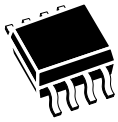
STSAFE-A1SX

State-of-the-art security for Sigfox Ready™ IoT devices

Datasheet - production data



SO8N
4 × 5 mm

UFDFPN8 (2 × 3 mm)

Features

- Ensures Sigfox™ device authentication
- Ensures Sigfox data exchange integrity service:
  - Uplink MAC generation service
  - Downlink MAC verification service
- Ensures Sigfox data exchange confidentiality service (Sigfox option)
  - Uplink encryption service
  - Downlink decryption service
- Sigfox frame anti-replay mechanism
- Comes preloaded with credentials to access the Sigfox network

Security features

- Latest generation of highly secure microcontrollers
  - 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 symmetric cryptography
  - Key wrapping and unwrapping using AES-128/AES-256
  - Secure channel protocols using AES-128
- Secure operating system
  - Secure STSAFE-A1SX kernel for authentication and data management
  - Protection against logical and physical attacks

Hardware features

- Highly secure microcontroller' platform
- 6 Kbytes of 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 105 °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

Contents

List of tables

List of figures

1 Description

The STSAFE-A1SX is a secure element that provides security services for the implementation of Sigfox LPWAN (low-power wide area network) security in Sigfox IoT devices.

Connected to the applicative microcontroller (MCU) of a Sigfox IoT device, the STSAFE-A1SX assists the MCU of this IoT device to achieve recognition, authentication and connection to the Sigfox network. The IoT device is then able to ensure and verify the integrity of exchanged data. Optionally, it can also ensure the confidentiality of exchanged data.

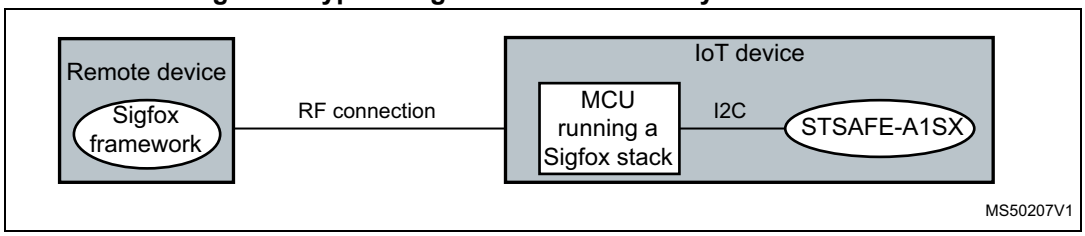
It comes preloaded with the Sigfox IDs and keys, and does not require any additional configuration.

The STSAFE-A1SX drastically simplifies and secures device onboarding. The customer no longer needs to save credentials to the IoT storage at manufacturing time. ST takes care of loading credentials into the secure element in a secure way. The IoT device can then directly exploit the Sigfox credentials preloaded in the secure element.

The STSAFE-A1SX is a full turnkey solution running a proprietary application and operating system on top of the latest secure microcontroller generation.

1.1 Overview of key functions

Figure 1. Typical Sigfox/STSAFE-A1SX system overview



1.1.1 STSAFE-A1SX functionality

This section describes the features supported by the STSAFE-A1SX secure element.

Authentication

The STSAFE-A1SX's authentication service provides proof to the Sigfox network that it is addressing a legitimate IoT device. In the same way, the Sigfox IoT device verifies that orders or data are coming from the legitimate Sigfox server.

The authentication service allowing this mutual authentication is based on MAC generation and verification on payload upload and download. This MAC generation uses symmetric AES-CBC algorithms executed with a 128-bit key.

Integrity of payload uplink and downlink

The STSAFE-A1SX provides proof to the Sigfox network that it is receiving payloads containing exhaustive, unmanipulated data. In the same way, the Sigfox IoT device that is

receiving orders or data from the Sigfox network verifies that the received orders and data are exhaustive and unmanipulated.

The exchanged data integrity service allowing this bidirectional integrity verification is based on MAC generation and verification on payload upload and download. This MAC generation uses symmetric AES-CBC algorithms executed with a 128-bit key.

Confidentiality of payload uplink and downlink (optional)

This service is based on the optional Sigfox encryption service. This service must be subscribed by the service provider at Sigfox level.

When the encryption service has been subscribed, the STSAFE-A1SX exchanges data with the Sigfox network in a confidential manner. Data sent from the Sigfox IoT device to the Sigfox network or from the Sigfox network to the Sigfox IoT device cannot be understood by someone accessing them.

The exchanged data confidentiality is based on a payload encryption and decryption mechanism using a symmetric AES algorithm executed with a 128-bit key.

Anti-replay mechanism

The STSAFE-A1SX provides proof to the Sigfox network that payloads are received in the expected order. It thus prevents eavesdroppers from replaying a specific payload. In the same way, the Sigfox network provides proof to the Sigfox IoT device that the payloads are received in the expected order. Suspicious payloads are rejected by the Sigfox network or the Sigfox IoT device.

This anti-replay mechanism is based on a sequence counter included in the messages. This sequence counter is incremented by the STSAFE-A1SX and the Sigfox network each time a payload is sent. All received messages with an invalid sequence counter are discarded.

Sigfox credentials preloading

The STSAFE-A1SX is delivered to customers preloaded with the Sigfox network credentials:

- It comes loaded with the Sigfox device ID, which must be used by the service provider to register the Sigfox IoT device to a specific Sigfox service provider account.
- IT comes loaded with the Sigfox PAC (porting authorization code). This code is a proof of device ownership. The PAC must be used with the Sigfox device ID at device registration.

Memory partition

The STSAFE-A1SX comes with eight data partitions of 777 bytes each, which are freely usable by the IoT device.

Two of these partitions offer a decounting counter starting from 100000.

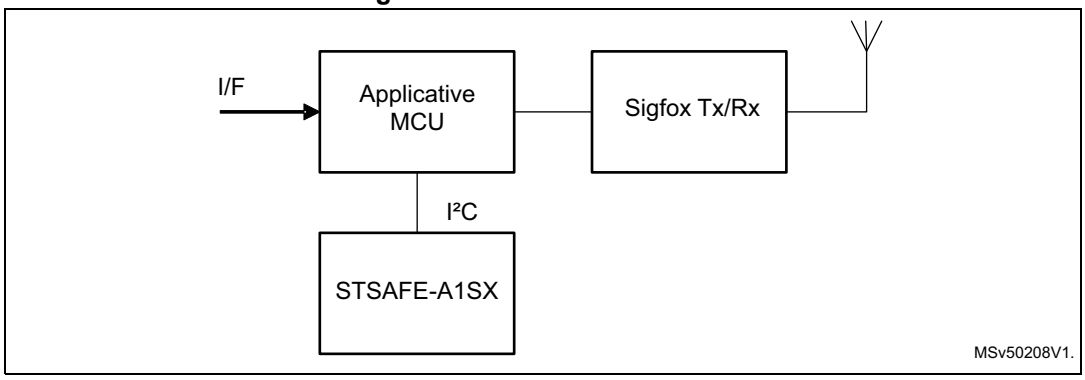
1.1.2 Possible integration architectures

The STSAFE-A1SX can be integrated in three kinds of devices architectures as described in the following paragraphs.

Discrete device architecture

In this architecture, the device contains an applicative MCU running the Sigfox stack and connected to a Sigfox transceiver. The STSAFE-A1SX is connected by I2C to the applicative MCU.

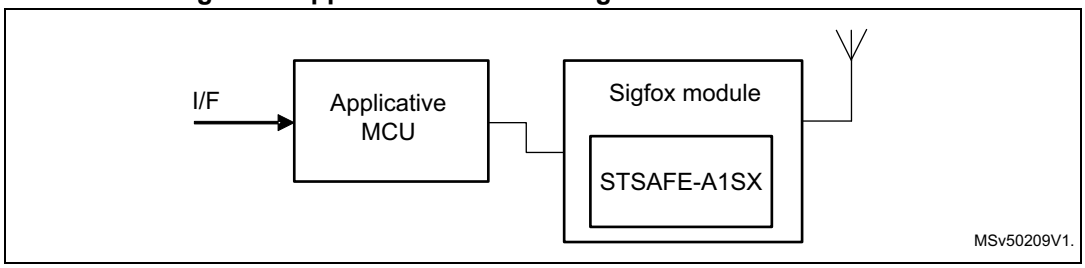
Figure 2. Discrete architecture



Applicative MCU with Sigfox module architecture

In this architecture, the device comprises an applicative MCU connected to a Sigfox module that includes a Sigfox transceiver and an MCU running the Sigfox stack. The STSAFE-A1SX is connected by I²C to the Sigfox module MCU.

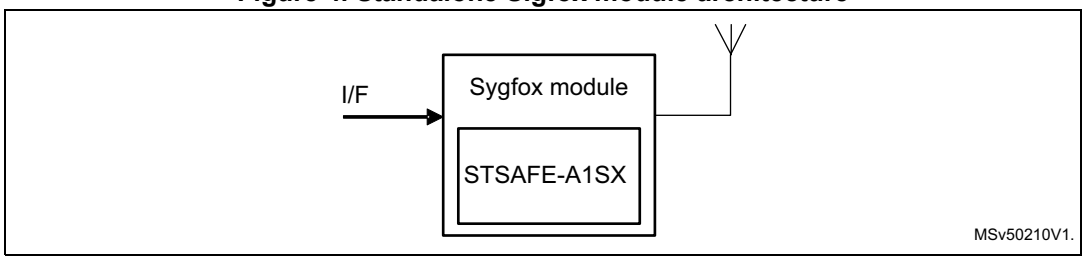
Figure 3. Applicative MCU with Sigfox module architecture



Standalone Sigfox module architecture

In this architecture, the device comprises a standalone module containing a Sigfox transceiver and an MCU running the Sigfox stack and the device application. The STSAFE-A1SX is connected by I²C to the Sigfox module MCU.

Figure 4. Standalone Sigfox module architecture



1.2 STSAFE-A1SX's environment

The STSAFE-A1SX comes with a host library that can be ported to a wide range of general-purpose microcontrollers or microprocessors. This library relies on the STSAFE-A1SX to provide access to the Sigfox security services.

STMicroelectronics offers Sigfox network credentials provisioning in a secure, certified environment.

1.3 Pin descriptions

Figure 5. SO8N pinout - Top view

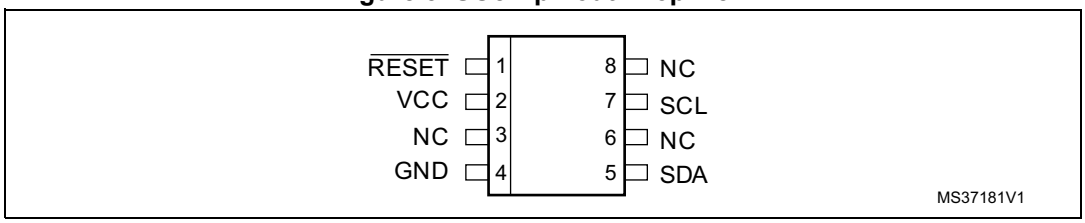


Figure 6. UFDFPN8 pinout - Top view

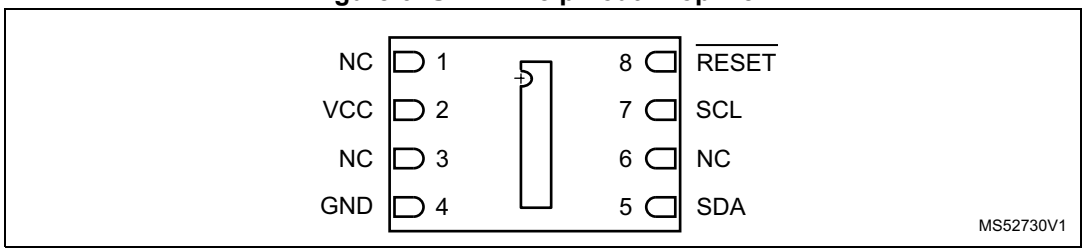


Table 1 provides the name and description of the four contacts on the STSAFE-A1SX device. Details on each are provided later in this text.

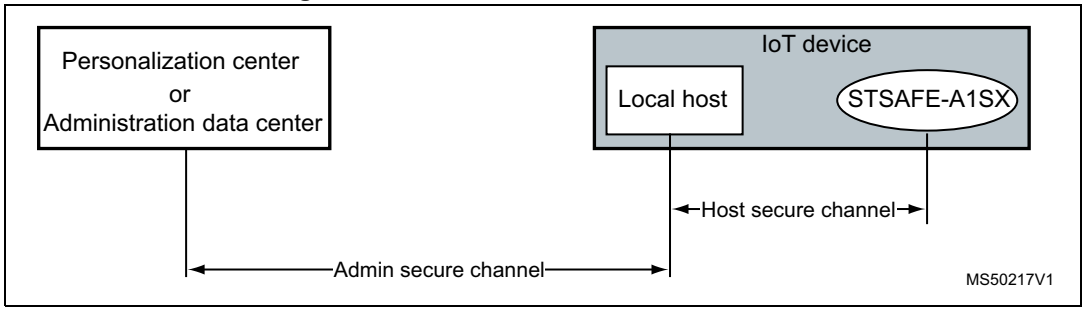
Table 1. Signal descriptions

Signal	Name	Description
V_{CC}	Supply voltage	The 1.62 to 5.5 V supply voltage is supported for powering all internal STSAFE-A1SX functions.
GND	Supply and signals ground	Ground reference pin for power and all I/O signals.
$\overline{\text{RESET}}$	Reset	This input signal is used to reset STSAFE-A1SX. The $\overline{\text{RESET}}$ pin is pull-down by default meaning that the device is reset if connected to ground or if the pin is floating. The device is active if the $\overline{\text{RESET}}$ pin is tied high.
SCL	Serial clock	This input signal is used to strobe all data in and out of STSAFE-A1SX. The signal is an input signal only and does not support the clock stretching mode common to generic I^2C. The Clock signal is driven by the I^2C master.
SDA	Serial data	This I/O signal is used to transfer data into and out of STSAFE-A1SX. The signal uses an open drain output configuration. An external pull-up resistor is used to “pull up” the output.
NC	-	Not connected internally

2 Pairing between the STSAFE-A1SX and the host MCU

With the objective of protecting and authenticating the link between STSAFE-A1SX and the local or remote host, some secure channel protocols using symmetric cryptography have been put in place, namely the host secure channel and the admin secure channel.

Figure 7. Host and Admin secure channels



The host secure channel protocol protects the link between a local host and the STSAFE-A1SX chip; it constitutes a kind of pairing. It is based on a set of four mechanisms using two symmetric keys, the so-called host keys. These keys are used to MAC the commands (C-MAC) and respective responses (R-MAC). They are also used to encrypt the commands and their respective response to avoid eavesdropping.

2.1 Host secure channel setup use case

In order to execute some specific commands requiring a C-MAC, the local host needs to generate a Host MAC key and a Host cipher key. It puts these keys into the STSAFE-A1SX's Host key slots.

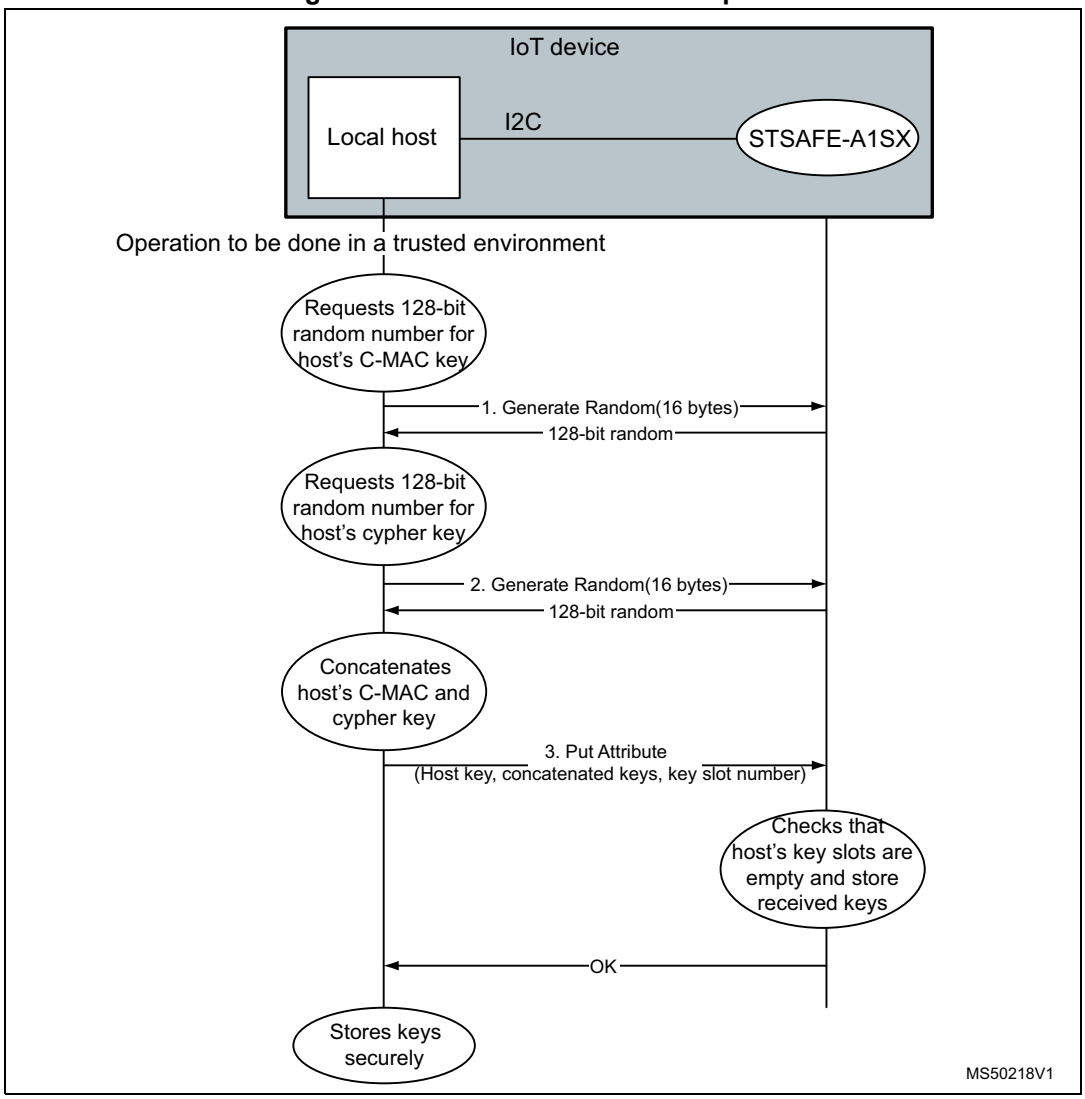
Command flow

This use case assumes that the slots are empty, and cannot be implemented a second time without first deleting the keys present in the slots.

This operation shall be performed in a secure environment, such as the customer manufacturing plant.

1. The local host requests the STSAFE-A1SX to generate a 128-bit random to be used as the host C-MAC key.
2. The local host requests the STSAFE-A1SX to generate a 128-bit random to be used as the host cipher key.
3. The local host sends the "Host key slot" attribute together with the two generated keys (forming a 256-bit payload).
4. The STSAFE-A1SX chip stores the keys into their respective slots and returns a successful response.
5. The local host stores the host C-MAC & cipher keys to a secure area.

Figure 8. Host secure channel setup case

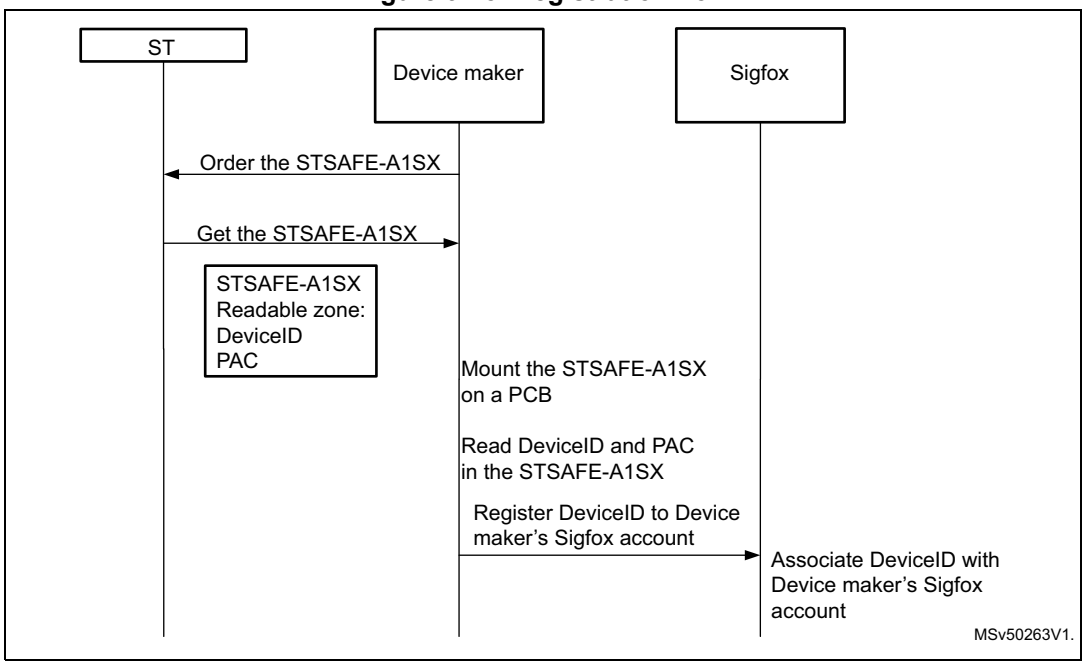


3 Description of the Sigfox security features

3.1 IoT device registration

The figure below describes the IoT device registration procedure.

Figure 9. IoT registration flow



Flow

- The device maker orders STSAFE-A1SX devices. The devices are preconfigured with the information and secret keys required to register on the Sigfox network.
- The device maker mounts the STSAFE-A1SX devices on its IoT devices.
- The device maker reads the DeviceIDs and PACs from the STSAFE-A1SX devices.
- The device maker registers the DeviceIDs to their Sigfox account.

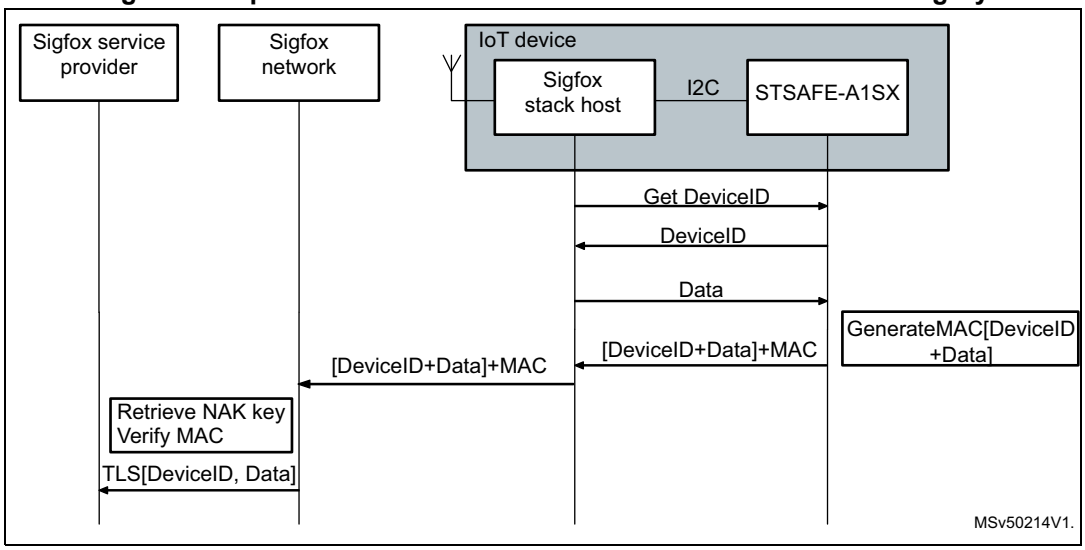
Note: This flow does not involve any secret exchange. It drastically eases and secures device onboarding.

3.2 Device authentication, uploaded and downloaded data integrity

The figure and command flow below describe the upload scenario: a Sigfox IoT device sends data to the Sigfox network and the expected service provider. This section explains the STSAFE-A1SX services that allow the Sigfox network to perform IoT device authentication and data integrity verification.

The download scenario corresponding to the service provider sending data to a Sigfox IoT device is similar, but not described here.

Figure 10. Upload scenario for device authentication and data integrity



Command flow

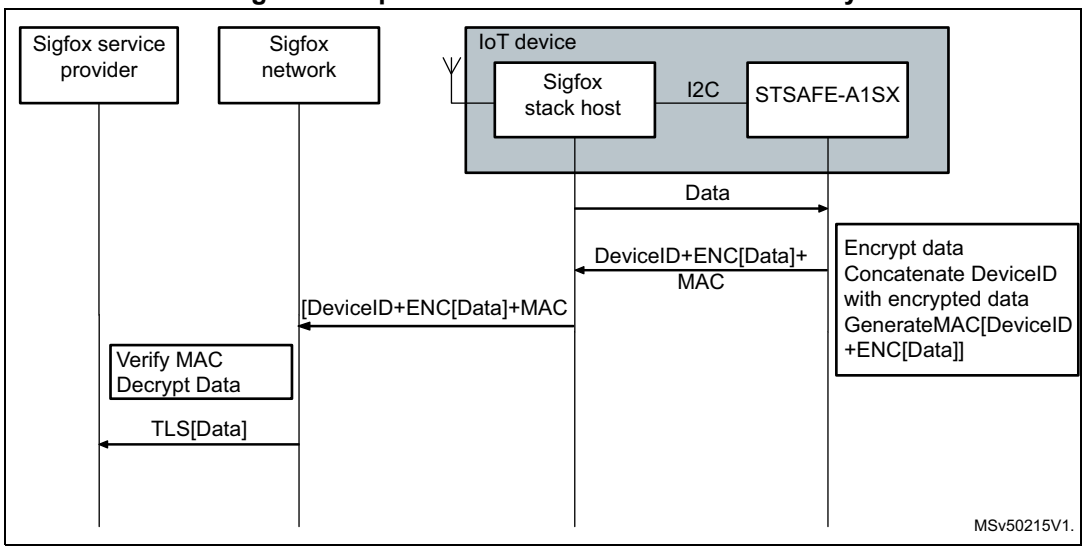
- Prerequisite:
  - The device host MCU operating the Sigfox stack must read DeviceID from the STSAFE-A1SX before sending the commands.
- The device host MCU operating the Sigfox stack sends DeviceID and data to the STSAFE-A1SX.
- The STSAFE-A1SX uses the NAK key to generate the data MAC.
- The STSAFE-A1SX returns the data with the generated MAC to the Sigfox stack host.
- The Sigfox IoT device sends the data and data MAC to the Sigfox network.
- The Sigfox network uses DeviceID to retrieve the IoT device's NAK key.
- The Sigfox network uses the NAK key to verify the MAC. A successful MAC verification means that the Sigfox IoT device is genuine and that the transmitted data have not been distorted.
- The Sigfox network provides the data to the service provider in a secure way.

3.3 Uploaded and downloaded data confidentiality

The figure and command flow below describe the upload scenario: a Sigfox IoT device sends data to the Sigfox network that ensures data confidentiality. This section describes the STSAFE-A1SX encryption service that allows the Sigfox IoT device to send encrypted data to the Sigfox network. It also explains how the Sigfox network decrypts the data before providing them in a secure way to the Sigfox service provider.

The download scenario corresponding to the service provider sending data to the Sigfox IoT device that ensures data confidentiality is similar, but not described here.

Figure 11. Upload scenario for data confidentiality



Command flow

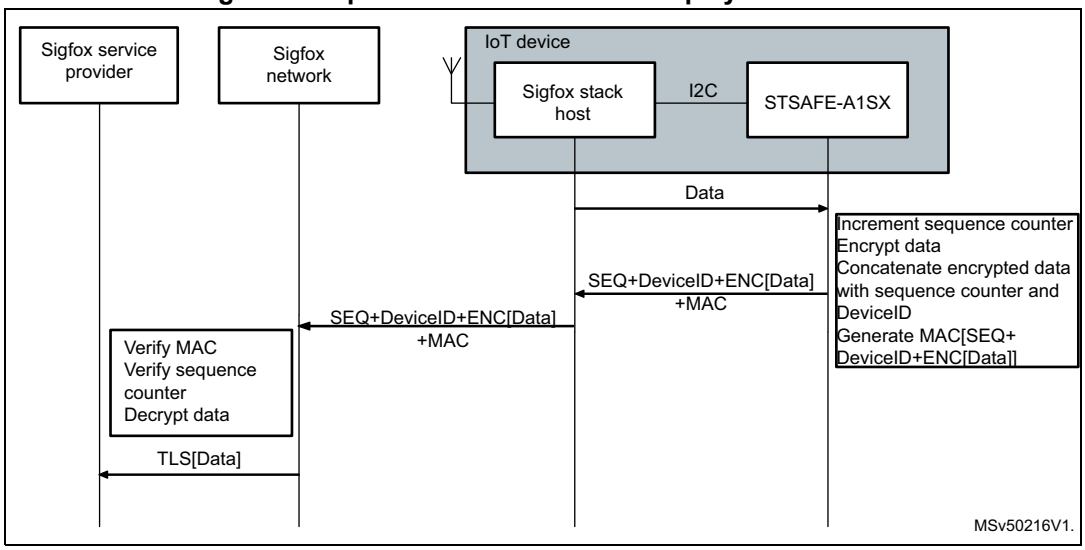
- Prerequisite:
  - The device host MCU operating the Sigfox stack must read DeviceID from the STSAFE-A1SX before sending the commands.
- The device host MCU operating the Sigfox stack sends DeviceID and the data to the STSAFE-A1SX.
- The STSAFE-A1SX encrypts the data, concatenates them with DeviceID, and generates the MAC.
- The STSAFE-A1SX returns the encrypted data with the MAC to the Sigfox stack host.
- The Sigfox IoT device sends the encrypted data and MAC to the Sigfox network.
- The Sigfox network uses the NAK key to verify the MAC. A successful MAC verification means that the Sigfox IoT device is genuine and that the transmitted data have not been distorted.
- The Sigfox network decrypts the payload.
- The Sigfox network provides the data to the service provider in a secure way.

3.4 Anti-replay mechanism

The figure and command flow below describe the upload scenario: a Sigfox IoT device sends data to the Sigfox network that ensures data confidentiality. The focus is on the anti-replay mechanism. This section describes the STSAFE-A1SX sequence counter service, which allows the Sigfox IoT device to associate a sequence counter with the encrypted data that are sent to the Sigfox network. It also explains how the Sigfox network verifies this sequence counter and decrypts the data before providing them in a secure way to the Sigfox service provider.

The download scenario corresponding to the service provider sending data to a Sigfox IoT device ensuring anti-replay is similar, but not described here.

Figure 12. Upload scenario with anti-replay mechanism



Command flow

- Prerequisite:
  - The device host MCU operating the Sigfox stack must read DeviceID from the STSAFE-A1SX before sending the commands.
- The device host MCU operating the Sigfox stack sends DeviceID and the data to the STSAFE-A1SX.
- The STSAFE-A1SX encrypts the data, concatenates them with DeviceID and with the sequence counter, and generates the MAC.
- The STSAFE-A1SX returns the encrypted data, DeviceID and the sequence counter with the MAC to the Sigfox stack host.
- The Sigfox IoT device sends the encrypted data and the MAC to the Sigfox network.

4 Command set

SE_API_get_version

Returns the API version of the STSAFE-A1SX.

SE_API_init

Initializes the STSAFE-A1SX's integration layer.

SE_API_open

Starts communication with the STSAFE-A1SX.

The STSAFE-A1SX can then be powered up or exit the low-power state. It must be operational when SE_API_open returns (which means that the SE's boot time must be considered).

SE_API_close

Stops communication with the STSAFE-A1SX. The device can then be powered down or enter the low-power mode.

SE_API_get_device_id

Returns the Sigfox DeviceID configured in the STSAFE-A1SX.

SE_API_get_initial_pac

Returns the Sigfox PAC (porting authorization code) configured in the STSAFE-A1SX.

SE_API_secure_uplink_message

Signs the data to upload from the STSAFE-A1SX to the Sigfox network. If the Sigfox encryption option is selected, this function signs and encrypts the data to upload from the device to the Sigfox network.

SE_API_verify_downlink_message

Verifies the signature of the data downloaded by the STSAFE-A1SX from the Sigfox network. If the Sigfox encryption option is selected, this function decrypts and verifies the signature of the downloaded data.

SE_API_set_rc_sync_period

Sets the sending rcsync frame's periodicity and resynchronizes the roll over counter.

SE_API_echo

Returns the data received as the command data in the response.

SE_API_reset

Interrupts the ongoing session.

SE_API_generate_random

Returns the requested number of random bytes.

SE_API_hibernate

Sets the STSAFE-A1SX in very-low-power consumption mode.

SE_API_activate_sigfox_frame_encryption

Sets the STSAFE-A1SX in the optional Sigfox encryption and decryption mode. This is a one-time setting that cannot be modified once done as there is no backward procedure.

SE_API_locate_host_keys

Provides the address location of the host key pair (Host MAC and cipher keys) through the MCU area memory.

SE_API_populate_pairing_keys

Populates the host key pair (Host MAC and cipher keys) through the STSAFE-A1SX.

SE_API_check_pairing_keys_presence

Checks the presence of the host key pair (Host MAC and cipher keys) through the STSAFE-A1SX.

SE_API_activate_pairing

Enables host pairing (I²C traffic encryption and command/response authentication).

5 Electrical characteristics

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the device. The parameters in the DC and AC characteristic tables that follow are derived from tests performed under the measurement conditions summarized in the relevant tables. Users should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

5.1 Absolute maximum ratings

Operation of STSAFE-A1SX at ranges above the absolute maximum specifications may cause permanent device damage. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Table 2. Absolute maximum ratings

Name	Description	Conditions	Min.	Max.	Units
$V_{CC\ ABS}$	Absolute maximum power supply	Pins: V_{CC}	–0.3	7	V
V_{IO}	Input or output voltage relative to ground	-	–0.3	$V_{CC\ ABS}$ + 0.3	V
V_{ESD}	Electrostatic Discharge Voltage according to EIA/JEDEC JESD22-A114E specification	Human Body Model. All pins according to specification	-	±5000	V
V_{LU}	Max over voltage for Latch-up Immunity according to EIA/JEDEC - JESD78 specification	Class 1 / Level A Maximum operating temperature		1.5 × $V_{CC\ ABS}$	V
T_A	Ambient operating temperature	-	–40	105	°C
T_{STG}	Storage temperature	-	–65	150	°C
T_{LEAD}	Lead temperature during soldering(1)		-	260	°C

1. SO8N and UFDFPN8 lead temperature during soldering shall be compliant with JEDEC Std J-STD-020D (for small body, Sn-Pb or Pb assembly), ST ECOPACK 7191395 specification, and the European directive on Restrictions on Hazardous Substances (ROHS directive 2011/65/EU, July 2011).

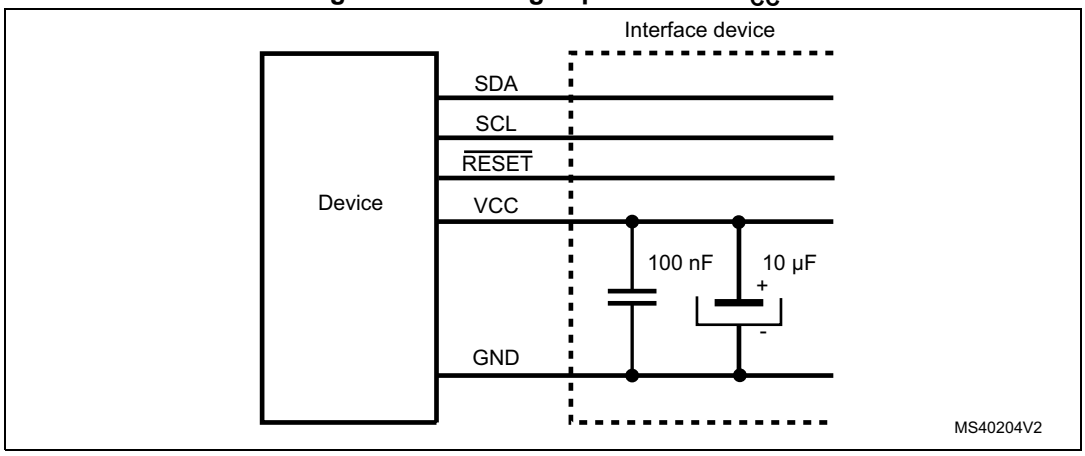
5.2 Power supply

The circuit includes a DC/DC converter that supplies the internal logic and memories with a low operating voltage. The device can operate with external voltages of 1.62 V to 5.5 V nominally, through GND and V_{CC} pins.

In order to filter spurious spikes on the supply voltage pins, decoupling capacitors (100 nF and 10 µF) must be added to the interface device as shown on *Figure 13*. They must be wired between GND and V_{CC} pins.

Note: For each device, the 100 nF decoupling capacitor must be located as close as possible to the device (within a few millimeters). If there are multiple power supplies, a 10 µF filtering capacitor must be located on each one.

Figure 13. Filtering capacitors on V_{CC}



5.2.1 Power supply specifications

Table 3 provides the detailed description of the power requirements of STSAFE-A1SX.

Table 3. Power supply specifications

Name	Description	Conditions	Min.	Typ.	Max.	Units
V_{POR}	Power on reset voltage	-	1.35	1.45	1.55	V
V_{CC}	Supply voltage	V_{CC} to GND	1.62	-	5.5	V
$V_{CC-HIPS}$	High power supply detection	Ambient temperature (25 °C)	5.6	6.3	6.9	V
$I_{CC-PROC}$	Supply current while processing a command	Ambient temperature (25 °C)	7	8.5	10.1	mA
$I_{CC-STDBY}$	Supply current in standby	IO pulled up to V_{CC}, T_A = 25 °C, 3 V to 5 V	160	245	460	µA
$I_{CC-RESET}$	Supply current during reset	$\overline{RESET}$ = 0	200	450	800	µA
$I_{CC-HIBERNATE}$	Supply current during hibernate	$\overline{RESET}$ = 1 (1) T_A = 25 °C	0.2	1.1	3	µA

1. $\overline{RESET}$ must be tied to V_{CC} ± 200mV in case of Wake-up from Hibernate on Reset event selected. $\overline{RESET}$, SDA and SCL must be tied to V_{CC} ± 200mV in case of Wake-up from Hibernate on Reset event or I²C start condition selected.

5.2.2 Power-on and power-off sequences, and power supply glitch tolerance

The power-on sequence on STSAFE-A1SX products need to follow the requirements mentioned below:

- The $\overline{RESET}$ pin must not be tight to High prior to the V_{CC} power pin.
- The $\overline{RESET}$ pin must be tied low prior to or simultaneously with the V_{CC} pin.
- The voltage applied to the V_{CC} pin must be less than or equal to 0.3 V prior to starting a new power-on sequence.

For security purposes, the STSAFE-A1SX features security detectors such as internal integrity checkers and environmental sensors.

When these detectors are triggered, the STSAFE-A1SX device enters the reset state until a power cycle or an external reset event occurs.

5.2.3 Reset pin (external reset)

The circuit is in reset state when the Reset signal available on the $\overline{\text{RESET}}$ pin is at logical level '0'. If this signal is low for less than t_{WL}, it is not taken into account.

When the $\overline{\text{RESET}}$ pin is floating, an external reset is not available and the device will remain in a Reset state as the pin is connected to an internal weak pull-down.

When pin V_{CC} is tied high, if the $\overline{\text{RESET}}$ pin switches from high to low and then to high again, a warm reset occurs. For more information, refer to *Figure 15: Warm reset sequence on page 20*.

5.2.4 Power-on and reset sequence

Figure 14. Power-on and reset sequence

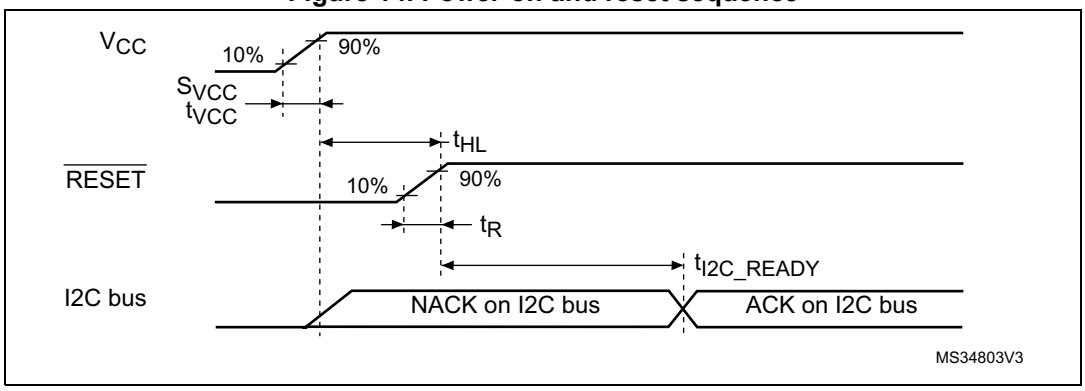


Figure 15. Warm reset sequence

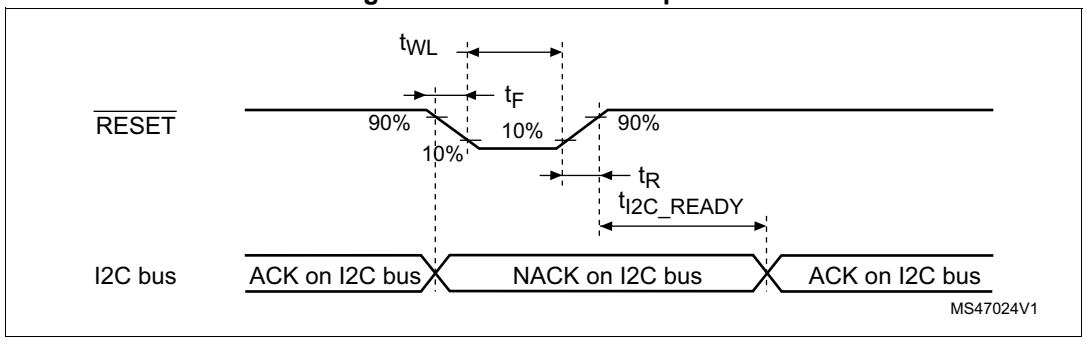


Table 4. Power-on and reset sequence timings

Name	Description	Conditions	Min.	Typ.	Max.	Units
t_{HL}	Minimum time before de-asserting $\overline{\text{RESET}}$ after power-up	-	0	-	-	µs
S_{VCC}	V_{CC} rising slope (from 10% to 90% of nominal value)	-	0.05	-	5	V/µs

Table 4. Power-on and reset sequence timings (continued)

Name	Description	Conditions	Min.	Typ.	Max.	Units
T_{set_4mA}	Minimum time required to supply 4 mA	From POWER OFF	-	-	500	ns
		From IDLE	-	-	150	
t_{WL}	Pulse width for Reset	-	1	-	-	µs
t_R/t_F Reset	Reset rise and fall time	$V_{CC} > V_{POR}$	-	-	1	µs
t_{I2C_READY}	Delay for STSAFE-A1SX to accept I^2C commands after a reset sequence.	-	20	-	50	ms

5.2.5 Power consumption optimization

When the STSAFE-A1SX is not in use, it is possible to decrease its power consumption by removing the power supply properly, knowing that the power supply must remain for operations that require a context, for instance during sessions.

This could be achieved by using a transistor to pilot the STSAFE-A1SX power supply, or by using a GPIO able to provide a $I_{CC\text{-}PROC}$ current that respects the STSAFE-A1SX powering conditions.

5.3 DC characteristics

The following tables provide the detailed description of the DC operating conditions of STSAFE-A1SX from 1.62 V to 5.5 V voltages.

Table 5. DC operating specifications and input parameters

Name	Description	Conditions(1)	Min.	Max.	Units
V_{IH}	Input high voltage	T = 25 °C	0.7 × V_{CC}	-	V
V_{IL}	Input low voltage	T = 25 °C	0	0.3 × V_{CC}	V
I_{IH}	Input high current	RST	0	20	µA
		SDA, SCL	−1	1	
I_{IL}	Input low current	RST	0	2	µA
		SDA, SCL	−1	1	µA
V_{OL}	Output low voltage	I_{OL} = 1 mA	-	0.54	V
I_{OL}	Output low current	V_{CC} = 3.3 V and V_{OL} = 0.4 V	3	-	mA
CIN1	SCL input capacitance	V_{IN} = 0 to $V_{CC\ Max}$	-	30	pF
CIN2	SDA input capacitance	V_{IN} = 0 to $V_{CC\ Max}$	-	30	pF

1. $V_{CC\ Max}$ is the maximum V_{CC} as defined in *Table 3: Power supply specifications*.

5.4 AC characteristics

Table 6. AC characteristics

Name	Description	Min.	Typ.	Max.	Units
t_R, t_F Reset	Reset rise and fall time	-	-	1	µs
t_{WL}	Pulse width for Reset	1	-	-	µs

Table 7. I²C operating conditions

Name	Description	Standard mode		Fast mode		Units
		Min.	Max.	Min.	Max.	
f_{SCL}	SCL frequency of sub-device: processor	-	100	-	400	kHz
$t_{HD;STA}$	Input low to Clock low (Start condition hold time)	4.0	-	0.6	-	µs
t_{LOW}	Low period of SCL clock	4.7	-	1.3	-	µs
t_{HIGH}	High period of SCL clock	4.0	-	0.6	-	µs
$t_{SU;STA}$	Clock high to Input Transition / Setup time for a (repeated) Start condition See Note	4.7	-	0.6	-	µs
$t_{HD;DAT}$	Clock low to Input transition	0(1)	(2)	0(1)	(2)	µs
$t_{SU;DAT}$	Input transition to Clock transition Data setup time	250	-	100	-	ns
$t_{SU;STO}$	Clock high to Input high (Stop)	4.0	-	0.6	-	µs
t_{BUF}	Input high to Input low (bus free between stop and start)	4.7	-	1.3	-	µs
t_R	Clock and Data rise time on load capacitance of 30 pF	-	1000	20	300	ns
t_F	Clock and Data fall time on load capacitance of 30 pF	-	300	10	300	ns

1. The device must internally provide a hold time of at least 300 ns for the SDA signal in order to bridge the undefined region of the falling edge of SCL.
2. The maximum $t_{HD;DAT}$ could be 3.45 µs and 0.9 µs for Standard mode and Fast mode, but must be less than the maximum of $t_{VD;DAT}$ or $t_{VD;ACK}$ by a transition time. This maximum must only be met if the device does not stretch the LOW period (t_{LOW}) of the SCL signal. If the clock stretches the SCL signal, the data must be valid by the setup time before it releases the clock.

Table 8. I²C filter characteristics

Symbol	Parameter	Min	Max	Unit
t_{SP}(1)	Pulse width of spikes that are suppressed by filter	0	50	ns

1. Guaranteed by design, not tested in production

Figure 16. AC clock and data timings

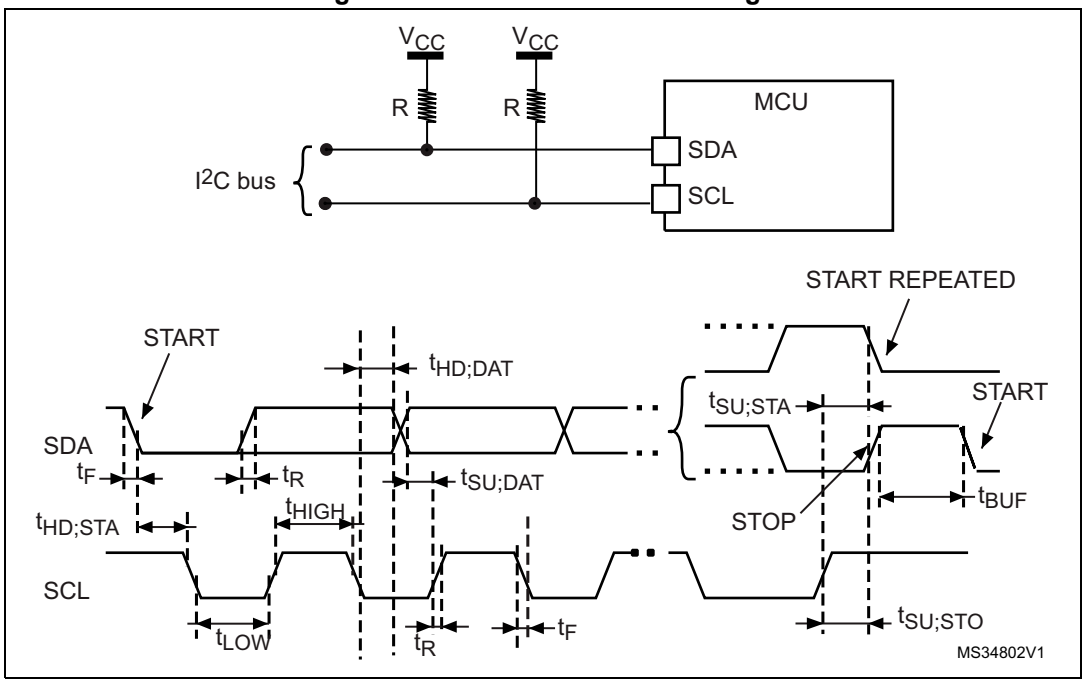


Table 9. AC measurement conditions

Description	Range	Units
Input pulse voltages	0.2 × V_{CC} to 0.8 × V_{CC}	V
Input and Output timing reference voltages	0.3 × V_{CC} to 0.7 × V_{CC}	V

6 Package information

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK packages, depending on their level of environmental compliance. ECOPACK specifications, grade definitions and product status are available at: *www.st.com*. ECOPACK is an ST trademark.

6.1 SO8N package information

Figure 17. SO8N – 8-lead plastic small outline, 150 mils body width, package outline

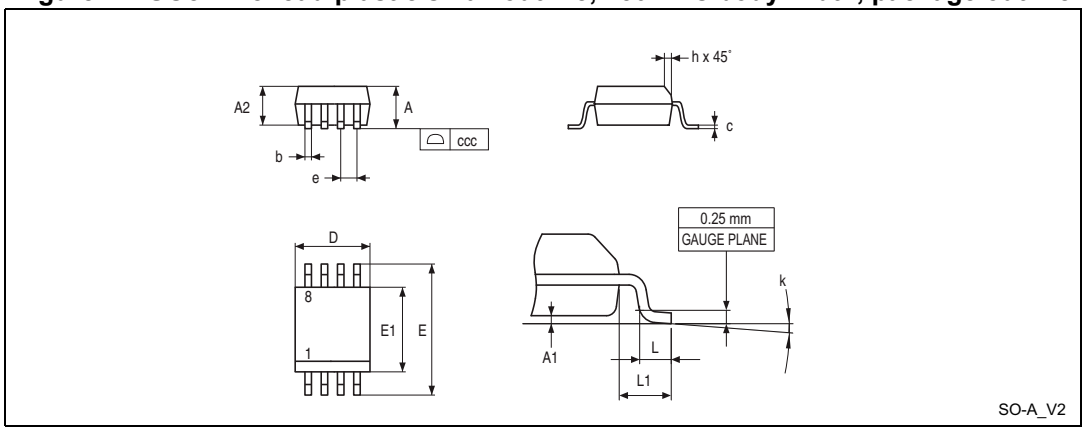


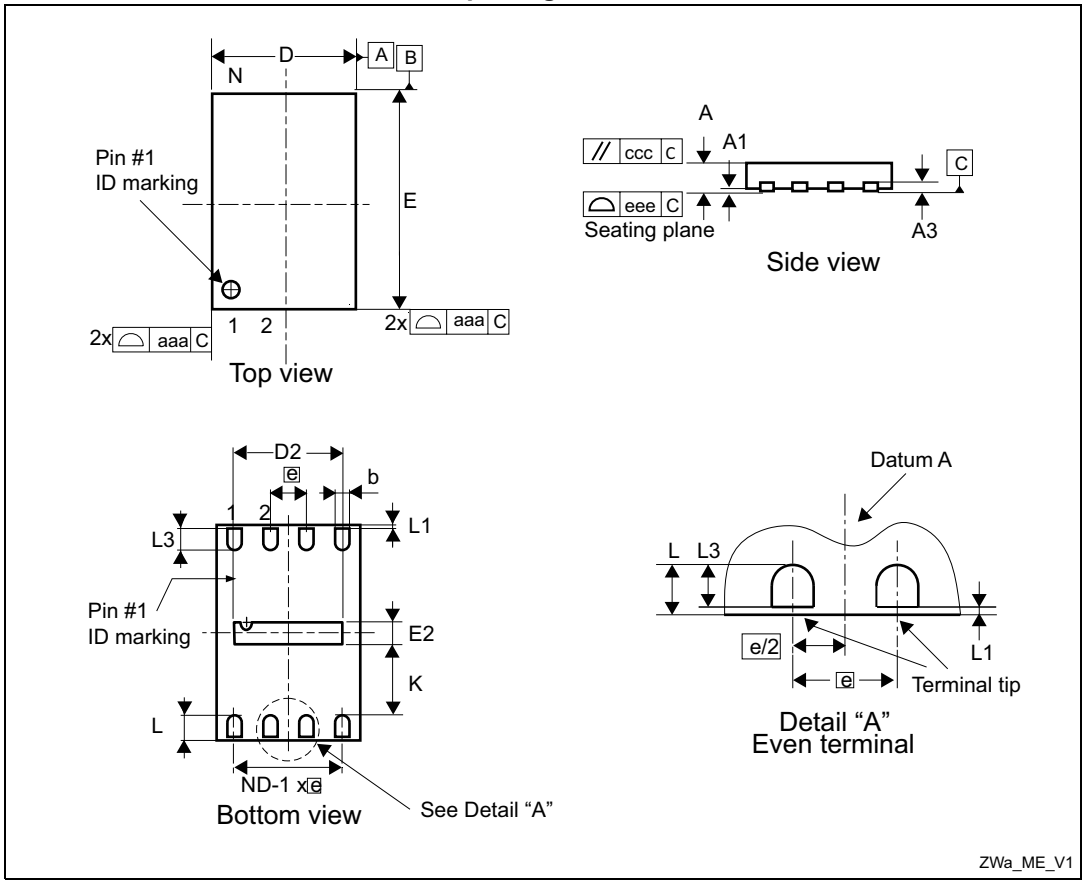
Table 10. SO8N – 8-lead plastic small outline, 150 mils body width, package mechanical data

Symbol	millimeters			inches [1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	-	-	1.750	-	-	0.0689
A1	0.100	-	0.250	0.0039	-	0.0098
A2	1.250	-	-	0.0492	-	-
b	0.280	-	0.480	0.0110	-	0.0189
c	0.170	-	0.230	0.0067	-	0.0091
ccc	-	-	0.100	-	-	0.0039
D	4.800	4.900	5.000	0.1890	0.1929	0.1969
E	5.800	6.000	6.200	0.2283	0.2362	0.2441
E1	3.800	3.900	4.000	0.1496	0.1535	0.1575
e	-	1.270	-	-	0.0500	-
h	0.250	-	0.500	0.0098	-	0.0197
k	0°	-	8°	0°	-	8°
L	0.400	-	1.270	0.0157	-	0.0500
L1	-	1.040	-	-	0.0409	-

1. Values in inches are converted from mm and rounded to four decimal digits.

6.2 UFDFPN8 package information

Figure 18. UFDFPN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package outline



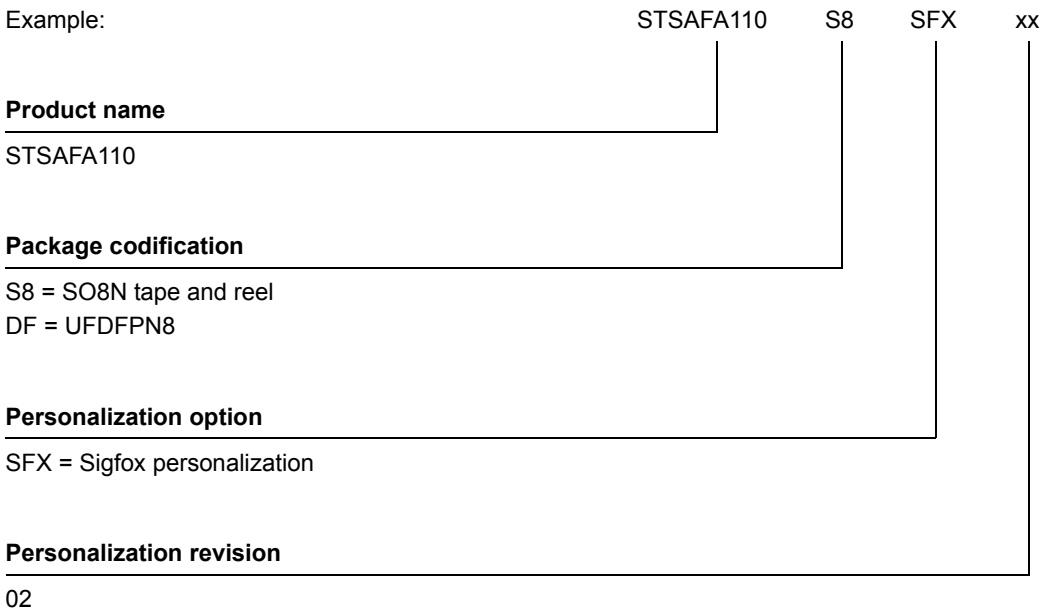
1. Max. package warpage is 0.05 mm.
2. Exposed copper is not systematic and can appear partially or totally according to the cross section.
3. Drawing is not to scale.

Table 11. UFDFPN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package mechanical data

Symbol	millimeters			inches[1]		
	Min	Typ	Max	Min	Typ	Max
A	0.450	0.550	0.600	0.0177	0.0217	0.0236
A1	0.000	0.020	0.050	0.0000	0.0008	0.0020
b[2]	0.200	0.250	0.300	0.0079	0.0098	0.0118
D	1.900	2.000	2.100	0.0748	0.0787	0.0827
D2	1.500	1.600	1.700	0.0591	0.0630	0.0669
E	2.900	3.000	3.100	0.1142	0.1181	0.1220
E2	0.100	0.200	0.300	0.0039	0.0079	0.0118
e	-	0.500	-	0.0197		
K	0.800	-	-	0.0315	-	-
L	0.400	0.450	0.500	0.0157	0.0177	0.0197
L1	-	-	0.150	-	-	0.0059
L3	0.300	-	-	0.0118	-	-
aaa	-	-	0.150	-	-	0.0059
bbb	-	-	0.100	-	-	0.0039
ccc	-	-	0.100	-	-	0.0039
ddd	-	-	0.050	-	-	0.0020
eee[3]	-	-	0.080	-	-	0.0031

1. Values in inches are converted from mm and rounded to 4 decimal digits.
2. Dimension b applies to plated terminal and is measured between 0.15 and 0.30 mm from the terminal tip.
3. Applied for exposed die paddle and terminals. Exclude embedding part of exposed die paddle from measuring.

7 Ordering information



Note: For a list of available options (speed, package, etc.) or for further information on any aspect of this device, please contact your nearest STMicroelectronics sales office.

8 Revision history

Table 12. Document revision history

Date	Revision	Changes
16-Nov-2018	1	Initial release.
20-Jun-2019	2	Updated document reference. Updated ambient operating temperature T_A. Small text changes.