STSAFE-A100 generic sample profile description

Introduction

This application note applies to STSAFE-A100 devices. It describes the generic sample personalization profile, called *SPL02 profile*, used to configure STSAFE-A100 generic samples.

This SPL02 profile contains:

- 1 unique serial number per chip
- 1 unique 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-A100 are *STSAFA100S8SPL02* (SO8N package) and *STSAFA100DFSPL02* (UFDFPN8 package).

For further information on the STSAFE-A100, refer to the STSAFE-A100 datasheet *Authentication, state-of-the-art security for peripherals and IoT devices* (DS12911).

1 STSAFE-A100 public key infrastructure (PKI)

The following figure illustrates the STSAFE-A100 public key infrastructure (PKI).

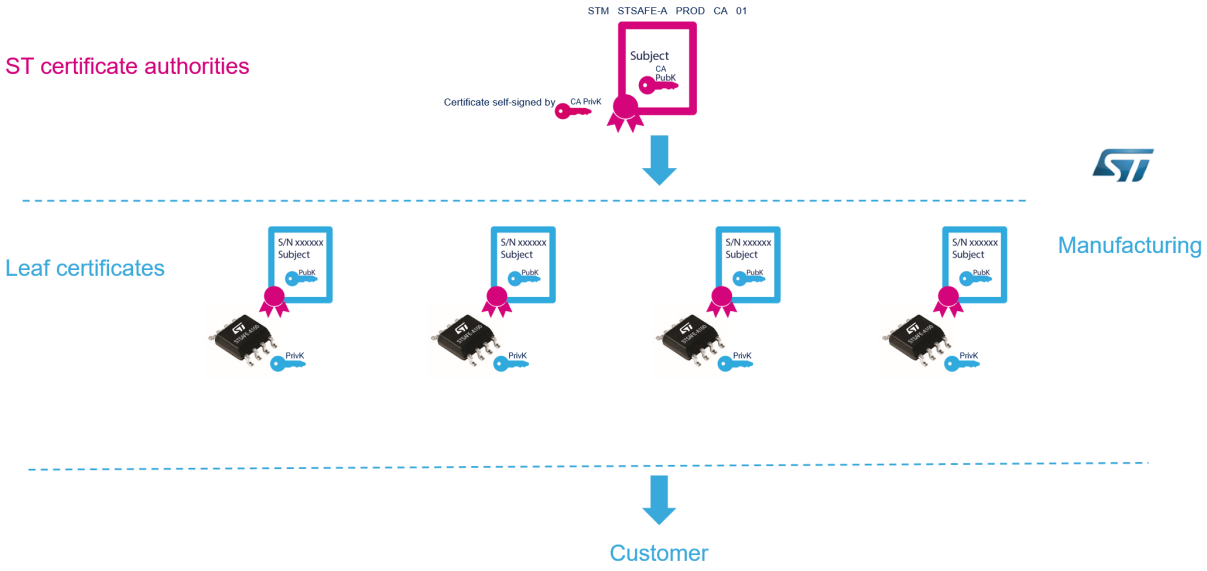
The first level of the PKI is a self-signed certificate owned by STMicroelectronics, with its dedicated key pair:

- 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-A100 web page (Tools & Software tab) and in Section 1.1 STM STSAFE-A PROD CA 01 certificate.

Each STSAFE-A100 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-P256 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-A100 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 certificate is the DER-encoded self-signed X509 certificate. It is available for download on the STSAFE-A100 web page.

```
308201A030820146A003020102020101300A06082A8648CE3D040302304F310B300906035504061302E4C311E301
C060355040A0C1553544D6963726F656C656374726F6E696373206E763120301E06035504030C1753544D20535453
4146452D412050524F442043412030313031E170D313830373237303030303030305A170D343830373237303030303
05A304F310B300906035504061302E4C311E301C060355040A0C1553544D6963726F656C656374726F6E69637320
6E763120301E06035504030C1753544D205354534146452D412050524F442043412030313059301306072A8648CE3
D020106082A8648CE3D030107034200048219 4F26CCA36E0E82195CE66658EC64A466922F58C9E64B5DE1A29E7F39
863D042692E4C8AC79F96D2FED52774D52819539F21F3ECD1938F83D70AEE09CCD8DA3133011300F0603551D13010
1FF040530030101FF300A06082A8648CE3D040302034800304502206EE5433247AC7234FC9D175AA51E83276901AD
EC1F005E371F40734DE38CC52E022100B1D9516AAD9A3E86D22B8E3B3BD0146FABB9B922F0452634FE927FF5D636C
D90
      (420 bytes)
```

1.2 Leaf key-pairs and their public key certificates

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

Every STSAFE-A100 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 3. 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 X509 certificate value

Parameter		Value
Version		V3
Serial number		11 bytes with the following format
		`0x0209` (constant)
		Unique number (7 bytes), different for every chip : chip serial number as read from 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 (Printable String)
	Organization name(1)	STMicroelectronics nv (UTF8 String)
	Common name	STM STSAFE-A PROD CA 01 (UTF8 String)
Validity	Not before	date/time at generation of the leaf certificate
	Not after	Not before + 30 years
Subject	Country name	FR (Printable String)
	Organization name	STMicroelectronics (1) (UTF8 String)
	Organizational unit name	STSAFE-A100 EVAL02 (UTF 8 String)
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. ST 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

The private key table contains two entries: slot 0 and slot 1.

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). It is forbidden to use on this key:

- Signature generation over a command and response sequence
- Key establishment using the ESTABLISH key.

Caution: A new key pair stored in slot 0 (PrivK) could be generated using the GENERATE KEY command but this would lead to the storage of a certificate inside a zone 0 not synchronized with the key pair stored inside Slot0. In this case, there would be no way to go back.

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)
- Signature generation over a command and response sequence
- Key establishment using ESTABLISH key

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 .

3 SPL02 data partition configuration

The NVM of the STSAFE-A100 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-A100 user manual.

Table 3. 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	Never	Leaf certificate
1	False, -	700	False	Always	True	Always	
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	-
6	True, 500.000	64	False	Always	True	Always	-
7	False, -	720	False	Always	True	Always	-

1. *True means that it is possible to switch access condition from Always to Host (operation requiring a valid host C-MAC on the command) for the defined zone. False means that it is not possible to change access condition for the defined zone.*

4 Configuration of other SPL02 parameters

The following table describes the configuration of the STSAFE-A100.

Table 4. STSAFE-A100 configuration data

Attribute	STSAFE-A100 configuration
I2C parameters	I2c address : 0100000b (0x20) and Standby mode enabled
Host key slot	Empty
Private key table	2 static slots
Wrap local envelope	(1)Host access condition
Unwrap local envelope	(1)Host access condition
Get Signature	Free command
Generate Signature	Free command
Local Envelope Key slots	Empty

1. *Operation requiring a valid host C-MAC in the command.*

5 Acronyms

Table 5. **List of acronyms**

Acronym	Description
AC	Access condition
CA	Certificate authority
C-MAC	Cipher-based message authentication code (cryptographic algorithm).
EC	Elliptic curve
ECDSA	Elliptic curve digital signature algorithm
Host C-MAC	C-MAC computed through a command to prevent removal of the STSAFE-A 100 from a device and subsequent building into a counterfeit device.
NVM	Non-volatile memory
PKI	Public key infrastructure
ST	STMicroelectronics

Revision history

Table 6. **Document revision history**

Date	Version	Changes
21-Oct-2019	1	Initial release.

Contents

List of tables

List of figures