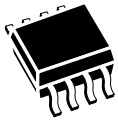
STSAFE-A100

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 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

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)

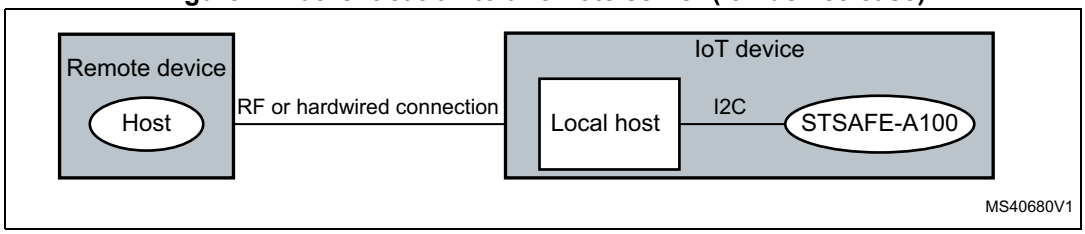
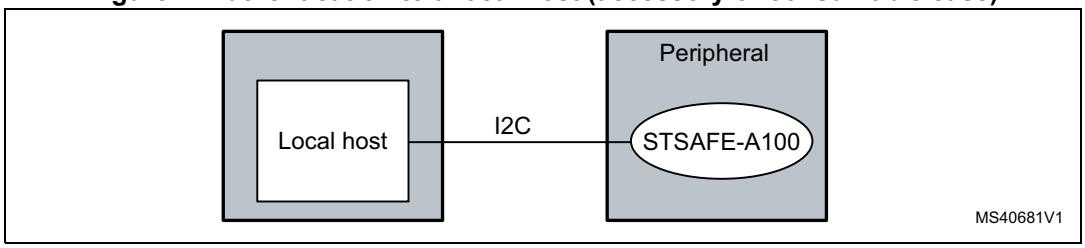


Figure 2. Authentication to a local host (accessory or consumable case)



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.

1.3 Pin and signal description

The two figures below show the pinouts of the device delivered in the SO8N and UFDFPN8 packages. *Table 1* describes the available pins/signals.

Figure 3. SO8N pinout - Top view

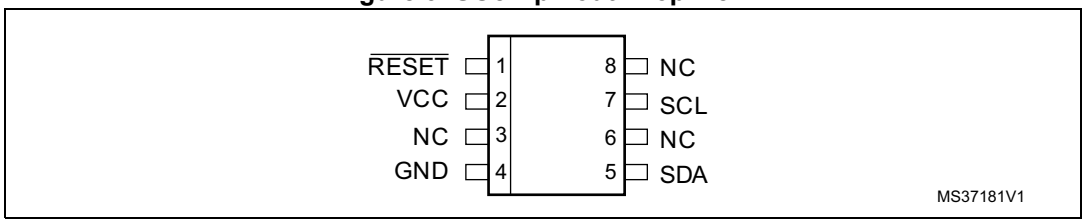


Figure 4. UFDFPN8 pinout - Top view

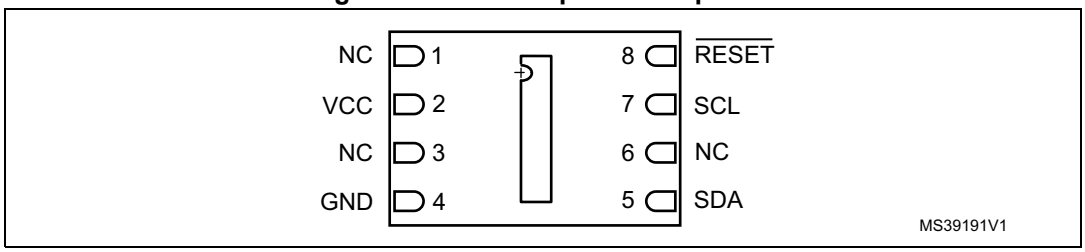


Table 1. Pin and signal description

Pin/signal	Function	Description
$\overline{\text{RESET}}$	Reset	This input signal is used to reset STSAFE-A100. 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.
V_{CC}	Power supply	The 1.62 to 5.5 V supply voltage is supported for powering all internal STSAFE-A100 functions.
GND	Ground supply	Ground reference pin for power and all I/O signals.
SCL	Serial clock	This input signal is used to strobe all data in and out of STSAFE-A100. 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-A100. The signal uses an open drain output configuration. An external pull-up resistor is used to “pull up” the output.
NC	Not connected	-

2 Electrical characteristics

Device operation is guaranteed as long as the device is operated within the operating limits specified below. Operating beyond these limits may affect the long-term reliability of the device.

2.1 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 5*. 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 5. Filtering capacitors on V_{CC}

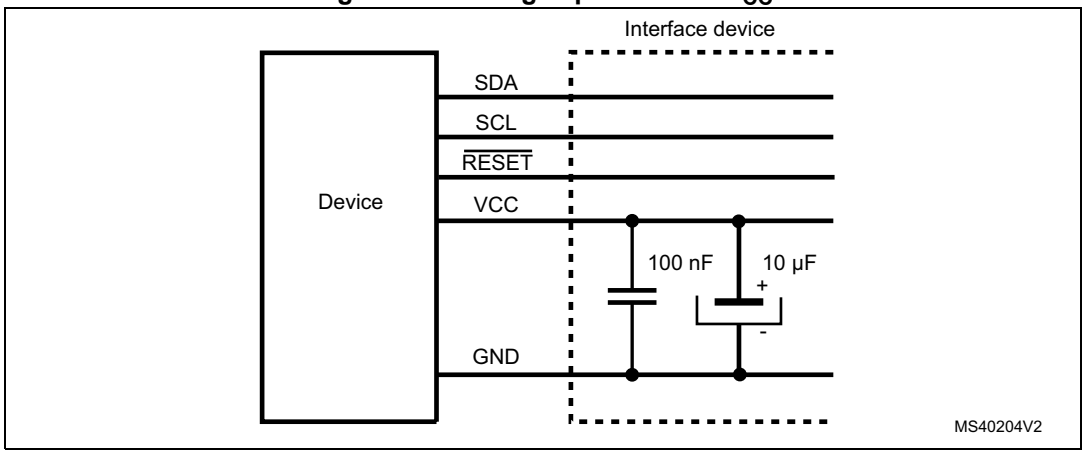


Table 2. V_{CC} rising slope

Symbol	Parameter	Min.	Typ.	Max.	Unit
S_{VCC}	V_{CC} rising slope (from 10% to 90% of nominal value)	0.05	-	5	V/µs

2.1.1 Power supply specifications

Table 3 provides the detailed description of the power requirements of STSAFE-A100.

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

Table 3. Power supply specifications (continued)

Name	Description	Conditions	Min.	Typ.	Max.	Units
$V_{CC-HIPS}$	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)	14	18	21	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. 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.

2.1.2 Power-on and reset sequence

Figure 6. Power-on and reset sequence

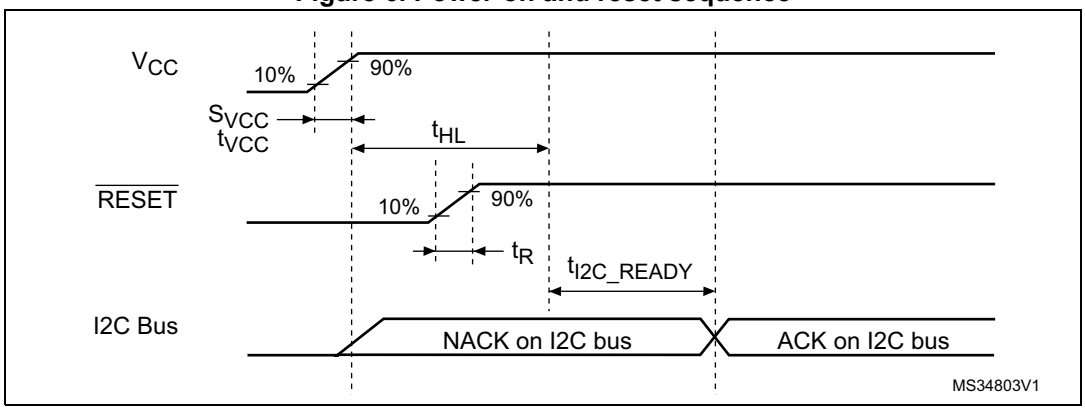


Figure 7. Warm reset sequence

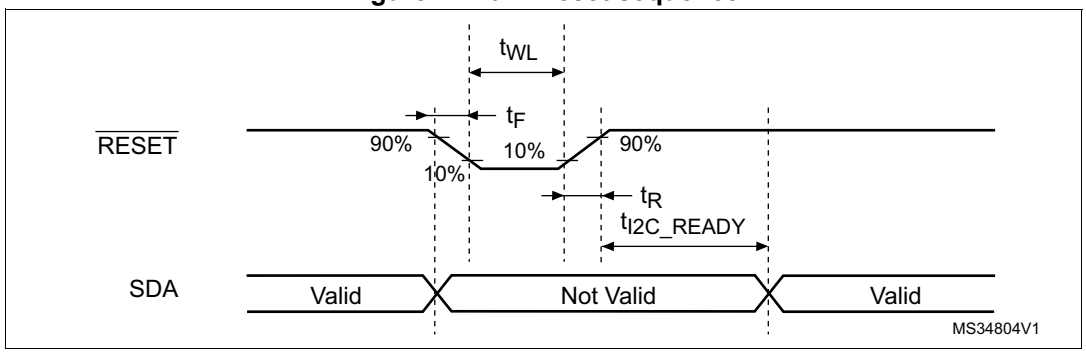


Table 4. Power-on and reset sequence timings

Name	Description	Conditions	Min.	Typ.	Max.	Units
t_{HL}	Minimum time before de-asserting RESET after power-up	-	0	-	-	µs
S_{VCC}	V_{CC} rising slope	-	0.05	-	5	V/µs
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-A100 to accept I^2C commands after a reset sequence.	-	20	-	50	ms

2.2 DC characteristics

The following tables provide the detailed description of the DC operating conditions of STSAFE-A100 from 1.62 V to 5.5 V voltages.

Table 5. DC operating specifications and input parameters

Name	Description	Conditions	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	0.2 × V_{CC}	V
I_{IH}	Input high current	RST	-	20	µA
		SDA, SCL	-	1	
I_{IL}	Input low current	-	-	2	µA
V_{OL}	Output low voltage	I_{OLmax} = 1 mA	-	0.54	V
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

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

2.3 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 subdevice: 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 8. AC clock and data timings

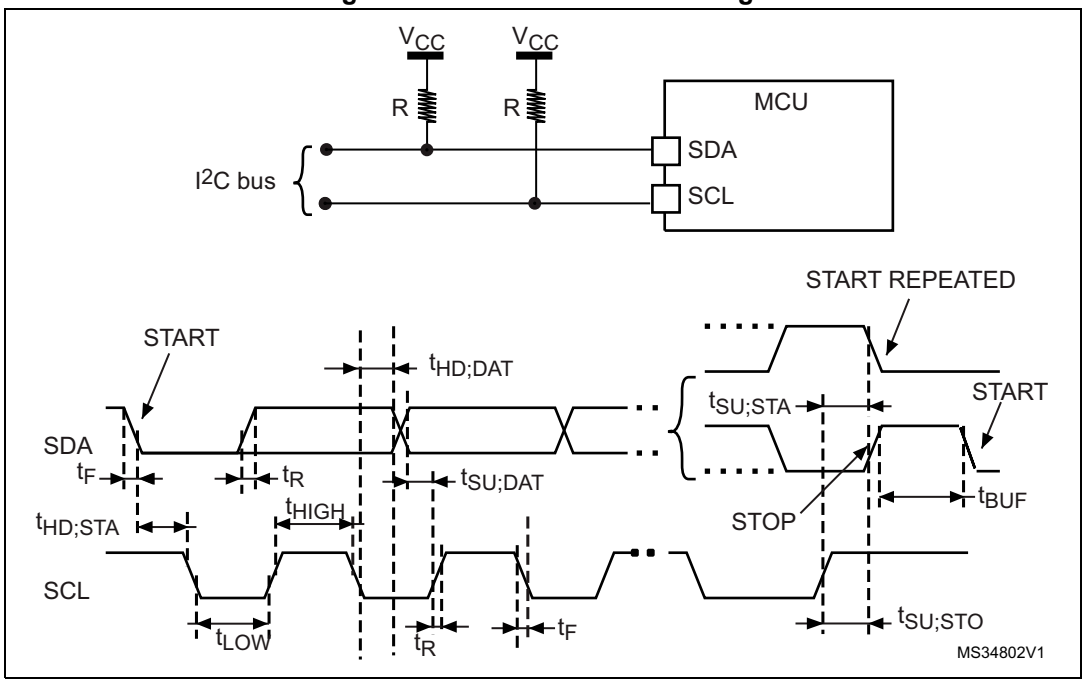


Table 9. AC measurement conditions

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

3 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.

3.1 SO8N package information

Figure 9. SO8N – 8-lead plastic small outline, 150 mils body width, package outline

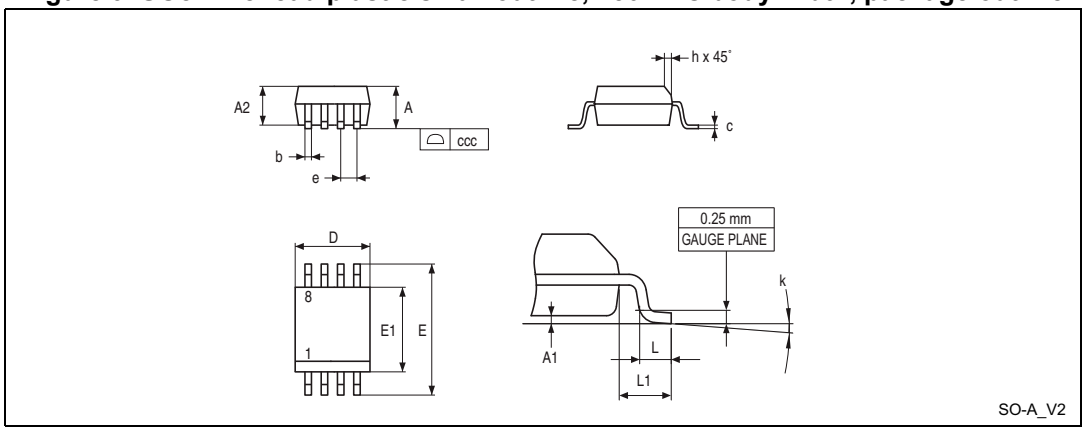


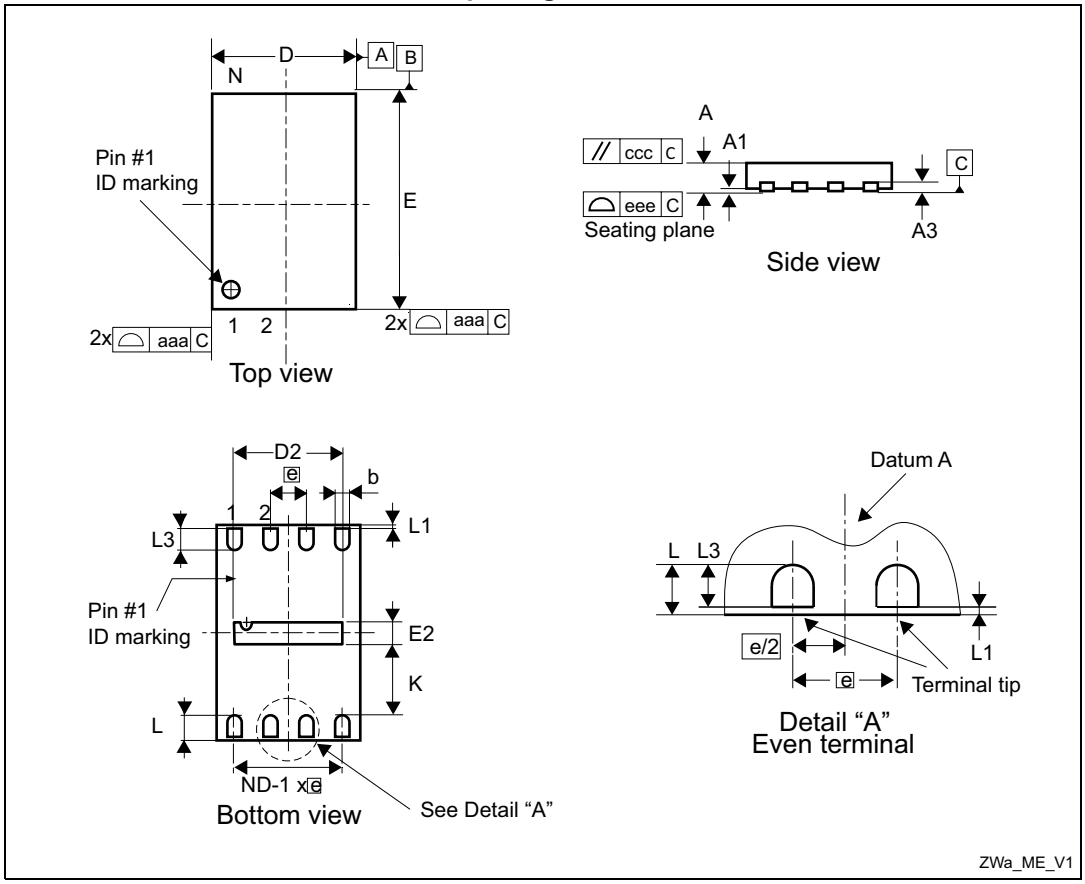
Table 10. SO8N – 8-lead plastic small outline, 150 mils body width, package mechanical data

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.

3.2 UFDFPN8 package information

Figure 10. 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.

4 Revision history

Table 12. Document revision history

Date	Revision	Changes
03-Feb-2016	1	Initial release.
19-Jul-2016	2	Updated *Table 1: Pin and signal description*. Added *Section 2: Electrical characteristics*. Added *Section 3: Package information*. Small text changes.
08-Dec-2016	3	Updated operating temperature in *Section : Hardware features*.