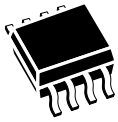
STSAFE-A100

Authentication, state-of-the-art security for peripherals and IoT devices

Data brief



SO8N
4 × 5 mm

UFDFPN8 (2 × 3 mm)

Features

- Authentication (of peripherals, IoT and USB Type-C devices)
- Secure channel establishment with remote host including transport layer security (TLS) handshake
- Signature verification service (secure boot and firmware upgrade)
- Usage monitoring with secure counters
- Pairing and secure channel with host application processor
- Wrapping and unwrapping of local or remote host envelopes
- On-chip key pair generation

Security features

- Latest generation of highly secure MCUs
  - CC EAL5+ AVA_VAN5 Common Criteria certified
  - Active shield
  - Monitoring of environmental parameters
  - Protection mechanism against faults
  - Unique serial number on each die
  - Protection against side-channel attacks
- Advanced asymmetric cryptography
  - Elliptic curve cryptography (ECC) with NIST or Brainpool 256-bit and 384-bit curves
  - Elliptic curve digital signature algorithm (ECDSA) with SHA-256 and SHA-384 for digital signature generation and verification
  - Elliptic curve Diffie-Hellman (ECDH) for key establishment
- Advanced symmetric cryptography
  - Key wrapping and unwrapping using AES-128/AES-256
  - Secure channel protocols using AES-128
- Secure operating system
  - Secure STSAFE-A100 kernel for authentication and data management
  - Protection against logical and physical attacks

Hardware features

- Highly secure MCU platform
- 6 Kbytes of configurable non-volatile memory
  - Highly reliable CMOS EEPROM technology
  - 30 years' data retention at 25 °C
  - 500 000 erase/program cycles endurance at 25 °C
  - 1.62 V to 5.5 V continuous supply voltage
- Operating temperature: -40 to 95 °C

Protocol

- I²C-bus slave interface
  - Up to 400 Kbps transmission speed (Fast mode) and true open-drain pads
  - 7-bit addressing

Packages

- ECOPACK®-compliant SO8N 8-lead plastic small outline and UFDFPN 8-lead ultra-thin profile fine pitch dual flat packages

1 Description

The STSAFE-A100 is a highly secure solution that acts as a secure element providing authentication and data management services to a local or remote host. It consists of a full turnkey solution with a secure operating system running on the latest generation of secure microcontrollers.

The STSAFE-A100 can be integrated in IoT (Internet of things) devices, smart-home, smart-city and industrial applications, consumer electronics devices, consumables and accessories.

1.1 Key function overview

Figure 1. Authentication to a remote server (IoT device case)

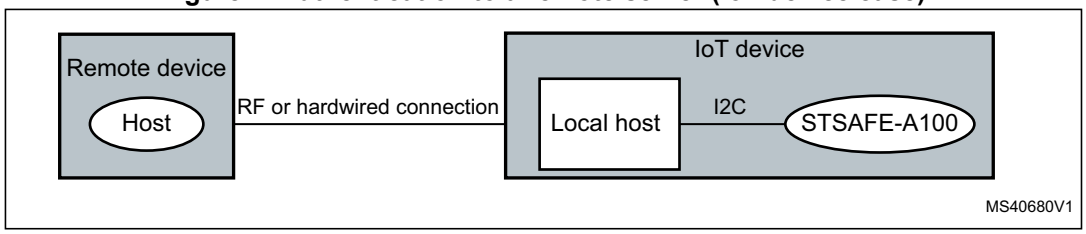
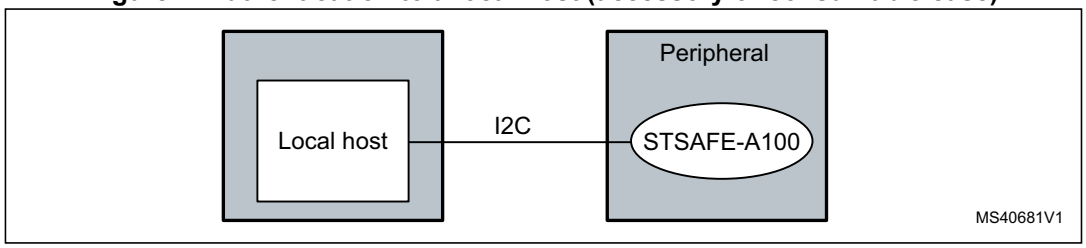


Figure 2. Authentication to a local host (accessory or consumable case)



The STSAFE-A100 can be mounted on:

- a device that authenticates to a remote host (IoT device case), the local host being used as a pass-through to the remote server.
- a peripheral that authenticates to a local host, for example games, mobile accessories or consumables.

The STSAFE-A100 secure element supports the following features:

- Authentication

  The STSAFE-A100's authentication service provides proof to a remote or local host that a certain peripheral or IoT is legitimate. An equipment manufacturer can thus ensure that only authentic peripherals like accessories or consumables can be used in conjunction with the original equipment. In the same way, a service provider can make sure that its service is only provided to the appropriate IoT device.

  The authentication service utilizes the ECC cryptographic scheme with NIST or Brainpool 256-bit and 384-bit curves. It also uses the widely deployed ECDSA signature scheme with SHA-256 and SHA-384 for generating digital signatures. In addition, it is compatible with the USB Type-C authentication scheme.

- Secure-channel key establishment (TLS)

  The STSAFE-A100 helps encrypt communications between a device and a remote host (such as a cloud server or gateway). The key establishment service uses the ECC cryptographic scheme with NIST, or Brainpool 256-bit and 384-bit curves. Moreover, it computes the shared secret with the widely recognized Diffie-Hellman schemes ECDH and ECDHE.

- Signature verification

  The STSAFE-A100 can verify an ECDSA signature by using a public key provided by the local host. This mechanism can offload a local application processor with limited computing power and no elliptic curve cryptography accelerator. It is typically used for the secure boot or secure firmware update of the local host.

- Host authentication

  With its public key slot, the STSAFE-A100 can authenticate a local or remote host. Successful authentication by the STSAFE-A100 grants the local or remote host access to some authorized commands or memory partitions.

- Secure one-way counters (peripheral usage monitoring)

  The manufacturer can limit the usage of disposable accessories or consumables to a given value by presetting the secure one-way counters. These counters can only be decremented.

- Memory partitioning

  The STSAFE-A100 comes with 6 Kbytes of non-volatile memory split into areas, whose read and write access rights can be configured to free access, local host access or remote host access.

- Pairing and secure channel with the host

  The STSAFE-A100 allows a secure channel to be set up with the local host based on AES-128-bit keys for command authorization, command data encryption, response data encryption and response authentication. Typically, this secure channel prevents eavesdropping of sensitive information on the I²C line.

- Wrapping & unwrapping local or remote host envelopes

  The STSAFE-A100 can be used to encrypt or decrypt data between the remote host and the local host. The local host may also use the STSAFE-A100’s encryption/decryption services to store sensitive data to a local, external storage like Fash memory.

1.2 STSAFE-A100's environment

The STSAFE-A100 comes with a host library that can be ported to a wide range of general-purpose microcontrollers or microprocessors. This library includes a command wrapper as well as generic use cases.

STMicroelectronics also offers key provisioning services for storage of customer credentials in a secure, certified environment.

LICENSED DPA COUNTERMEASURES™

1.3 Pin descriptions

Figure 3. SO8N pinout - Top view

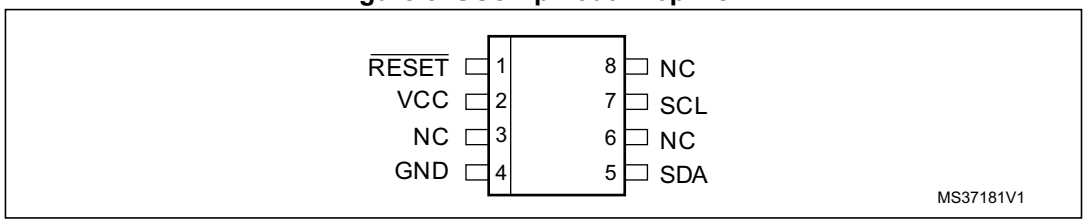


Figure 4. UFDFPN8 pinout - Top view

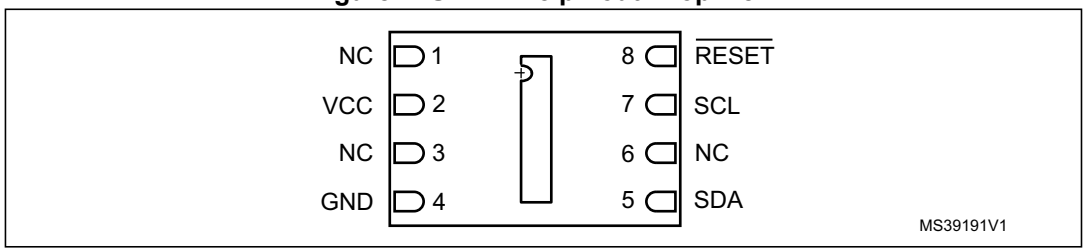


Table 1. Pin description

Pin name	Description
$\overline{\text{RESET}}$	Reset
V_{CC}	Power supply
GND	Ground supply
SCL	Serial clock
SDA	Serial data
NC	Not connected

2 Revision history

Table 2. Document revision history

Date	Revision	Changes
03-Feb-2016	1	Initial release.