STSAFE-A110 SPL03 generic sample profile description

Introduction

This application note explains the SPL03 personalization profile that is used to configure the generic samples of the STSAFE-A110 devices.

The SPL03 profile comprises:

- Personalization with a private key and an X.509 certificate attestable by the ST root CA.
- The "Subject common name" field of the leaf certificate contains the serial number of the certificate, which is unique for each chip. This enables the use of the SPL03 configuration for cloud-based solutions.
- An *ECC NIST P-256* key pair: a public key embedded in the signed leaf certificate and a private key stored in the STSAFE-A110 device.
- A generic segmented storage zone to write and read the data based on the access conditions.
- 16 symmetric *AES*-128 key slots with the first four slots preloaded with fixed known evaluation keys.

The order codes (sales reference) for this profile dedicated to the STSAFE-A110 product are STSAFEA110S8SPL03 (*SO8N* package) and STSAFEA110DFSPL03 (*UFDFPN*8 package).

For further information, refer to the STSAFE-A110 datasheet (DS13039).

1 STSAFE-A110 public key infrastructure (PKI)

The following figure illustrates the STSAFE-A110 public key infrastructure (PKI).

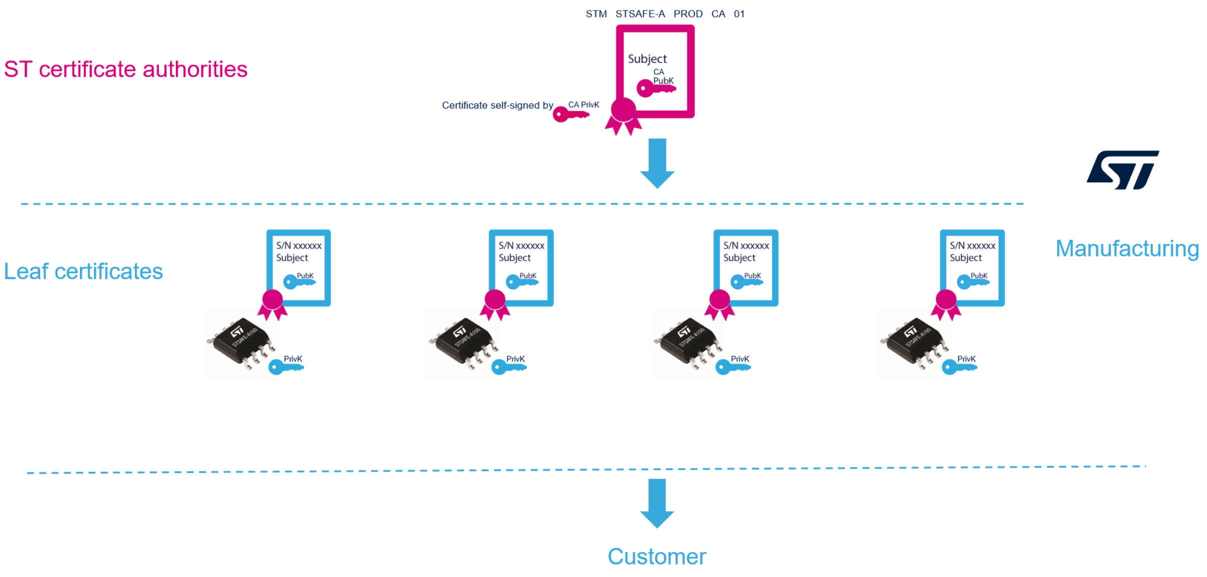
The first level of the PKI is a self-signed root certificate owned by the STMicroelectronics CA, with its dedicated key pair:

- 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-A110 web page (Tools & Software tab) and in Section 1.1 STM STSAFE-A PROD CA 01 certificate.

Each STSAFE-A110 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-A110 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	27 July 2018
	Not after	27 July 2048 (not before + 30 years)
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-A110 web page.

DER encoded certificate

```
308201A030820146A003020102020101300A06082A8648CE3D040302304F310B3009060355040613024E4
C311E301C060355040A0C1553544D6963726F656C656374726F6E696373206E763120301E06035504030C
1753544D205354534146452D412050524F44204341203031301E170D3138303732373030303030305A170
D3438303732373030303030305A304F310B3009060355040613024E4C311E301C060355040A0C1553544D
6963726F656C656374726F6E696373206E763120301E06035504030C1753544D205354534146452D41205
0524F442043412030313059301306072A8648CE3D020106082A8648CE3D0301070342000482194F26CCA3
6E0E82195CE66658EC64A466922F58C9E64B5DE1A29E7F39863D042692E4C8AC79F96D2FED52774D52819
539F21F3ECD1938F83D70AEE09CCD8DA3133011300F0603551D130101FF040530030101FF300A06082A86
48CE3D040302034800304502206EE5433247AC7234FC9D175AA51E83276901ADEC1F005E371F40734DE38
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-A110 SPL03 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 5. 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
Unique serial number as read from the chip		11 bytes with the following format
		`0x0209` (constant)
		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	eval3 – Unique serial number, for example “eval3-0209A0949081D4C16B0139”
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 SPL03 profile is a generic configuration profile. Subject 'organization name' is the same in all parts, and all these generic parts can only be distinguished with their serial number. We expect customers who intend to use SPL03 samples for production purposes to regenerate their own leaf certificates filled with their own information in the subject section, or to keep a clear tracking of the serial numbers of their parts. STMicroelectronics recommends defining and ordering parts personalized with customer information and customization. This option is available for any order of at least 5000 parts. Contact your local STMicroelectronics sales office.*

2 SPL03 private key table

An STSAFE-A110 chip has a private key table that contains two static slots in EEPROM (slot 0 and slot 1) and one ephemeral slot in RAM (slot 255).

Each slot is capable of storing a private key with any of the domain parameters that are supported by the STSAFE-A110.

The SPL03 STSAFE-A110 chips are delivered with slot 0 populated, and slot 1 empty and ready for use.

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.

The curve ID for this key-pair is NIST P-256.

The private key stored in slot 0 (PrivK) allows a signature generation on receipt of a message digest (using the *GENERATE SIGNATURE* command). This key cannot be used for key establishment using the *ESTABLISH KEY* command.

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 configuration

The curve ID selected for this slot 1 must be one of the following allowed curves:

- NIST P-256;
- NIST P-384;
- BRAINPOOL P-256;
- BRAINPOOL P-384.

The private key stored in slot 1 allows:

- Signature generation on receipt of a message digest (using the *GENERATE SIGNATURE* command)
- Key establishment using the *ESTABLISH KEY* command.

At slot 1 key creation, it is possible to dedicate the key usage to signature generation, key establishment, or both.

Note: When a new key pair is generated in slot 1, the STSAFE-A110 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-A110's 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

Slot 255 can hold an ephemeral key which can be used only once for key establishment.

The private key stored in slot 255 is generated using the *GENERATE KEY* command.

The curve ID selected for this slot 255 must be one of the following allowed curves:

- NIST P-256
- NIST P-384
- BRAINPOOL P-256
- BRAINPOOL P-384.

The private key stored in slot 255 allows key establishment using the *ESTABLISH KEY* command.

During key generation, it is possible to change the access conditions to slot 255 to restrict its usage.

3 SPL03 symmetric key functionality

Sixteen (16) symmetric slots are defined during the configuration process. The first four slots are configured as described below, using the fixed key values from Table 4. Symmetric keys. The 12 remaining slots are empty and cannot be provisioned.

Table 3. **Symmetric key slot configuration**

Slot	Key type	Mode of operation	Key usage	Parameters	Key name
0	AES-128	CCM*	Encrypt/Decrypt	0000(1)	KEY4TESTSYMM1
1	AES-128	CCM*	Encrypt/Decrypt	0480(2)	KEY4TESTSYMM2
2	AES-128	ECB	Encrypt/Decrypt	-	KEY4TESTSYMM3
3	AES-128	C-MAC	Generate/Verify MAC	04(3)	KEY4TESTSYMM4

1. *0000 means: 00 = byte length of the authentication tag, 00 = no counter used.*
2. *0480 means: 04 = byte length of the authentication tag, 80 = counter used (MSB=1), counter offset in nonce = 0 (7 LSBs).*
3. *04 means: the minimum MAC size is 04 for Verify MAC. For Generate MAC, there is no minimum MAC size limitation.*

Table 4. **Symmetric keys**

Key name	Key value
KEY4TESTSYMM1	AABBCCDDEEFF01112233445566778899
KEY4TESTSYMM2	AABBCCDDEEFF02112233445566778899
KEY4TESTSYMM3	AABBCCDDEEFF03112233445566778899
KEY4TESTSYMM4	AABBCCDDEEFF04112233445566778899

4 SPL03 data partition configuration

The NVM of the STSAFE-A110 contains zones which can be accessible in read or write mode under certain conditions.

The table below describes these zones and their access conditions.

For more information on this principle and on the use of these zones, please read the STSAFE-A110 user manual.

Table 5. **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	Comment
0	False, -	1000	False	Always	True[2]	Never	Leaf certificate
1	False, -	700	False	Always	True	Always	Can be used to store certificate associated with key pair slot 1
2	False, -	600	False	Always	True	Always	-
3	False, -	600	False	Always	True	Always	-
4	False, -	1696	False	Always	True	Always	-
5	True, 500.000	64	False	Always	True	Always	Zone with counter
6	True, 500.000	64	False	Always	True	Always	Zone with counter
7	False, -	1578	False	Always	True	Always	-

1. *True means that it is possible to switch access condition from Always to Host for the defined zone. False means that it is not possible to change access condition for the defined zone.*
2. *The update AC for zone 0 cannot be changed, even if change right = true, because update AC = never.*

5 Command authorization configuration

The following figure describes the command authorization configuration.

Table 6. **Command authorization configuration**

This configuration cannot be modified.

Command	Command access condition (AC)	Encryption of command data	Encryption of response data
Derive Key	Free	No	No
Generate MAC	Host C-MAC	No	No
Verify MAC	Host C-MAC	No	No
Wrap Local Envelope	Host C-MAC	Yes	No
Unwrap Local Envelope	Host C-MAC	No	Yes
Generate Signature	Free	No	No
Establish Key	Host C-MAC	No	Yes
Encrypt	Host C-MAC	Yes	No
Decrypt	Host C-MAC	No	Yes

6 SPL03 configuration parameters

The following table describes the configuration of the keys and I² parameters of the STSAFE-A110.

Table 7. **STSAFE-A110 configuration data**

Attribute	STSAFE-A110 configuration
I^2C parameters	I^2C address: 0100000b (0x20) and standby mode enabled
Host key slot	Empty
Private key table	2 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

7 MAC sequence counter

A host key can be specified in the host key slot (see Section 6 SPL03 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 $2^{21} - 1$, which means that a maximum of 2 097 151 MAC operations are allowed with the STSAFE-A110. This corresponds to approximately 190 uses of the host key per day for 30 years.

Revision history

Table 8. **Document revision history**

Date	Revision	Changes
07-Feb-2022	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 MAC

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 Identifier

MAC Cipher-based message authentication code (cryptographic algorithm)

NIST special publication 800-38B – Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST, May 2005

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 MAC

SO8N Eight-lead small outline package – narrow

ST STMicroelectronics

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

Contents

List of tables

IMPORTANT NOTICE – PLEASE 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 acknowledgement.

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, please 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.