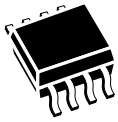
STSAFE-A1SX

Authentication, data integrity and confidentiality for Sigfox Ready™ IoT devices

Data brief



SO8N
4 × 5 mm

UFDFPN8 (2 × 3 mm)

Features

- Data integrity over the Sigfox network:
  - Signature of payloads before uplink
  - Verification of downlink payloads
- Optional data confidentiality over the Sigfox network:
  - Encryption of payloads before uplink
  - Decryption of downlink payloads

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 symmetric cryptography
  - AES-128
- Secure operating system
  - Secure STSAFE-A1SX kernel for authentication and data management
  - Protection against logical and physical attacks

Hardware features

- Highly secure MCU platform
- 6 Kbyte 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

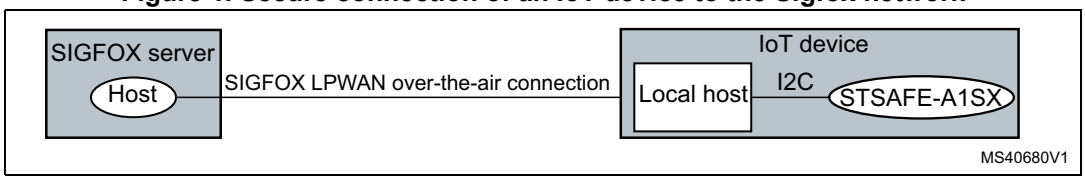
1 Description

The STSAFE-A1SX is a secure element that comes preloaded with Sigfox network keys, and provides secure services for data exchanges on the Sigfox's low-power wide-area network (LPWAN). It constitutes a plug-and-play solution that allows Sigfox Ready™ IoT (Internet of things) devices to connect to the Sigfox network while ensuring data integrity and confidentiality. The STSAFE-A1SX is a highly secure, tamper-resistant solution that relies on a certified, secure EAL5+ Common Criteria chip, on top of which runs a dedicated secure operating system.

The STSAFE-A1SX can be integrated in IoT devices designed for the Sigfox LPWAN in applications such as industrial, utility or transportation.

1.1 Key function overview

Figure 1. Secure connection of an IoT device to the Sigfox network



The STSAFE-A1SX can be integrated in an IoT device designed to connect to the Sigfox LPWAN network through a secure connection that ensures device authentication, data exchange integrity and data exchange confidentiality.

The STSAFE-A1SX secure element supports the following features:

- Preprovisioned keys

  The STSAFE-A1SX comes preloaded with device IDs and Sigfox network keys that allow the IoT device to directly connect to the Sigfox network. The keys are never exposed or used outside of the secure element.

- Data exchange integrity

  The STSAFE-A1SX generates the MACs of uplink frames for verification by the network server. Likewise, the STSAFE-A1SX verifies the MACs of downlink frames generated by the Sigfox network server.

Note: The verification of the MAC of an uplink frame provides authentication of the secure element. It proves that the data were sent by an authentic Sigfox Ready™ IoT device.

- Data confidentiality
  - The STSAFE-A1SX encrypts uplink frames before uplink, and decrypts downlink frames after downlink.
  - This service is based on AES (advanced encryption standard) symmetric cryptography.
  - The activation of this service is optional.
- Pairing and secure channel with the host
  - The STSAFE-A1SX allows a secure channel to be set up with the local host based on AES-128-bit keys. Typically, this secure channel prevents eavesdropping of sensitive information on the I²C line.
  - The activation of this service is optional.

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 includes a command wrapper as well as generic use cases.

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 2. SO8N pinout - Top view

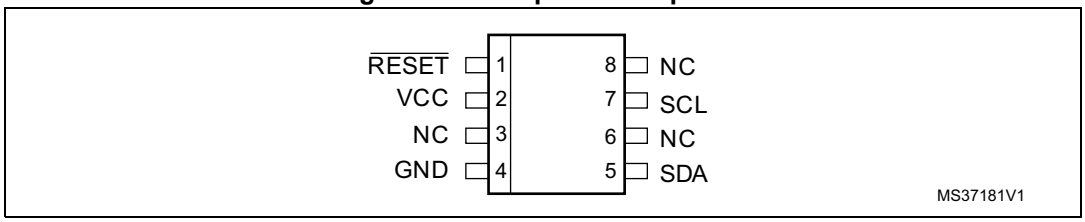


Figure 3. UFDFPN8 pinout - Top view

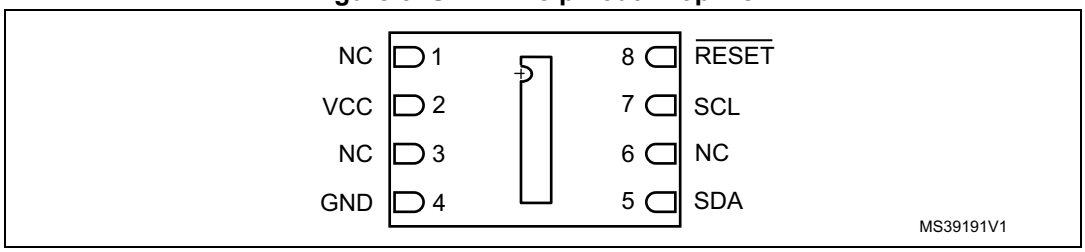


Table 1. Pin and signal description

Pin/signal	Function	Description
$\overline{\text{RESET}}$	Reset	This input signal is used to reset STSAFE-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.
V_{CC}	Power supply	The 1.62 to 5.5 V supply voltage is supported for powering all internal STSAFE-A1SX 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-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.

Table 1. Pin and signal description (continued)

Pin/signal	Function	Description
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	-

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 4*. 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 4. Filtering capacitors on V_{CC}

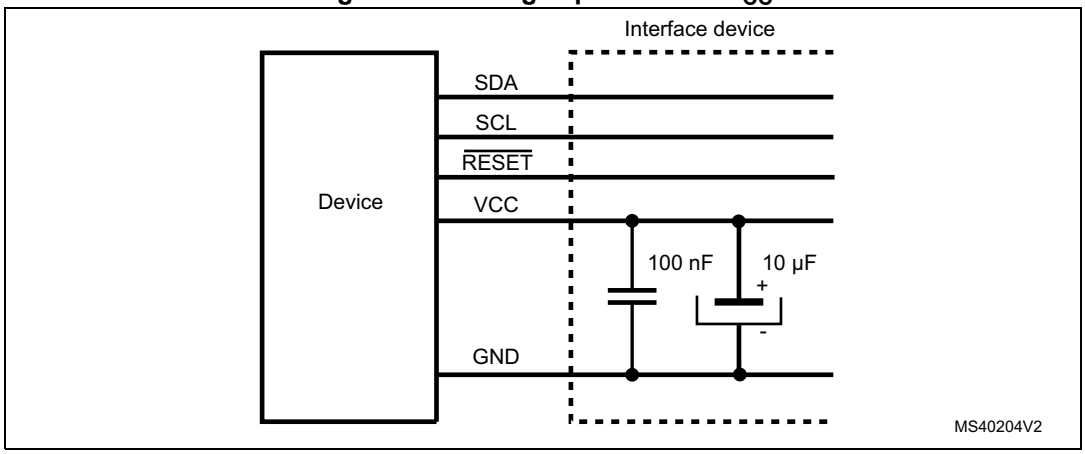


Table 2. V_{CC} rising slope

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-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.

2.1.2 Power-on and reset sequence

Figure 5. Power-on and reset sequence

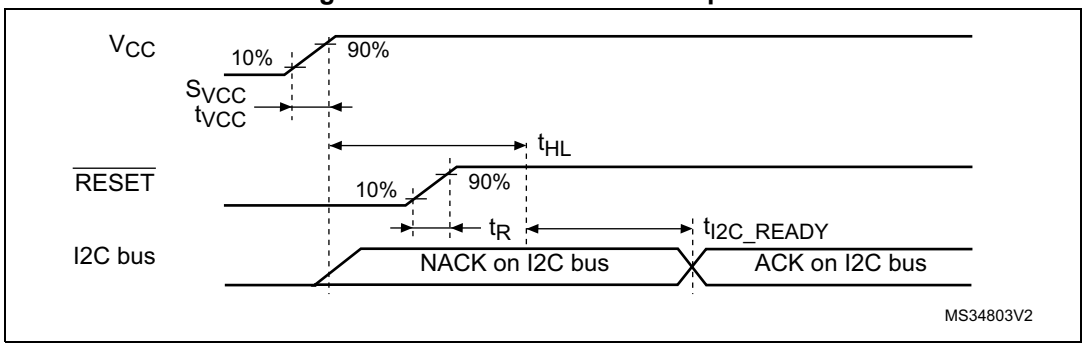


Figure 6. Warm reset sequence

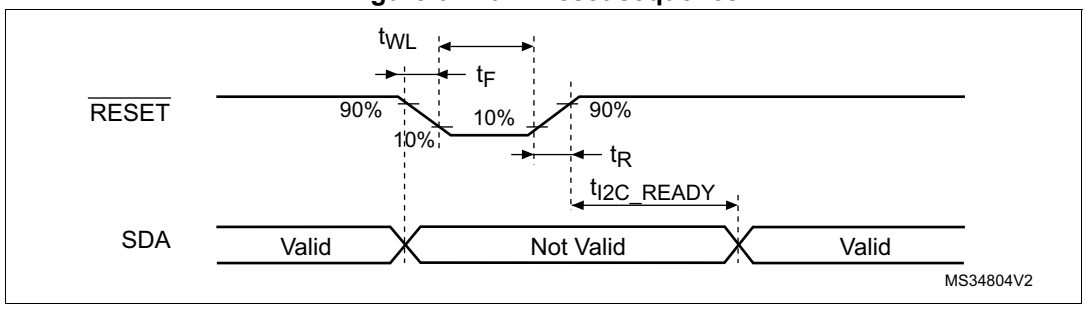


Table 4. Power-on and reset sequence timings

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-A1SX 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-A1SX 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 7. AC clock and data timings

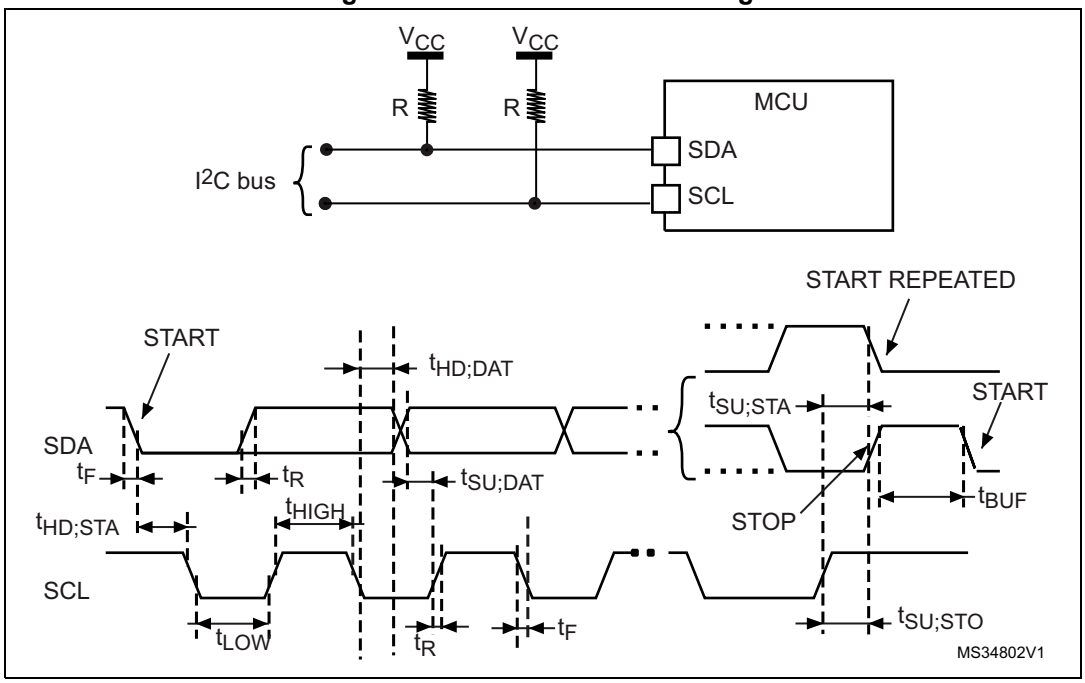


Table 9. AC measurement conditions

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

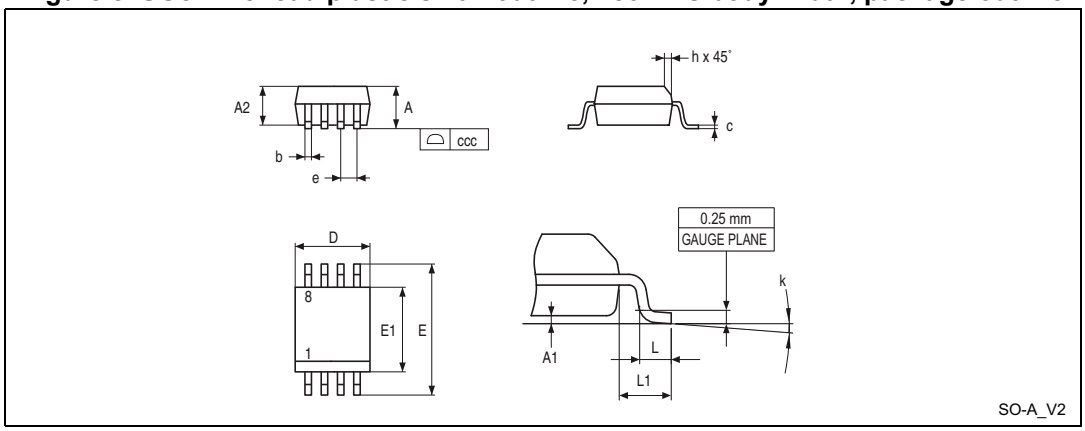


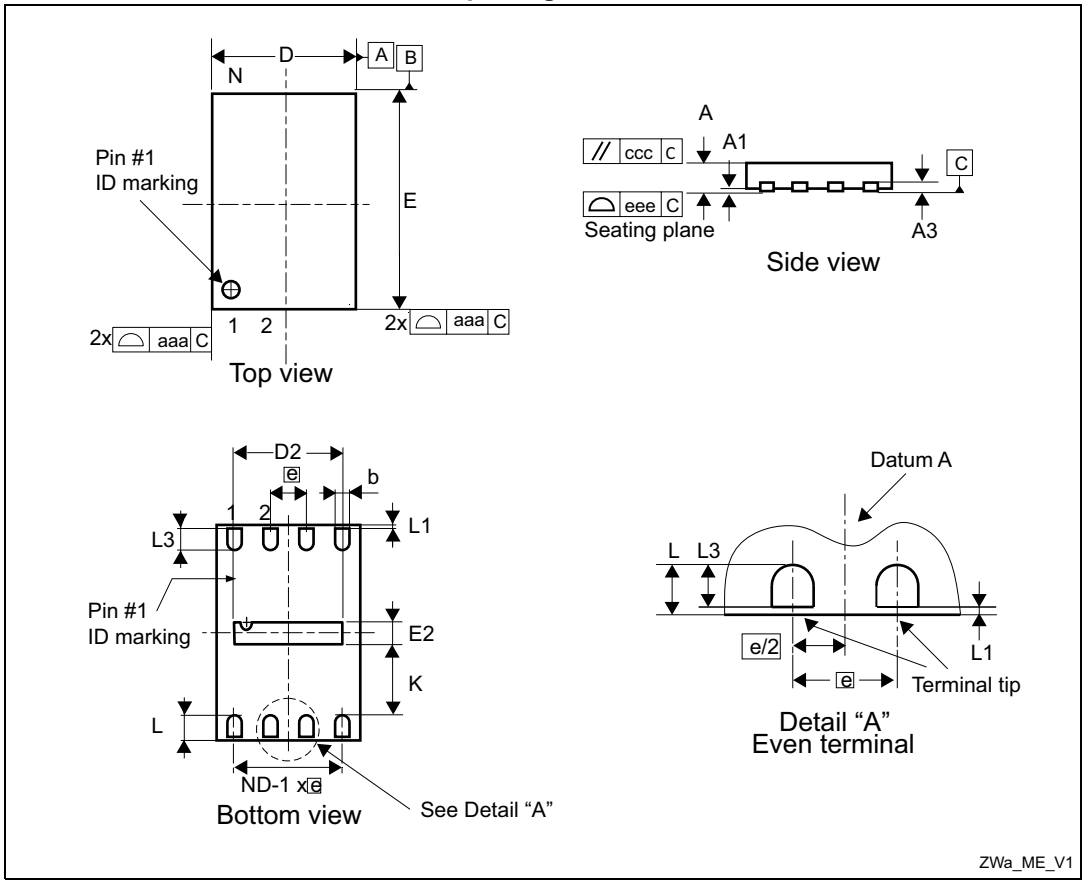
Table 10. SO8N – 8-lead plastic small outline, 150 mils body width, package mechanical data

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 9. 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
20-Feb-2017	1	Initial release.