter presence**, and **access conditions flags** for read, update/ decrement, and increment operations.

The following table summarizes the zone configuration used in SPL01 / SPL02 profiles.

Table 3. SPL01 / SPL02 data partition configuration

Zone Index	Data length (bytes)	Counter presence	Counter Initial Value	Read		Update / Decrement		Increment		Data
				AC	Change right	AC	Change right	AC	Change right	
0	510	No	N.A.	Always	No	Never	No	Never	No	Device public key leaf-certificate + 0xFF padding bytes
1 to 31	510	No	N.A.	Always	Yes	Always	Yes	Never	Yes	Default (all 0xFF)
32 to 63	507	Yes	0xFFFFFF	Always	Yes	Always	Yes	Always	Yes	Default (all 0xFF)

This User NVM profile configuration is optimized to:

- Makes use of full User-NVM product physical implementation (all available STSAFE-L010 physical pages used).
- Optimize zone endurance (100k cycles/zone).
- Offer flexibility in both applicative evaluation and end device development context (32 data zone; 32 counter zones)

*Note: For more information on zone usage and access condition, refer to the **STSAFE-L010 user manual**.*

3 STSAFE-L010 SPL01 / SPL02 command set

The SPL01 and SPL02 profiles support the following command set:

- **GENERATE SIGNATURE**
  Digital signature generation using the device-unique Ed25519 private key.
- **GET DATA**
  Read device configuration and traceability information (tags).
- **PUT DATA**
  Write configuration data (tags), subject to change rights.
- **REPEAT RESPONSE**
  Repeat the last command response.
- **READ**
  Read zone data (and counter value, if any), subject to READ access conditions.
- **UPDATE / DECREMENT**
  Update data in zones without counter, subject to UPDATE access conditions.
  Decrement counter and update data in zone with counter.
- **INCREMENT**
  Increment the counter and update data in counter zones

*Note: For the command response encoding, parameters, and error codes, refer to the **STSAFE-L010 User Manual**.*

4 STSAFE-L010 SPL01 / SPL02 communication interface

The SPL01 and SPL02 profiles differ only by the selected physical communication interface.

Table 4. Communication interface

Profile	Interface
SPL01	I²C at 100 kHz, fixed 7-bit address `0x0C`
SPL02	ST1Wire at 100 kHz

*Note: Electrical characteristics, bus timing, and protocol details are specified in the **STSAFE-L010 datasheet (DS15016)**.*

5 STSAFE-L010 SPL01 / SPL02 security consideration and customization

The **SPL01** and **SPL02** personalization profiles are **generic evaluation configurations** for STSAFE-L010. All SPL01 and SPL02 devices share the same Issuer (STM_STSAFE-L_CA0001) and **subject organization name** (STMicroelectronics). Only the device serial number and public key are unique per device.

For **end-product production** use of SPL01 and SPL02, STMicroelectronics strongly recommends users to switch PKI root CA to its own Certificate Authority (CA). For this, users can use any of available zones to store new certificates following these operations:

1. Extracting the public key of STMicroelectronics Leaf-certificate
2. Building a Certificate Signing Request for the device
3. Request Certificate Authority (CA) to create the new certificate using CSR
4. Store the new leaf certificate in an available User-NVM zone

Note: STMicroelectronics can offers customization options and secure pre-provisioning services (at STMicroelectronics secure factories), including:

- *Allocation and use of a **dedicated customer CA***
- *Custom leaf certificate generation and personalization*
- *Modification of device I2C address*

These services are subject to **minimum order quantities (MOQ)**.

For more details, contact your **local STMicroelectronics sales office**.

Revision history

Table 5. **Document revision history**

Date	Revision	Changes
06-Aug-2026	1	Initial release.

Contents

1 STSAFE-L010 SPL01 / SPL02 public key infrastructure (PKI) 2
1.1 STM_STSAFE-L_CA0001 certificate 3
1.2 Device Leaf-certificate format 4
2 STSAFE-L010 SPL01 / SPL02 data partition configuration 6
3 STSAFE-L010 SPL01 / SPL02 command set 7
4 STSAFE-L010 SPL01 / SPL02 communication interface 8
5 STSAFE-L010 SPL01 / SPL02 security consideration and customization 9
Revision history 10
List of tables 12
List of figures 13

List of tables

Table 1. STM STM_STSAFE-L_CA0001 certificate fields . . . 3
Table 2. Device Leaf Certificate fields . . . 5
Table 3. SPL01 / SPL02 data partition configuration . . . 6
Table 4. Communication interface . . . 8
Table 5. Document revision history . . . 10

List of figures

Figure 1. Generic STSAFE-L010 device 2

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