STSAFE-A110 generic sample profile description

Introduction

This application note describes the personalization profile, called *SPL02 profile*, used to configure the generic samples of the STSAFE-A110 devices.

This SPL02 profile contains:

- A unique serial number per chip
- An ECC NIST-P-256 key pair: a private key and a public key embedded in a signed leaf certificate
- A generic segmented storage zone to write and read data depending on access condition

The order codes (sales references) for this profile dedicated to the STSAFE-A110 are *STSAFA110S8SPL02* (SO8N package) and *STSAFA110DFSPL02* (UFDFPN8 package).

For further information, refer to the STSAFE-A110 datasheet *Authentication, state-of-the-art security for peripherals and IoT devices* (DS12911).

Acronyms

Table 1. Acronyms and abbreviations

Term	Description
AC	Access condition
CA	Certification authority
C-MAC	Cipher-based message authentication code (cryptographic algorithm)
Host C-MAC	C-MAC computed through a command to prevent removal of the STSAFE-A110 from a device and subsequent building into a counterfeit device.
EC	Elliptic curve
ECDSA	Elliptic curve digital signature algorithm
NVM	Non-volatile memory
PKI	Public-key infrastructure
S/N	Serial number
ST	STMicroelectronics

1 STSAFE-A110 public key infrastructure (PKI)

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

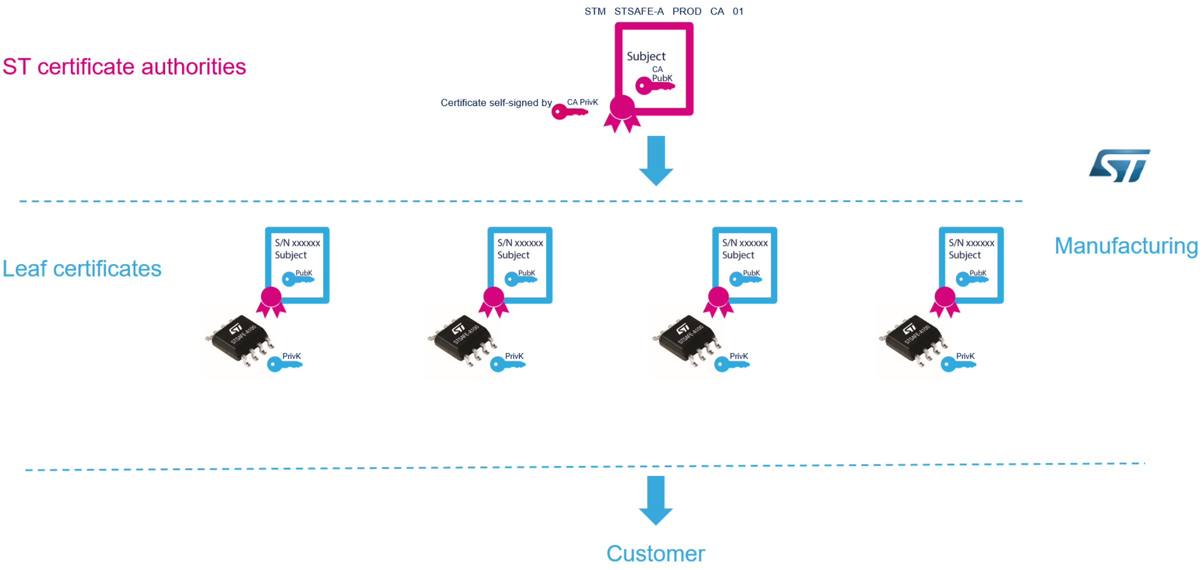
The first level of the PKI is a self-signed certificate owned by the STMicroelectronics CA, with its dedicated key pair:

- 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 2. 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 X509 certificates. They are available for download on the STSAFE-A110 web page.

DER encoded certificate

```
308201A030820146A003020102020101300A06082A8648CE3D040302304F310B3009060355040613024E4
C311E301C060355040A0C1553544D6963726F656C656374726F6E696373206E763120301E06035504030C
1753544D205354534146452D412050524F442043412030311301E170D3138303732373030303030305A170
D3438303732373030303030305A304F310B3009060355040613024E4C311E301C060355040A0C1553544D
6963726F656C656374726F6E696373206E763120301E06035504030C1753544D205354534146452D41205
0524F44204341203031305930130607 2A8648CE3D020106082A8648CE3D030107034200048219 4F26CCA3
6E0E82195CE66658EC64A466922F58C9E64B5DE1A29E7F39863D042692E4C8AC79F96D2FED52774D52819
539F21F3ECD1938F83D70AEE09CCD8DA3133011300F0603551D130101FF040530030101FF300A06082A86
48CE3D0403020348003045022 06EE5433247AC7234FC9D175AA51E83276901ADEC1F005E371F40734DE38
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 key-pairs and their public key certificates

The STSAFE-A leaf key-pair is based on the NIST-P256 elliptic curves.

Each STSAFE-A110 SPL02 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 index 0 of the data partition as a DER-encoded X509 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 3. DER-encoded X509 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	STSAFE-A110 EVAL2
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:

SPL02 profile is a generic configuration profile. Subject 'organization name' is the same and all these generic parts can only be distinguished with their serial number. We expect customers who intend to use SPL02 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 to define and order parts personalized with customer information and customization. This option is available for any order of at least 5k parts. Contact your local STMicroelectronics sales office.

2 SPL02 private key table

An STSAFE-A110 chip has a private key table that contains two static slots in EEPROM (slot 0 and slot1) 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 STSAFE-A110.

The static slots can be used for signature generation and for key establishment.

The ephemeral slot can only be used for key establishment. It cannot be used to generate signatures.

2.1 Static slot 0 configuration

The private key of the leaf key-pair (see Section 1.2 Leaf key-pairs and their public key certificates) is written in slot 0, which is unerasable.

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 generated by the host (using the *GENERATE SIGNATURE* command). This key can not 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 slot 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-P256
- BRAINPOOL-P384.

The private key stored in slot 1 allows:

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

It is also allowed to change rights for the use of slot 1. For example, it is possible to forbid the use of the slot 1 key for signature generation or key establishment .

Note: *The slot 1 can be used to generate a new key pair that can be used to build a certificate which is stored in zone 1 or in other zones, depending of the certificate size. Once signed by the right certificate authorities, it can provide another way to authenticate the device, thus allowing a renewal of the leaf certificate stored in zone 0.*

2.3 Ephemeral slot 255 configuration

The slot 255 can be used to generate an ephemeral key which can be used for key establishment. It cannot be used for generating signatures.

The private key stored in slot 255 can be 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-P256
- BRAINPOOL-P384.

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

It is also allowed to change rights for the use of slot 255. For example, it is possible to change the access conditions for the slot 255 (key generation) .

3 SPL02 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.

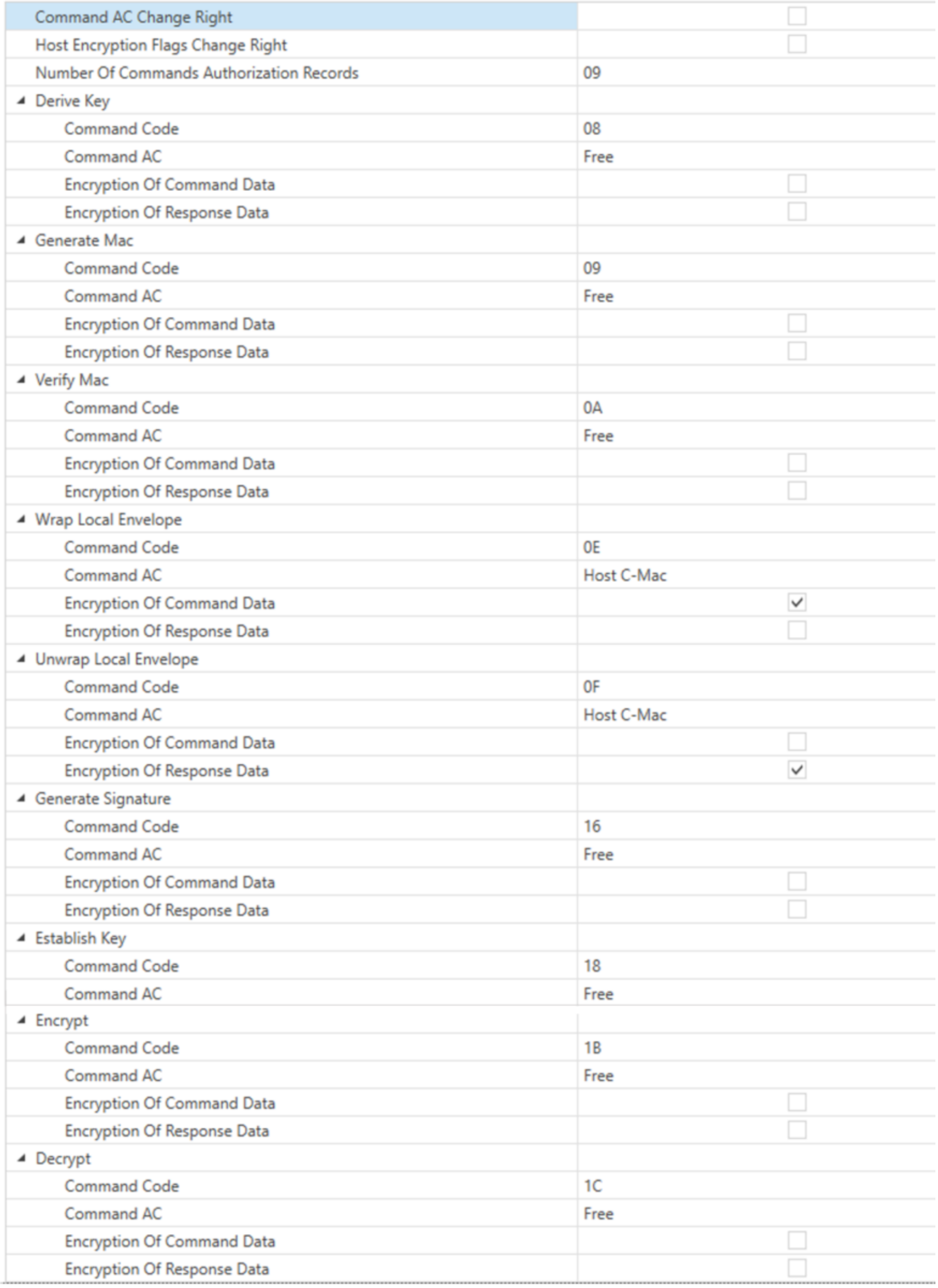
Table 4. **Zone access conditions**

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	Comment
0	False, -	1000	False	Always	True	Never	Leaf certificate
1	False, -	700	False	Always	True	Always	Can be used to store certificate associated with keypair 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.*

4 Command authorization configuration

The following figure describes the command authorization configuration.



Command AC Change Right	□
Host Encryption Flags Change Right	□
Number Of Commands Authorization Records	09
◢ Derive Key	
Command Code	08
Command AC	Free
Encryption Of Command Data	□
Encryption Of Response Data	□
◢ Generate Mac	
Command Code	09
Command AC	Free
Encryption Of Command Data	□
Encryption Of Response Data	□
◢ Verify Mac	
Command Code	0A
Command AC	Free
Encryption Of Command Data	□
Encryption Of Response Data	□
◢ Wrap Local Envelope	
Command Code	0E
Command AC	Host C-Mac
Encryption Of Command Data	☑
Encryption Of Response Data	□
◢ Unwrap Local Envelope	
Command Code	0F
Command AC	Host C-Mac
Encryption Of Command Data	□
Encryption Of Response Data	☑
◢ Generate Signature	
Command Code	16
Command AC	Free
Encryption Of Command Data	□
Encryption Of Response Data	□
◢ Establish Key	
Command Code	18
Command AC	Free
◢ Encrypt	
Command Code	1B
Command AC	Free
Encryption Of Command Data	□
Encryption Of Response Data	□
◢ Decrypt	
Command Code	1C
Command AC	Free
Encryption Of Command Data	□
Encryption Of Response Data	□

Figure 2. **Command authorization configuration**

5 Configuration of other SPL02 parameters

The following table describes the configuration of the STSAFE-A110.

Table 5. **STSAFE-A110 configuration data**

Attribute	STSAFE-A110 configuration
I^{2}C parameters	I^{2}C 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*

Revision history

Table 6. **Document revision history**

Date	Version	Changes
19-Dec-2019	1	Initial release.
09-JuL-2020	2	Updated: • Section Introduction • Section 1 STSAFE-A110 public key infrastructure (PKI) • Section 1.1 STM STSAFE-A PROD CA 01 certificate • Section 1.1 STM STSAFE-A PROD CA 01 certificate • Section 1.2 Leaf key-pairs and their public key certificates • Section 2.1 Static slot 0 configuration • Section 2.2 Static slot 1 configuration • Section 2.3 Ephemeral slot 255 configuration • Section 5 Configuration of other SPL02 parameters Added Section 4 Command authorization configuration

Contents

List of tables

List of figures