



SQ7131/SQ7133

Brief Datasheet V1.3

SQ7131/SQ7133 , Low Power Secure Coprocessor, ECC-256/384, ECDSA, ECDH, AES-128/ AES-256, SHA-256,TRNG

◆ Basic Information

- Operating Voltage: 2.0V ~ 5.5V
- Operating Temperature: -40°C ~ 85°C

◆ Communication

- SQ7131 support standard I2C (Max: 1MHz)
- SQ7133 support standard SPI (Max: 10MHz@MODE3)

◆ Security Features

- NIST Standard H/W Accelerator for Asymmetric Sign, Verify, Key Agreement
 - NIST Standard P-256 /P-384 Elliptic Curve Support
 - ECDSA: FIPS186-4 Curve Digital Signature
 - ECDH: FIPS SP800-56A Key Agreement
- NIST Standard H/W Support for Symmetric Algorithm
 - FIPS 180-4 SHA-256 & FIPS 198-1 HMAC Hash Algorithm
 - FIPS-197 AES-128/256 : Encrypt/ Decrypt, Galois Field Multiply for GCM
- Networking Key Management Support
 - PRF/HKDF Calculation for TLS 1.2 & 1.3
 - ECDHE : Ephemeral key generation and key agreement
- High Quality NIST SP800-22 Compliant TRNG
- Active Tamper Detection and Reacts to Perturbation Attacks.
- Simple/ Differential Power Analysis Attact Countermeasuer (SPA/DPA)
- Independent Internal Clock to Prevent Glitch Attack
- 128-bit Unique ID (UID)

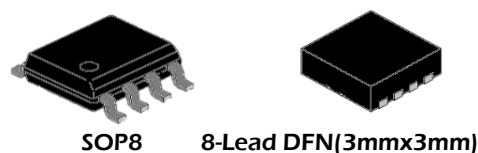
◆ Secure Storage

- Chip-Dependent Encryption Technology
- Secure Storage for Key, X.509 Compressed Certificate , Data
- Large User Data Storage : 5.6KB

◆ Application

- | | |
|--|----------------------------|
| ■ Secure TLS 1.2 and 1.3 Communication | ■ Accessory Authentication |
| ■ AIoT Device Security | ■ End-to-End Encryption |
| ■ Secure Boot/ Secure OTA | ■ Anti-cloning |

Package Type



SOP8

8-Lead DFN(3mmx3mm)

No. : TDDS01-S7131-EN(B)	Name : SQ7131/SQ7133 Brief Datasheet	Version : V1.3
--------------------------	--------------------------------------	----------------

Content

1.PREFACE	4
2. PIN ASSIGNMENT/ DESCRIPTION	5
2.1 SQ7131 PIN ASSIGNMENT/ DESCRIPTION	5
2.2 SQ7133 PIN ASSIGNMENT/ DESCRIPTION	6
3. ELECTRONIC CHARACTERISTICS	7
3.1 ABSOLUTE MAXIMUM RATINGS	7
3.2 OPERATION CONDITIONS.....	8
3.2.1 Operation Conditions	8
3.2.2 I/O Characteristics.....	8
3.3 DC CHARACTERISTICS.....	9
3.4 POWER-ON RESET CHARACTERISTICS	10
3.5 BROR CHARACTERISTICS	11
3.6 AC CHARACTERISTICS	12
3.6.1 AC Parameters	12
3.6.2 I2C Characteristics	13
3.6.3 SPI Characteristics	14
3.7 EEPROM CHARACTERISTICS	15
APPENDIX A. PACAKGE INFORMATION	16
APPENDIX B. APPLICATION NOTE.....	18
REVISION HISTORY	19

1. Preface

SQ7131/SQ7133 supports many hardware cryptographic accelerators: embedded high-quality TRNG (True Random Number Generator), SHA-256, asymmetric encryption ECC-384/ECC-256, and symmetric encryption AES-128/AES-256. It also has secure storage for ECC and AES keys storage.

The device is suitable for building high-security applications, such as IoT symmetric/asymmetric authentication, attestation, TLS1.2/1.3 secure connections, secure boot, secure OTA, and F/W protection, etc.

Secure storage for ECC and AES keys :

Key Type	SQ7131/SQ7133	Note
AES Key (AES-128/256)	12	Slot 8~19
ECC Private Key – 256	7	Slot 1~7
ECC Private Key – 384	2	Slot 20,21
ECC Public Key – 256	4	Slot 24,26~28
ECC Public Key – 384	4	Slot 30,32~34

TABLE 1-1 AES AND ECC KEY SLOTS

2. Pin Assignment/ Description

2.1 SQ7131 Pin Assignment/ Description

PRODUCTS : SQ7131SP008C00R

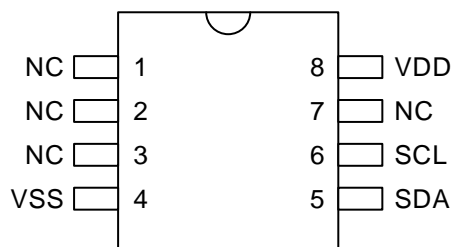


FIGURE 2-1 PIN ASSIGNMENT OF SQ7131 SOP8

PRODUCTS : SQ7131N3008C00R

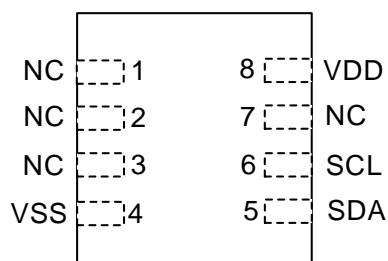


FIGURE 2-2 PIN ASSIGNMENT OF SQ7131 8-LEAD DFN

Pin No.	Pin Name	I/O Type	Function Description
1	NC	-	No Connect
2	NC	-	No Connect
3	NC	-	No Connect
4	VSS	GND	Ground
5	SDA	I/O	SDA, I2C bus data input/output
6	SCL	I	SCL, I2C bus clock input/output
7	NC	-	No Connect
8	VDD	Power	Positive Power Supply

2.2 SQ7133 Pin Assignment/ Description

PRODUCTS : SQ7133SP008S00R

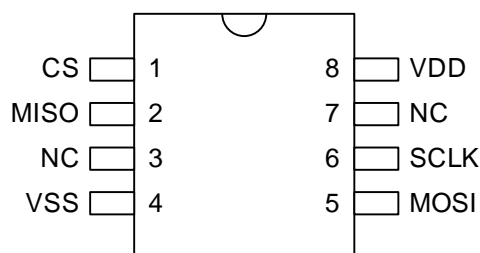


FIGURE 2-3 PIN ASSIGNMENT OF SQ7133 SOP8

PRODUCTS : SQ7133N3008S00R

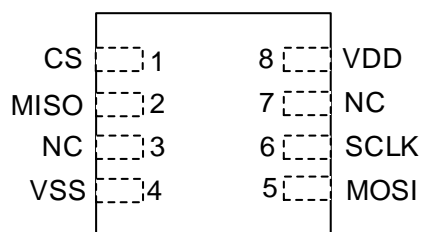


FIGURE 2-4 PIN ASSIGNMENT OF SQ7133 8-LEAD DFN

Pin No.	Pin Name	I/O Type	Function Description
1	CS	I	SPI, Chip Select
2	MISO	O	SPI, Master In Slave Out
3	NC	-	No Connect
4	VSS	GND	Ground
5	MOSI	I	SPI, Master Out Slave In
6	SCLK	I	SPI, SPI Clock
7	NC	-	No Connect
8	VDD	Power	Positive Power Supply

3. Electronic Characteristics

3.1 Absolute Maximum Ratings

The absolute maximum ratings are rated values which must not be exceeded during operation, even for an instant. Any one of the ratings must not be exceeded. If any absolute maximum rating is exceeded, a device may break down or its performance may be degraded, causing it to catch fire or explode resulting in injury to the user. Thus, when designing products which include this device, ensure that no absolute maximum rating value will ever be exceeded.

(V_{SS}=0V)

Parameter	Symbol	Pins	Ratings	Unit
Supply Voltage	V _{DD}	-	-0.3 to 6.0	V
Input Voltage	V _{IN}	All I/O pins	-0.3 to V _{DD} +0.3	V
Output Current(Total)	I _{OL}	All I/O pins	100	mA
Storage Temperature	T _{STG}	-	-50 to 125	°C

3.2 Operation Conditions

The following defines the electrical characteristics of the device when it is operated at voltage and temperature maximum/minimum values. Unless otherwise stated, the standard conditions were determined at "operating temperature 25 °C and operating voltage VDD = 3.3 V".

3.2.1 Operation Conditions

Parameter	Symbol	Condition	Min.	Typ.	Max.	Unit
Supply Voltage	V _{DD}		2.0	3.3	5.5	V
Operating Temperature	T _a		-40	25	85	°C

3.2.2 I/O Characteristics

Parameter	Symbol	Condition	Min.	Typ.	Max.	Unit
Input Low Voltage	V _{IL}	VDD=5V, temperature=25 °C	0		0.3 VDD	V
Input High Voltage	V _{IH}	VDD=5V, temperature=25 °C	0.7 VDD		VDD	V
Output Low Voltage	V _{OL}	VDD=5V, temperature=25 °C IOL= 3 mA	0		0.1 VDD	V
Output High Voltage	V _{OH}	VDD=5V, temperature=25 °C IOH= -3 mA	0.9VDD		VDD	V

3.3 DC Characteristics

Parameter	Symbol	Min.	Typ.	Max.	Unit
Supply Current in Operation Mode (Note)	I_{DD_NI}	-	3.7	-	mA
Supply Current in Deep Sleep Mode	I_{DD_DS}	-	0.3	-	uA

Note : The condition is waiting for Commands.

3.4 Power-on Reset Characteristics

Ta=-40~85°C					
Symbol	Description	Min.	Typ.	Max.	Unit
tPPW	Power-on reset minimum pulse width	1	-	-	ms
tPWUP	Warming-up time after a reset is clear and device ready	-	4	-	ms
tVDD	Power supply rise time	0.5	-	5	ms

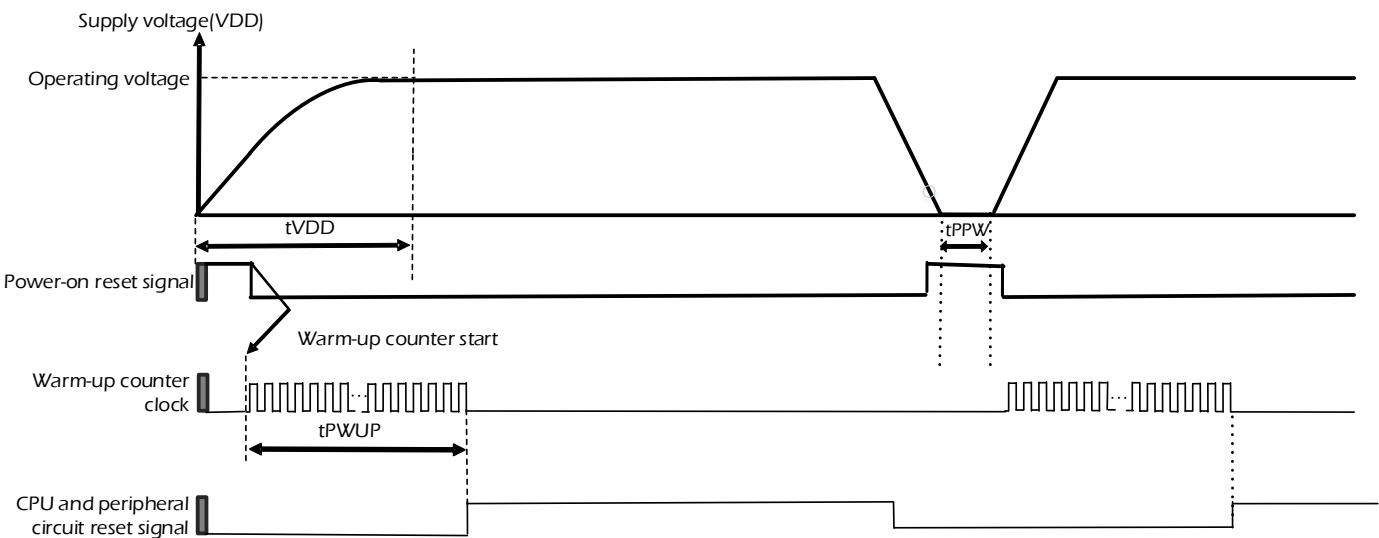


FIGURE 3- 1 OPERATION TIMING OF POWER-ON RESET

Note : In power-down process, the VDD must be 0V, then re-power-on to ensure the IC operating normal.

No. : TDDS01-S7131-EN(B)	Name : SQ7131/SQ7133 Brief Datasheet	Version : V1.3
--------------------------	--------------------------------------	----------------

3.5 BROR Characteristics

Ta=-40~85°C

Parameter	Symbol	Condition	Min.	Typ.	Max.	Unit
BROR detected voltage	VBROR_Falling	VDD fall time > tVDD (tVDD please refer to CH3.4 Power-on Reset Characteristics)	1.85	1.90	1.95	V

3.6 AC Characteristics

3.6.1 AC Parameters

Parameter	Symbol	Min.	Typ.	Max.	Unit
Power-Up Ready Time	T_{PU_RDY}	-	9.5	-	ms
Power-Up Ready Time – Ready for Command	T_{CMD_RDY}	-	18.5	-	ms
Standby Time, Entering the deep sleep mode	T_{STB}	-	20	-	us
Wake-Up Ready Time, deep sleep mode	T_{WDS_RDY}	-	2.4	-	ms

Note: The “Typ.” value is based on 25°C room temperature, and the Sleep command will change this value.

3.6.2 I2C Characteristics

Parameter	Symbol	Min	Max.	Unit
Clock Frequency	f_{SCL}	0	1	MHz
Hold Time Repeated START Condition	$t_{HD;STA}$	0.45	-	us
Low Period of SCL Clock	t_{LOW}	0.65	-	us
High Period of SCL Clock	t_{HIGH}	0.35	-	us
Setup Time for a Repeated START Condition	$t_{SU;STA}$	0.35	-	us
Data Hold Time	$t_{HD;DAT}$	-	0.5	us
Data Setup Time	$t_{SU;DAT}$	0.1	-	us
Rise Time of both SDA and SCL	t_r	20	300	ns
Fall Time of both SDA and SCL	t_f	20	300	ns
Setup Time of STOP Condition	$t_{SU;STO}$	0.6	-	us
Bus Free Time between a STOP and START Condition	t_{BUF}	1.3	-	us
Capacitive Load for each Bus Line	C_b	-	400	pF

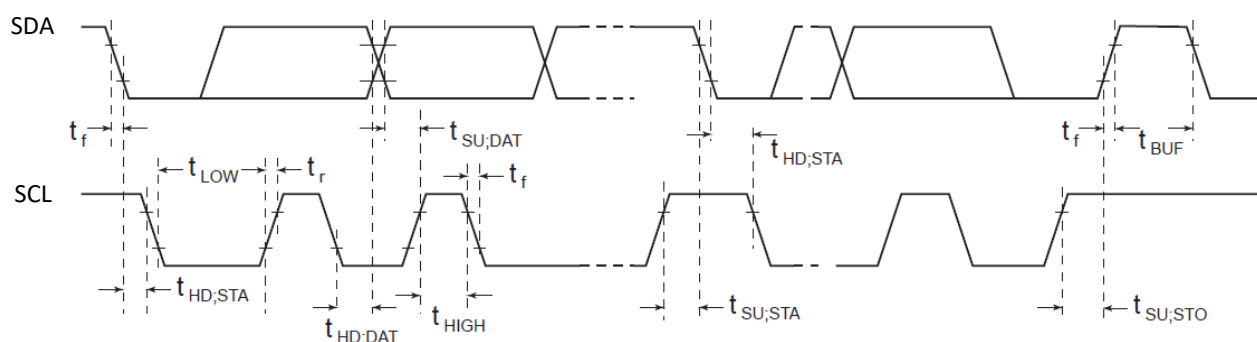


FIGURE 3-2 I2C TIMING SEQUENCE

3.6.3 SPI Characteristics

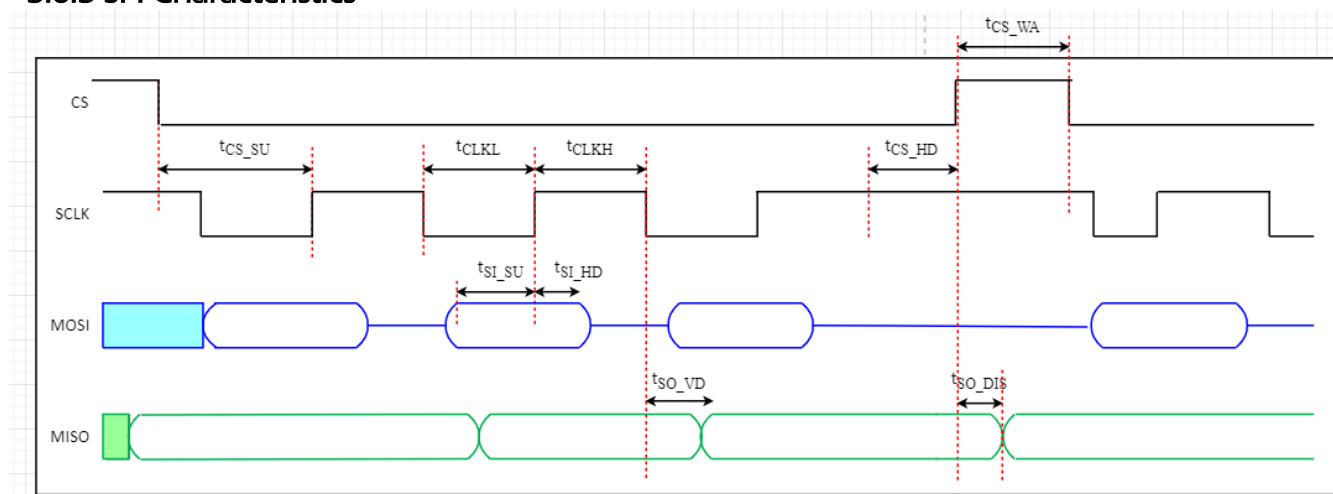


FIG 3-3 SPI TIMING SEQUENC

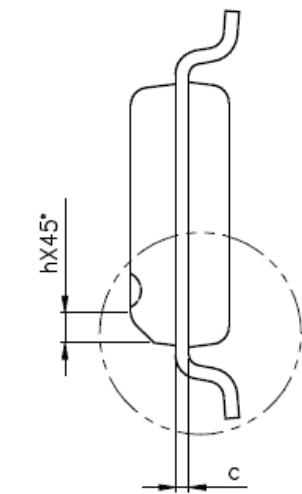
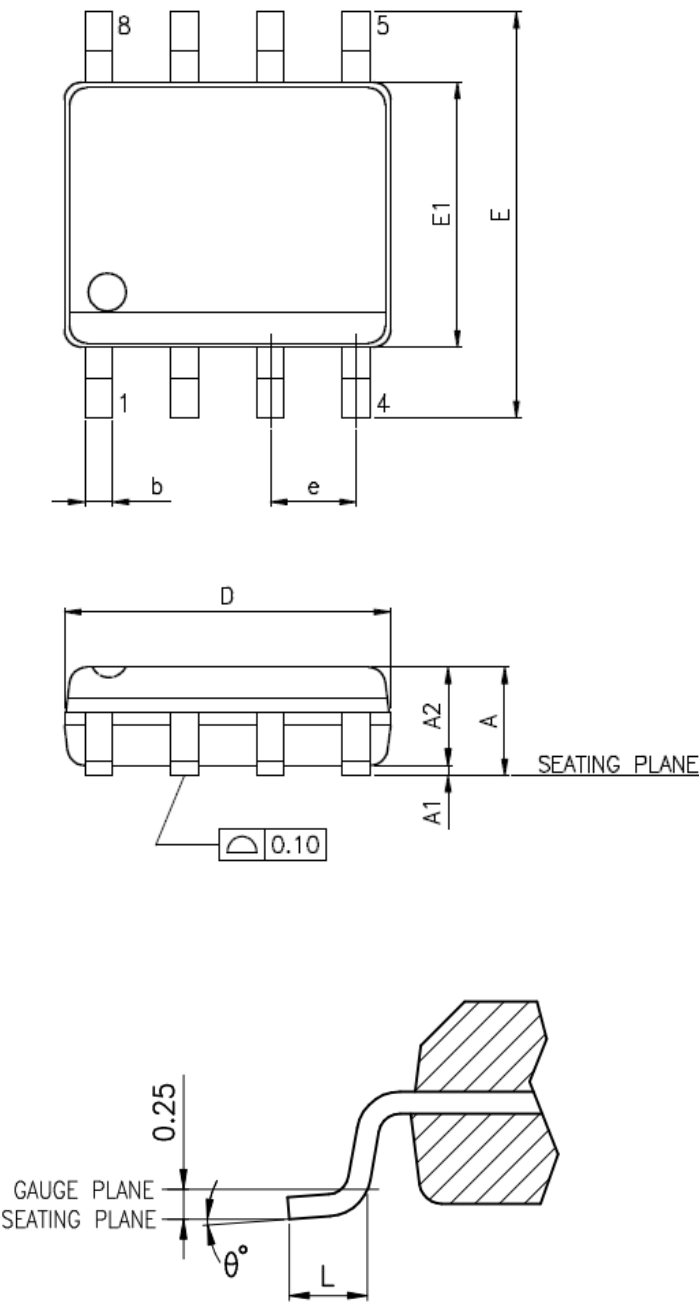
Parameter	Symbol	Min.	Max.	Unit
SPI Frequency	fSPI	-		
(VDD=2.7V~5.5V)			10	MHz
(VDD=2.0V~2.7V)			5	MHz
SPI Period	tSPI	1/fSPI	-	ns
High period of the SCLK pin	tCLKH	0.4 tSPI	-	ns
Low period of the SCLK pin	tCLKL	0.4 tSPI	-	ns
From SPICS active to first sample edge	tCS_SU	2.0 tSPI	-	ns
From last SCLK shift edge to SPICS inactive	tCS_HD	2.0 tSPI	-	ns
Time between SPI transaction	tCS_WA	3.0 tSPI	-	ns
Data Input Setup Time	tSI_SU	25	-	ns
Data Input Hold time	tSI_HD	10	-	ns
Data Output Valid Time	tSO_VD	-	25	ns
Data Output Disable Time	tSO_DIS	-	25	ns

3.7 EEPROM Characteristics

Parameter	Min.	Typ.	Max.	Unit
Write Endurance (Sector Endurance)	100,000	-	-	Cycles
Data Retention(at 25°C)	100	-	-	Years
Data Retention(at 85°C)	20	-	-	Years

Appendix A. Pacakge Information

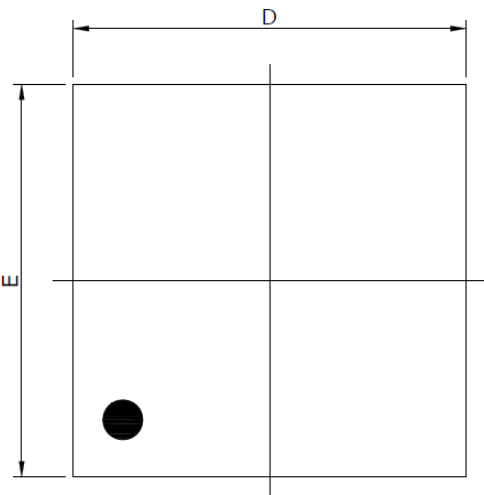
SOP8



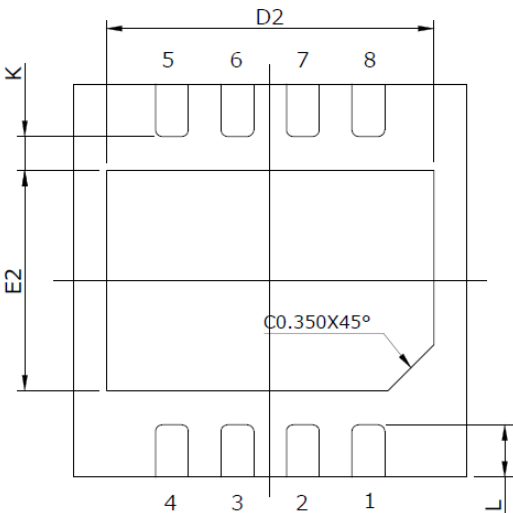
Symbol	mm		
	Min.	Typ.	Max.
A	–	–	1.75
A1	0.10	–	0.25
A2	1.25	–	–
b	0.31	–	0.51
c	0.10	–	0.25
D	4.90 BSC		
E	6.00 BSC		
E1	3.90 BSC		
e	1.27 BSC		
L	0.40	–	1.27
h	0.25	–	0.50
θ	0°	–	8°

No. : TDDS01-S7131-EN(B)	Name : SQ7131/SQ7133 Brief Datasheet	Version : V1.3
--------------------------	--------------------------------------	----------------

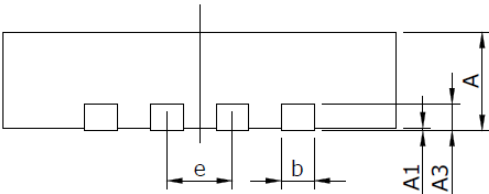
8-Lead DFN (3mm x3mm)



TOP VIEW



BOTTOM VIEW



Symbol	mm		
	Min.		Max
A	0.70	0.75	0.80
A1	0.00	0.02	0.05
A3	0.203 REF.		
b	0.20	0.25	0.30
D	2.90	3.00	3.10
E	2.90	3.00	3.10
e	0.50 BSC		
L	0.35	0.40	0.45
D2	2.35	2.40	2.45
E2	1.65	1.7	1.75
K	0.20	-	-

Appendix B. Application Note

(A) DC Characteristics Related:

The reference data of IDD during Command execution.

Parameter	Symbol	Min	Typ.	Max.	Unit
Supply Current in Operation Mode (Waiting for Command)	I_{DD_N1}		3.7		mA
Supply Current in Operation Mode (During non-ECC Command Execution)	I_{DD_N2}		4.3		mA
Supply Current in Operation Mode (During ECC Command Execution)	I_{DD_N3}		7		mA

No. : TDDS01-S7131-EN(B)	Name : SQ7131/SQ7133 Brief Datasheet	Version : V1.3
--------------------------	--------------------------------------	----------------

Revision History

Version	Issued Data	Description
V1.3	2023/12/28	1. Sync with datasheet V1.3 full version 2. Add PRODUCT number : SQ7131SP008C00R, SQ7131N3008C00R, SQ7133SP008S00R, SQ7133N3008S00R 3. Modify Supply Current in Operation MODE(During ECC Command Execution) in Appendix B to 7mA
V1.0	2023/1/18	1 st version issue