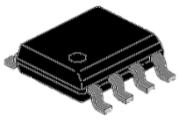
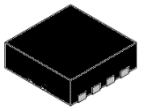
SQ7131/SQ7133
Brief Datasheet V1.0

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

Package Type



SOP8



8Lead-DFN(3x3)

- 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)
- Security Features
  - H/W Accelerator for Asymmetric Sign, Verify, Key Agreement
    - NIST Standard P256 /P384 Elliptic Curve Support
    - ECDSA: FIPS186-4 Curve Digital Signature
    - ECDH: FIPS SP800-56A Key Agreement
  - 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)
  - NIST CAVP Certification
- 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
  - AIoT Device Security
  - Secure Boot/ Secure OTA
  - Accessory Authentication
  - End-to-End Encryption
  - Anti-cloning

Content

1.Preface

SQ7131/SQ7133 is Asymmetric Secure Element, embedded high quality TRNG(True Random Number Generator), Hardware Asymmetric Cryptography ECC384/ECC-256, Hardware Symmetric Cryptography AES-128/AES-256, and SHA-256. The high level secure storage can support ECC and AES keys and compressed Certificate(as below table) The device supports IoT Symmetric/Asymmetric authentication, attestation,and TLS1.2 and 1.3 secure connection. The device is suitable for Secure Boot, Secure OTA,F/W protection .. etc high security applications.

Features	SQ7131/SQ7133	Note
Slot	52	
ECC Private Key – 256	7	Slot 1~7
ECC Public Key – 256	4	Slot 24,26,27,28
ECC Private Key – 384	2	Slot 20,21
ECC Public Key – 384	4	Slot 30,32,33,34
ECC Compressed Certificate	2	
AES Key (AES-128/256)	12	Slot 8~19
I/O Protection Key	1	Slot 22
Data	32x6	Slot 36~41
Data	512 x11	Slot 42~52

TABLE 1-1 MEMORY SUMMARY

2. Pin Assignment/ Description

2.1 SQ7131 Pin Assignment/ Description

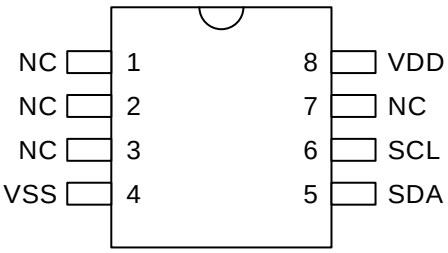


FIGURE 2-1 PIN ASSIGNMENT OF SQ7131 SOP8

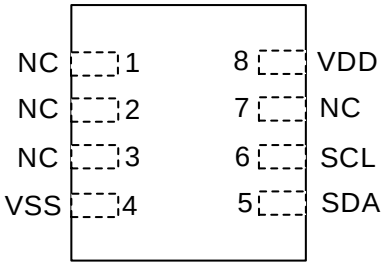


FIGURE 2-2 PIN ASSIGNMENT OF SQ7131 8-LEAD DFN

Pin No.	Pin Name	I/O Type	Function Decription
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

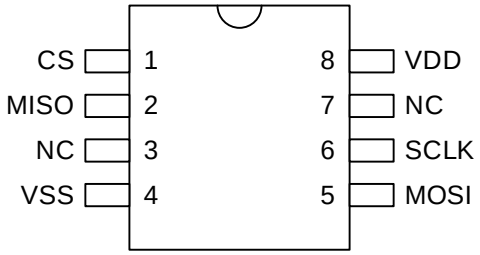


FIGURE 2-3 PIN ASSIGNMENT OF SQ7133 SOP8

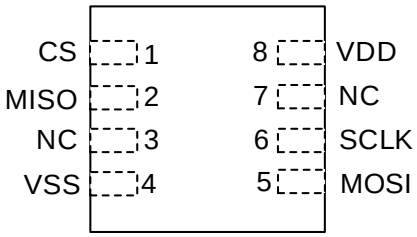


FIGURE 2-4 PIN ASSIGNMENT OF SQ7133 8-LEAD DFN

Pin No.	Pin Name	I/O Type	Function Decription
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. Electonic 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 VDD+0.3V	V
Output Current (total)	I_{OL}	All I/O pins	50	mA
Storage Temperature	T_{STG}		-50 to 125	℃

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	Min	Typ.	Max.	Unit
Supply Voltage	V_{DD}	2.0	3.3	5.5	V
Operating Temperature	Ta	-40	25	85	℃

3.2.2 I/O Characteristics

Parameter	Symbol	Min	Typ.	Max.	Unit
Input Low Voltage	V_{IL}	0		0.3 VDD	V
Input High Voltage	V_{IH}	0.7 VDD		VDD	V
Output Low Voltage	V_{OL}	0		0.1VDD	V
Output High Voltage	V_{OH}	0.9VDD		VDD	V

3.3 DC Characteristics

Parameter	Symbol	Min	Typ.	Max.	Unit
Supply Current in Operation Mode (Note)	I_{DD_N1}		3.7		mA
Supply Current in Deep Sleep Mode	I_{DD_DS}		0.8		uA

Note : The condition is waiting for Commands. The IDD when executing the command please refer to Appendix B.

3.4 Power-on Reset Characteristics

Ta=-40~85℃

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 CPU ready	-	4	-	ms
tVDD	Power supply rise time	0.5		5	ms

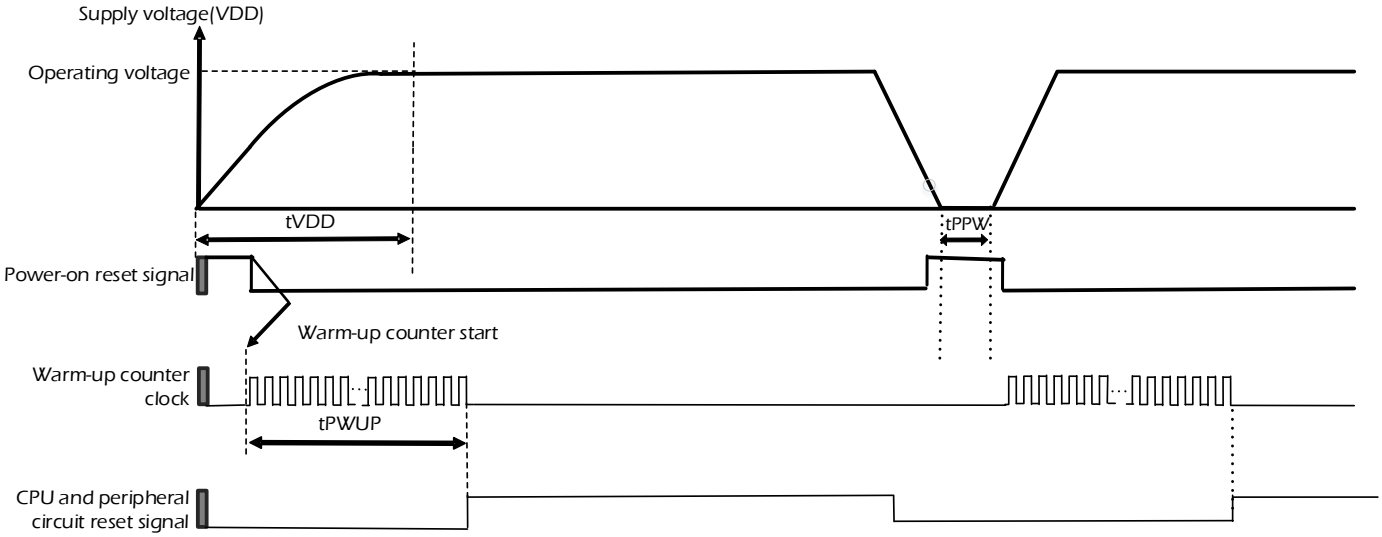


FIGURE 3- 1 OPERATION TIMING OF POWER-ON RESET

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

3.5 BROR Characteristics

Ta=-40~85℃

Parameter	Symbol	Condition	Min	Typ.	Max.	Unit
BROR detect voltage	VBROR_Rising	VDD rise time and fall time > tVDD (tVDD please refer to Ch3.4 Power-on Reset Characteristics)	1.95	2.0	2.05	V
	VBROR_Falling		1.85	1.90	1.95	V

3.6 AC Characteristics

Parameter	Symbol	Condition	Min	Typ.	Max.	Unit
Power-Up Delay(Note3)	T_{PU}	Min. time between VSS > VSS minprioro to start of TWLO	100	-	-	us
Wake Low Duration	T_{WLO}	-	60	-	-	us
Wake High Delay to Data Comm	T_{WHI}	SDA should be stable high for this entire duration unless polling is implemented. SelfTest is not enabled at power-up.	1500	-	-	us
Wake High Delay when SelfTest is Enabled	T_{WHIST}	SDA should be stable high for this entire duration unless polling is implemented.	20	-	-	ms
Watchdog Timeout	$T_{WATCHDOG}$	Time from wake untill device is forced into Sleep mode if Config.ChipMode{2} is 0.	0.7	1.3	1.7	us

Note 1 : Writer cycle time is include data update.

Note 2 : These parameters are characterized, but not production tested..

Note 3 :" Direction -" To crypto Authentication"

Note 4 : The power-up delay will be significantly longer if power-on self test is enabled in the Configuration zone.

3.6.1 AC Parameters

Parameter	Symbol	Min	Typ.	Max.	Unit
Power-Up Ready Time	T_{PU_RDY}		1200	1500	uS
Standby Time, Entering the deep sleep mode	T_{STB}		55	90	uS
Wake-Up Ready Time, deep sleep mode	Tw_{DS_RDY}		300	-	uS

3.6.2 I2C Charasteristics

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
Note: Guaranteed by characteristic, not tested in production.				

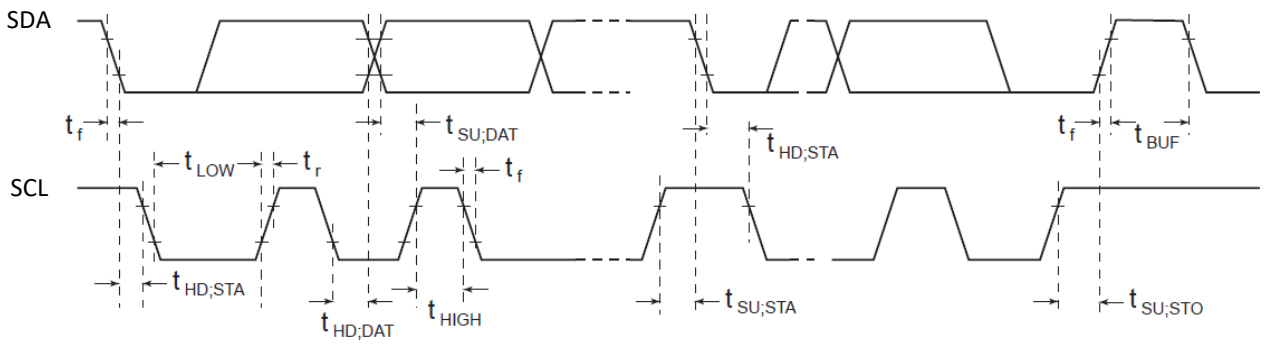


FIGURE 3-2 I2C TIMING SEQUENCE

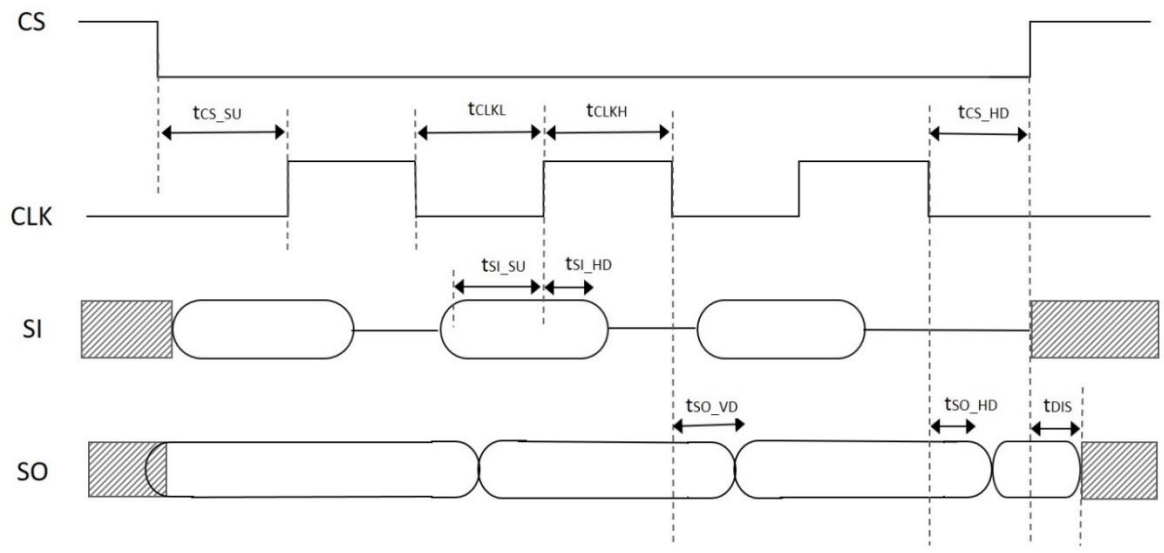
3.6.3 SPI Characteristics

(VDD=2.7V~5.5V)

Parameter	Symbol	Min	Max.	Unit
SPI Frequency	f_{SPI}		10	MHz
SPI Period	t_{SPI}	100		ns
High period of the SCLK pin	t_{CLKH}	40		ns
Low period of the SCLK pin	t_{CLKL}	40		ns
From SPICS active to first edge	t_{CS_SU}	20		ns
From last SCLK edge to SPICS inactive	t_{CS_HD}	20		ns
Time between SPI transaction	t_{CS_WA}	(1)		us
Data Input Setup Time	t_{SI_SU}	5		ns
Data Input Hold time	t_{SI_HD}	5		ns
Data Output Valid Time	t_{SO_VD}		20	ns
Data Output Hold Time	t_{SO_HD}	0		ns
Data Output Disable Time	t_{SO_DIS}		20	ns

(VDD=2.0V~2.7V)

Parameter	Symbol	Min	Max.	Unit
SPI Frequency	f_{SPI}		5	MHz
SPI Period	t_{SPI}	200		ns
High period of the SCLK pin	t_{CLKH}	80		ns
Low period of the SCLK pin	t_{CLKL}	80		ns
From SPICS active to first edge	t_{CS_SU}	40		ns
From last SCLK edge to SPICS inactive	t_{CS_HD}	40		ns
Time between SPI transaction	t_{CS_WA}	(2)		us
Data Input Setup Time	t_{SI_SU}	10		ns
Data Input Hold time	t_{SI_HD}	10		ns
Data Output Valid Time	t_{SO_VD}		40	ns
Data Output Hold Time	t_{SO_HD}	0		ns
Data Output Disable Time	t_{SO_DIS}		40	ns



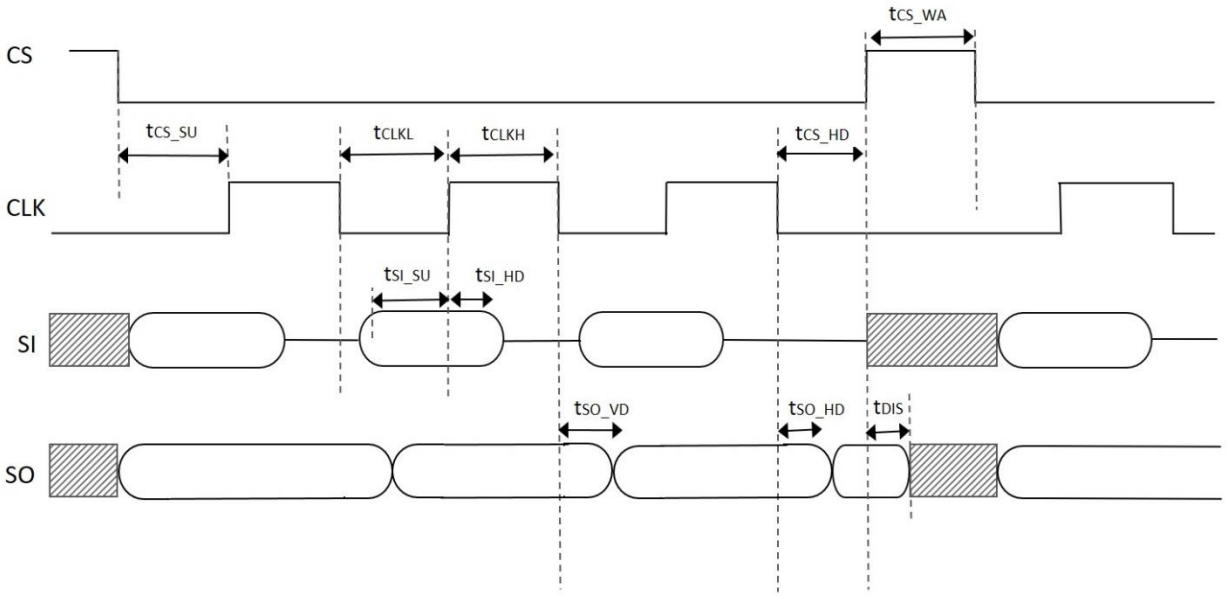


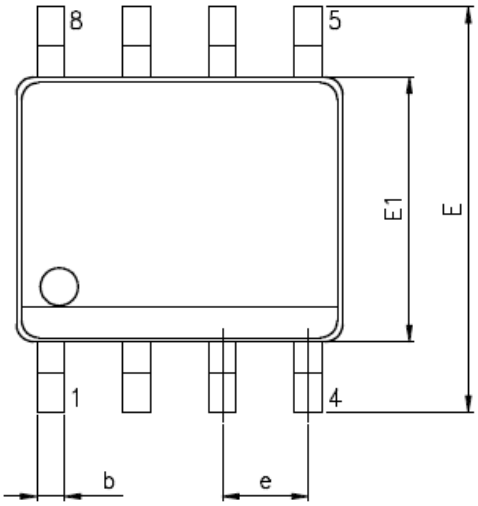
FIGURE 3-3 SPI TIMING SEQUENCE

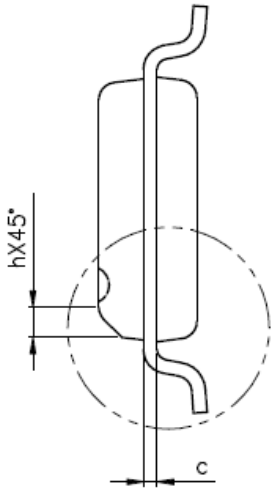
3.7 EEPROM Characteristics

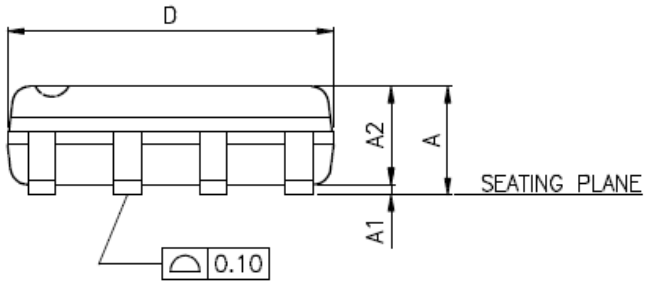
Parameter	Symbol	Min	Max.	Unit
Write Endurance (Sector Endurance)	100,000	-	-	Cycles
Data Retention(at 25°C)	100	-	-	Years
Data Retention(at 85°C)	20	-	-	Years

Appendix A. Pacakge Information

SOP8

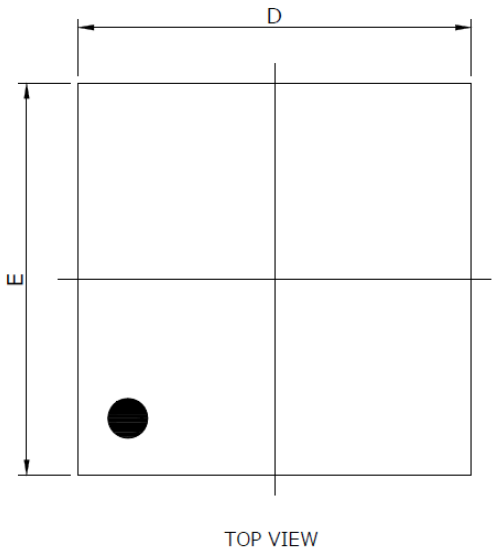




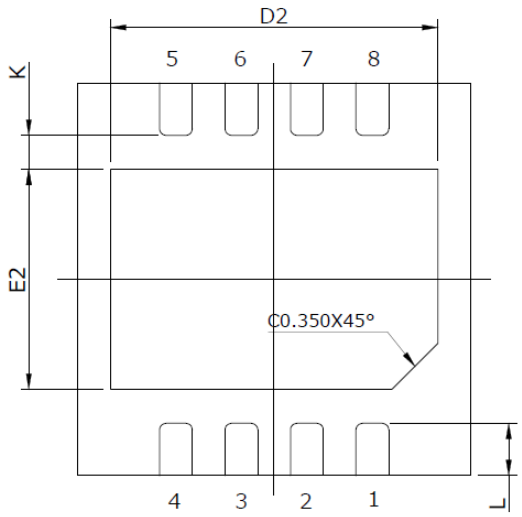


Symbol	mm		
	Min		Max
A	–	–	1.75
A1	0.10	–	0.25
A2	1.25	–	–
b	0.31	–	0.51
c	0.10	–	0.25
D	4.90 BSC		
E	6.00 BSC		
E1	3.90 BSC		
e	1.27 BSC		
L	0.40	–	1.27
L1	1.00 REF		
h	0.25	–	0.50
θ	0°	–	8°

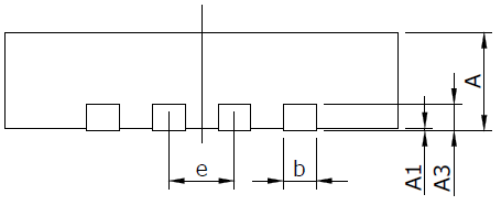
8-Lead DFN (3x3)



TOP VIEW



BOTTOM VIEW



Symbol	mm		
	Min		Min
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	2.45	2.50	2.55
E2	1.63	1.68	1.73
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}		9.2		mA

Revision History

Version	Approved Data	Description
V1.0	2023/1/18	1st version issue