KEROS®

KEROS

AES256 CODEC

『 Cipher Memory 2KB 』

Data Sheet Version 1.11

ChipsBrain Global, All right reserved.

CHIPSBRAIN GLOBAL

Table of Contents

CHIPSBRAIN GLOBAL

Revision History

Doc. Rev.	Date	Comments
KEROS_v1.11	2017/11/07	Document update
KEROS_v1.10	2017/03/16	Document update
KEROS_v1.00	2016/12/06	Document update.
KEROS_v0.30	2016/05/10	Change the Application Circuit of 8SOP
KEROS_v0.20	2015/12/31	China Office Update
KEROS_v0.00	2015/9/10	Initial document release #2
KEROS_B	2015/8/17	Document update.
KEROS_A	2015/7/20	Initial document release.

CHIPSBRAIN GLOBAL

1   Introduction

The KEROS is a family of high performance secure memory device providing 2K Bytes of user memory with advanced built-in AES 256 security engine and cryptographic features. The memory is divided into 8 user zones each of which individually set with different security access right or used together to provide space for one or multiple data files. A configuration zone contains registers to define the AES256 secret keys used by security logic of Chips Brain Global Security IC.

Through dynamic, symmetric mutual authentication, data encryption and the use of data decryption provides a secure place for storage of sensitive information within a system. With its protection circuit, this information remains safely even under attack.

The KEROS also provides high security, low cost and easy implementation of host-client type systems without the needs for a MCU operating system. The embedded AES256 cryptographic engine provides for a dynamic, symmetric mutual authentication between the device and host, as well as performs encryption for all data and passwords exchanged between the device and host. The AES256 unique key set may be used for these operations.

The simplified host library providing to customers and customers can access easily to deal with the KEROS
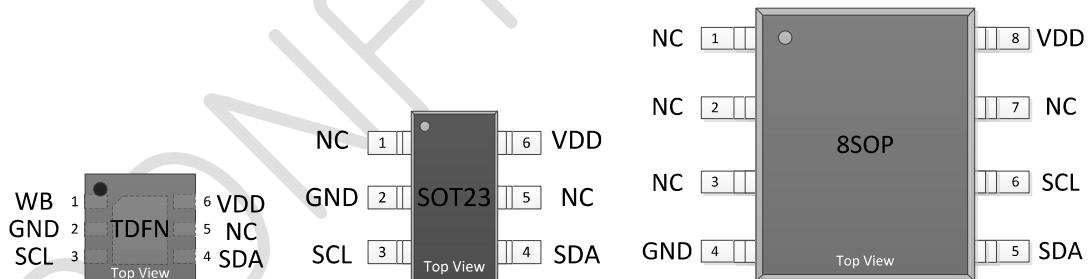
Figure [1.1] available package of KEROS (Top view)

1.1 Features

> High security features

- Symmetric-mutual authentication

- AES128/192/256 bits encryption and decryption engine

- I2C or one-wire protocol with random stream encryption and decryption function

- Unique key set for authentication, encryption and decryption

> 2K Bytes secure EEPROM user memory

15 User Blocks

- Support OTP/MTP user area

> Embedded application features

- Support 5 Bytes serial number

- Support multiple host-client interfaces I2C and One-Wire

- Support increment only counting function for inkjet printer and cartridge

- Wide input power range : 1.8V ~ 3.6V

- SOT23-6, 8SOP and TDFN-6 packages

1.2 Application

I2C interface running at 400KHz is used for fast and efficient communications with up to 127 devices that may be individually addressed. The KEROS is available in industry standard 8-lead or 6-lead packages with the same familiar pin layout as 2-wire serial EEPROM's supporting only the synchronous communication protocol.

CHIPSBRAIN GLOBAL

## 2 Pin Information

2.1 Application Circuit
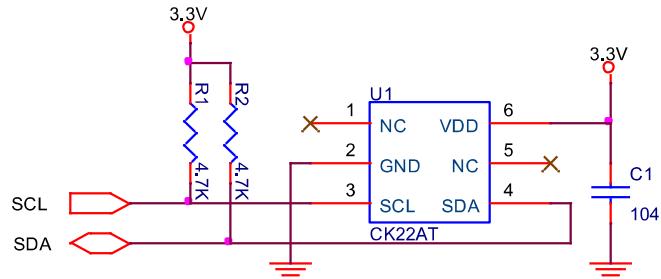

Figure [2.1.1] SOT23-6 Package
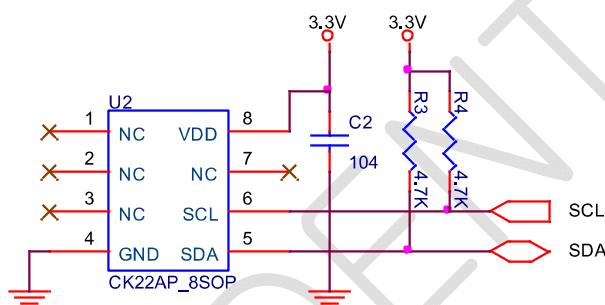
Figure [2.1.2] 8SOP Package
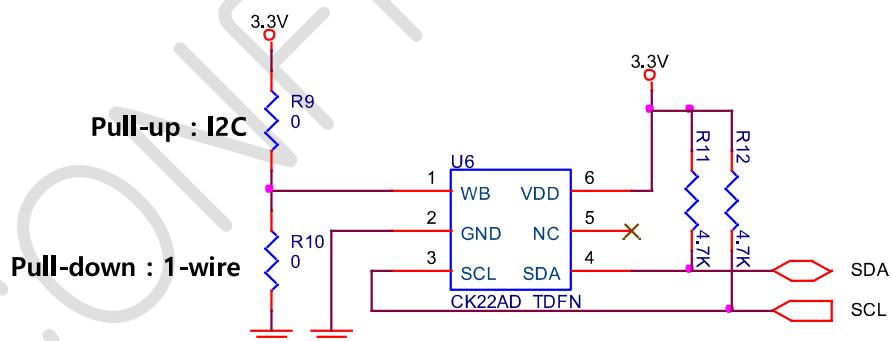
Figure [2.1.3] TDFN-6 Package

CHIPSBRAIN GLOBAL

2.2 Pin configuration(SOT23-6)

Pin number	Pin name	Direction	Description
1	NC	-	Not Connect
2	GND	-	Ground
3	SCL	I	Serial Clock
4	SDA	I/O	Serial Data
5	NC	-	Not Connect
6	VCC	-	Power Supply

Table [2.1] SOT23-6 Pin description

2.3 Pin configuration (8SOP)

Pin number	Pin name	Direction	Description
1	NC	-	Not Connect
2	NC	-	Not Connect
3	NC	-	Not Connect
4	GND	-	Ground
5	SDA	I/O	Serial Data
6	SCL	I	Serial Clock
7	NC	-	Not Connect
8	VCC	-	Power Supply

Table [2.2] 8SOP Pin description

2.4 Pin configuration (TDFN-6)

Pin number	Pin name	Direction	Description
1	WB	I	Communication Mode Selection High : I2C Low : One-Wire
2	GND	-	Ground
3	SCL	I	Serial Clock
4	SDA	I/O	Serial Data
5	NC	-	Not Connect
6	VCC	-	Power Supply

Table [2.3] TDFN-6 Pin description

CHIPSBRAIN GLOBAL

2.5 Pin description

2.5.1 Supply Voltage (VCC)

The VCC input is 1.8V to 3.6V positive voltage supplied by host

2.5.2 SCL

The SCL input used to clock data on the positive clock edge and clock data out on the negative clock edge.

2.5.3 SDA

The SDA pin is bi-directional for serial data transfer. This pin is open drain driven and may be wired with any number of other open drain and open collector devices. An external pull up resister should be connected SDA and VCC, a normal value of 4.7K Ohm may be used. The value of this resister and the system capacitance loading the SDA bus will determine the rise time of SDA. This rise time will determine the maximum frequency during read operations. Low value pull up resisters will allow higher frequency operations while drawing higher average power supply current.

2.5.4 WB

The WB input pin is used for select of interface I2C and One-Wire. If WB pin connected to high(VCC), it select I2C interface. If WB pin connected to low(GND), it select One-Wire interface.
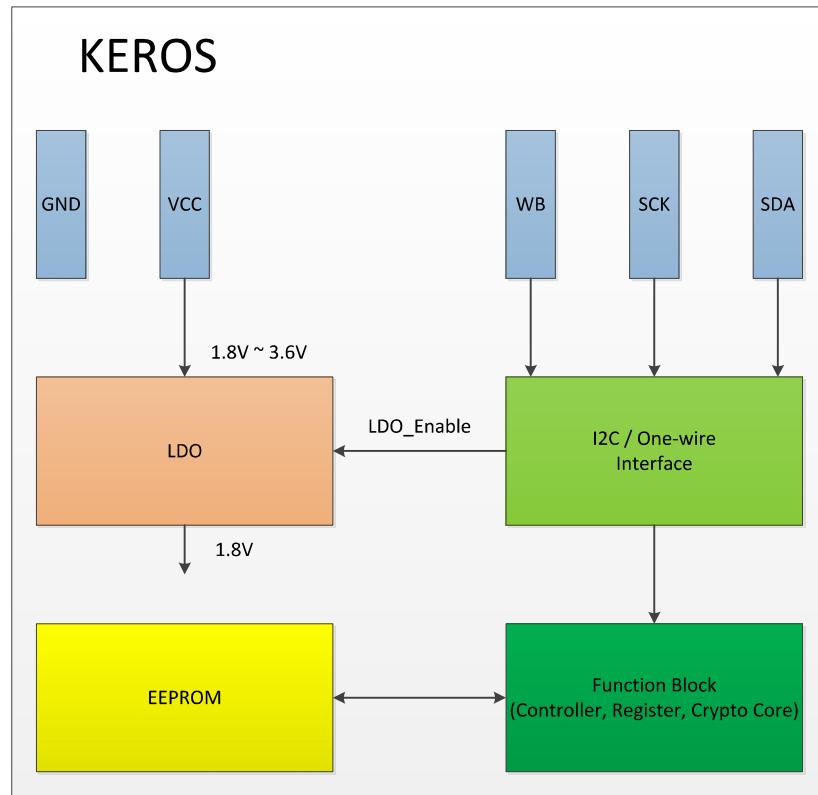
Figure [3.1] Block Diagram

4 Operation

4.1 Initial : Boot sequence and access wait time
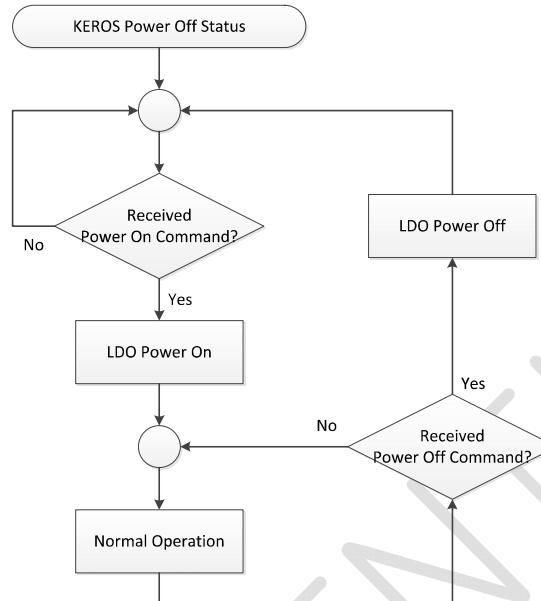
Figure [4.1] Boot sequence flow

The wait time for LDO Power On is about 100us.

4.2 Authentication
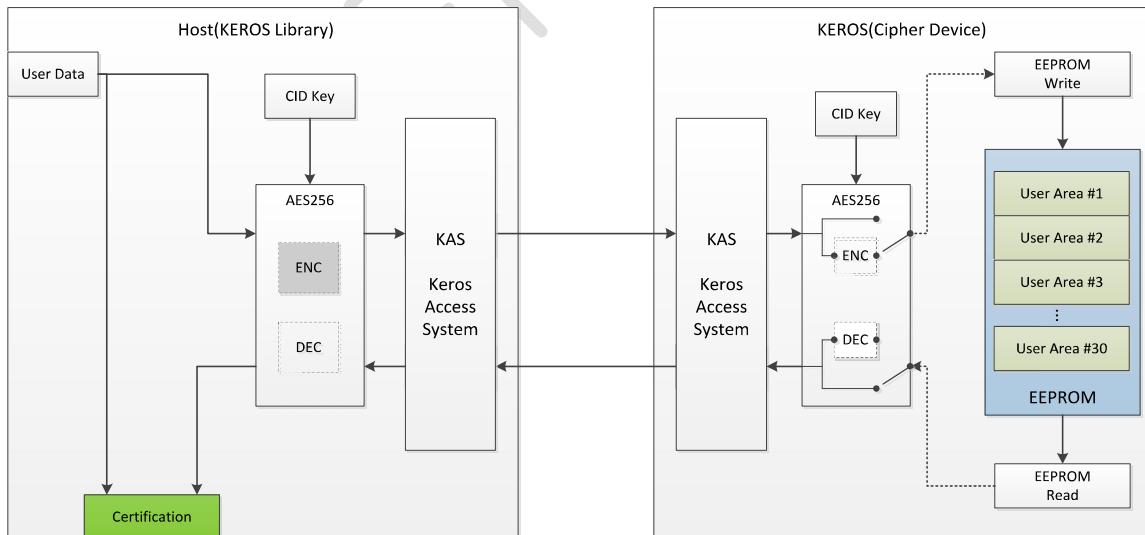
Figure [4.2] Authentication flow

This sequence determines whether the authentication is successful by checking cryptogram which generated by the host and KEROS. If the authentication process of the host is not successful, the authentication of KEROS was failed.

5 Communication Protocol

5.1 Power On Command I2C bus and one-wire type

5.1.1 Write packet

S	Dev Addr								Data	P
	0	0	1	1	1	0	0	0	(1Bytes)	

5.2 Normal Command I2C bus and one-wire type

5.2.1 Write packet

| S	Dev Addr								Sub Addr	Data	P
	0	0	1	1	1	0	0	0	(2Bytes)	(nBytes)	

5.2.2 Read packet

S	Dev Addr								Sub Addr	Sr	Dev Addr								Data	P
	0	0	1	1	1	0	0	0	(2Bytes)		0	0	1	1	1	0	0	1	(nBytes)	

CHIPSBRAIN GLOBAL

6 Memory Map

Block		Description	Access
Block15	Page30	Block 15 OTP/MTP Data Area (EEPROM Memory)	Read/Write
	Page29		
		<omitted...>	
Block1	Page02	Block 1 OTP/MTP Data Area (EEPROM Memory)	
	Page01		

Table [6.1] memory map

7 Ordering Part Number

CKABCD-XXXX

CID : 0000 ~ FFFF

Package Type
 D : TDFN
 P : 8 SOP
 T : SOT23-6

Encryption Algorithm
 A : AES

Comm. Interface
 1 : 1-wire
 2 : I2C

EEPROM Capacitance
 2 : 2K Bytes

Keros (Kerberos)

Chipsbrain Global
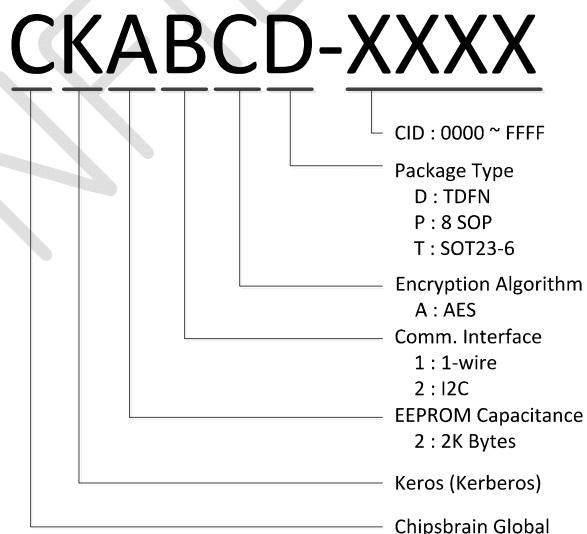
Figure [7.1] Ordering Part Number

CHIPSBRAIN GLOBAL

8 DC and AC Characteristics

8.1 DC Electrical Characteristics

Parameter	Symbol	Condition	Min	Typ	Max	Unit
Operation Voltage	VCC	Power supply	1.8	3.3	3.6	V
	VDD	Core Power supply(only output)	1.65	1.8	1.95	V
Input Low Voltage	V$_{IL}$	All input pins	GND-0.3	-	0.3	V
Input High Voltage	V$_{IH}$	All input pins	VCC-0.3	-	VCC+0.3	
Output High Voltage	V$_{OH}$	VCC=3.3V I$_{OH}$=100uA	VCC-0.3	-	-	
Output Low Voltage	V$_{OL}$	VDD=3.3V I$_{OL}$=4mA	-	-	0.4V	
Output Low Current	I$_{OL}$	V$_{OL}$= 0.4V	-	-	4	mA
Active Power Supply Current	I$_{CC}$	Normal operation mode VCC=3.3V	-	1.3	3	mA
Sleep Current	I$_{SLEEP}$	VCC=3.3V		-	1	uA

Table [8.1] DC electrical characteristics

LDO (Ta=25℃, Vcc=3.3V) Characteristics

Parameter	Condition	Min	Typ	Max	Unit	Note
Operating Voltage		1.8	3.3	3.6	V	
Regulation Output Voltage	VCC=2.0~3.6V	1.65	1.8	1.95	V	
Current Drivability	VCC=1.5V	-	-	20	mA	

Table [8.2] LDO characteristics

EEPROM Reliability

Parameter	Min	Typ	Max	Unit
Write Endurance	10,000	-	-	Write Cycles
Data Retention	10	-	-	Years
	Unlimited			Read Cycles

Table [8.3] EEPROM reliability

Absolute Maximum Ratings

Parameter	Symbol	Condition	Rating	Unit
Supply voltage	Vdd	-	-0.3 to +3.6	V
Input voltage	Vi	All ports	-0.3 to Vdd+0.3	V
Output voltage	Vo	All output ports	-0.3 to Vdd+0.3	V
Output Current High	Ioh	One I/O pin active	-200	uA
Output Current Low	Iol	One I/O pin active	10	mA
Operating temperature	Ta	-	-20 to +85	°C
Storage temperature	Ts	-	-65 to +150	°C
Junction temperature	Tj		150	°C

Table [8.4] absolute maximum ratings

CHIPSBRAIN
GLOBAL

8.2 AC Parameters

8.2.1 I2C Interface
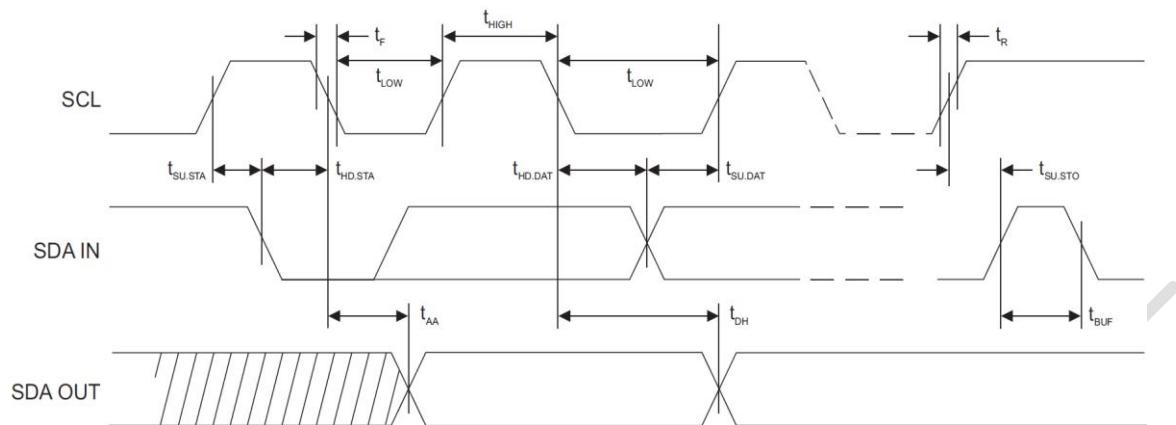
Figure [8.1] I2C interface timing

Symbol	Parameter	Min	Max	Units
f_{SCK}	SCK Clock Frequency	-	400	KHz
	SCK Clock Duty Cycle	40	60	%
t_{HIGH}	SCK High Time	1	-	us
t_{LOW}	SCK Low Time	800	-	ns
$t_{SU.STA}$	Start Setup Time	500	-	ns
$t_{HD.STA}$	Start Hold Time	500	-	ns
$t_{SU.STO}$	Stop Setup Time	500	-	ns
$t_{SU.DAT}$	Data in Setup Time	100	-	us
$t_{HD.DAT}$	Data in Hold Time	0	-	ns
t_R	Input rise time	-	300	ns
t_F	Input Fall Time	-	100	ns
t_{AA}	Clock Low to Data Out Valid	100	700	ns
t_{DH}	Data Out Hold	100	-	ns
t_{BUF}	Time bus must be free before a new transmission can start	1	-	us

Table [8.5] I2C interface parameter

CHIPSBRAIN GLOBAL

8.2.2　One-wire interface
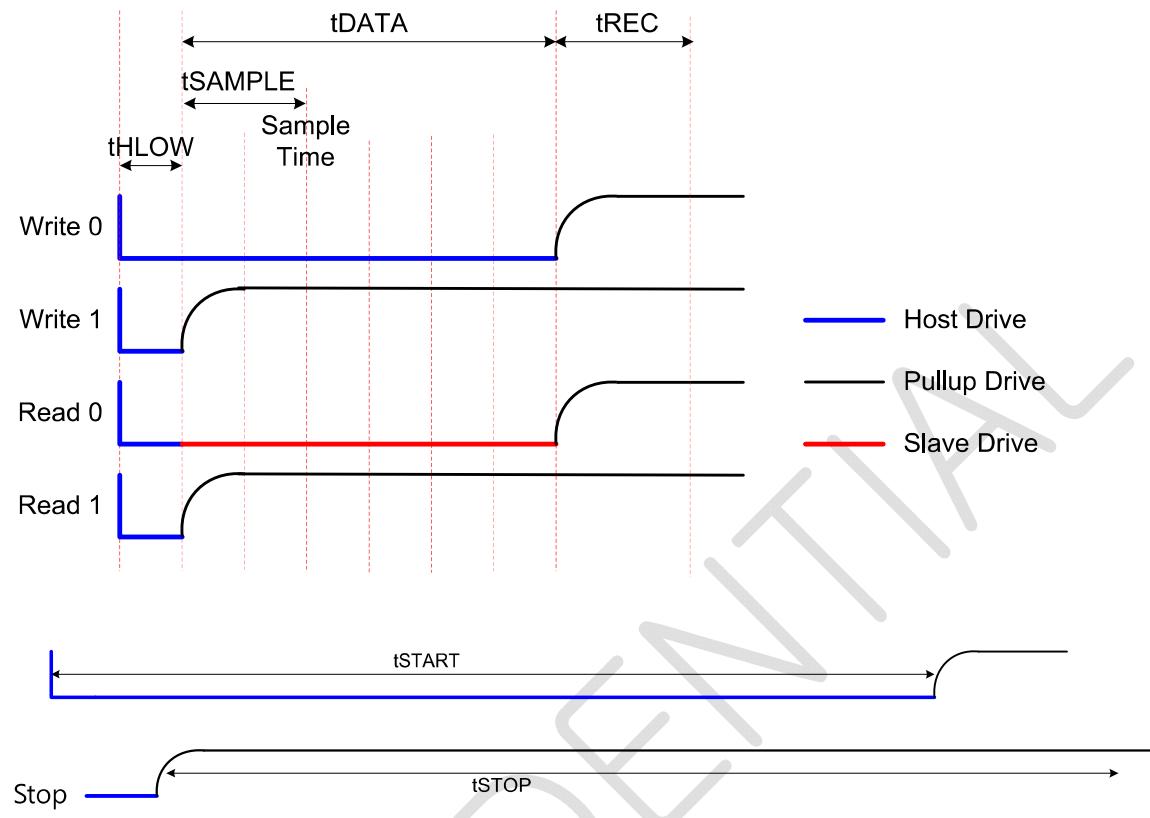
Figure [8.2] one-wire interface timing

Symbol	Parameter	Min	Typ	Max	Units
tHLOW	Start Pulse Duration	4.5	5	5.5	us
tDATA	Data Period	29	30	31	us
tREC	Recovery time for next data	9	10	15	us
tSAMPLE	Data Sampling Time for data read	9	10	11	us
tSTART	Single Wire Start (1)	100	-	1000	us
tSTOP	Single Wire Stop (2)	100	-	-	us

(Note)　1. If tSTART is over 100us, Single Wire communication will start.
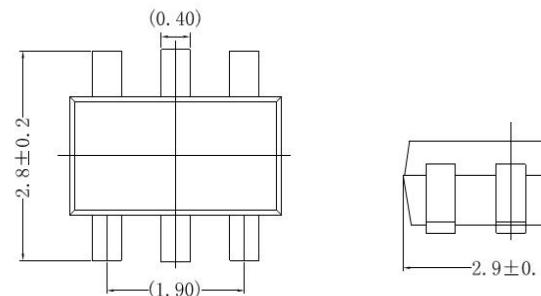
If tSTART is more than Max. 1ms, then Single Wire communication will restart

2. If tSTOP is over 100us, Single Wire communication will be stopped

Table [8.6] one-wire interface parameter

9   Package Dimension

SOT23-6

Note
1. All dimensions are in mm
2. Dimensions marked with a parenthesis are reference dimensions
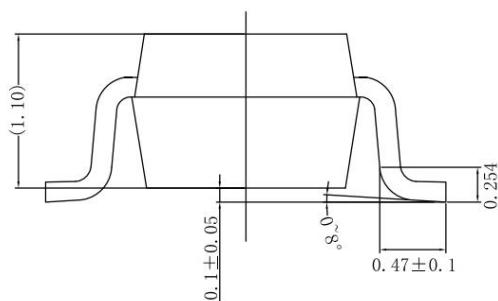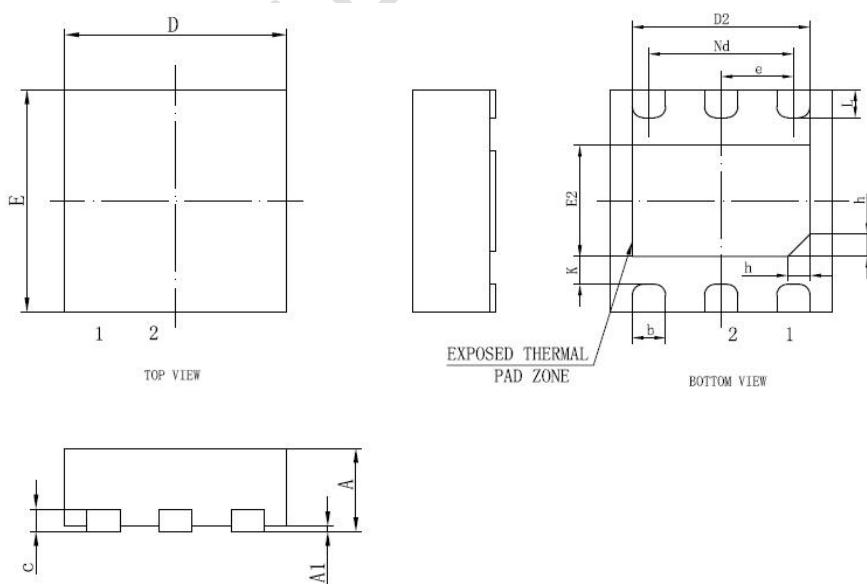
Figure [9.1] package dimension (SOT23-6)

DFN
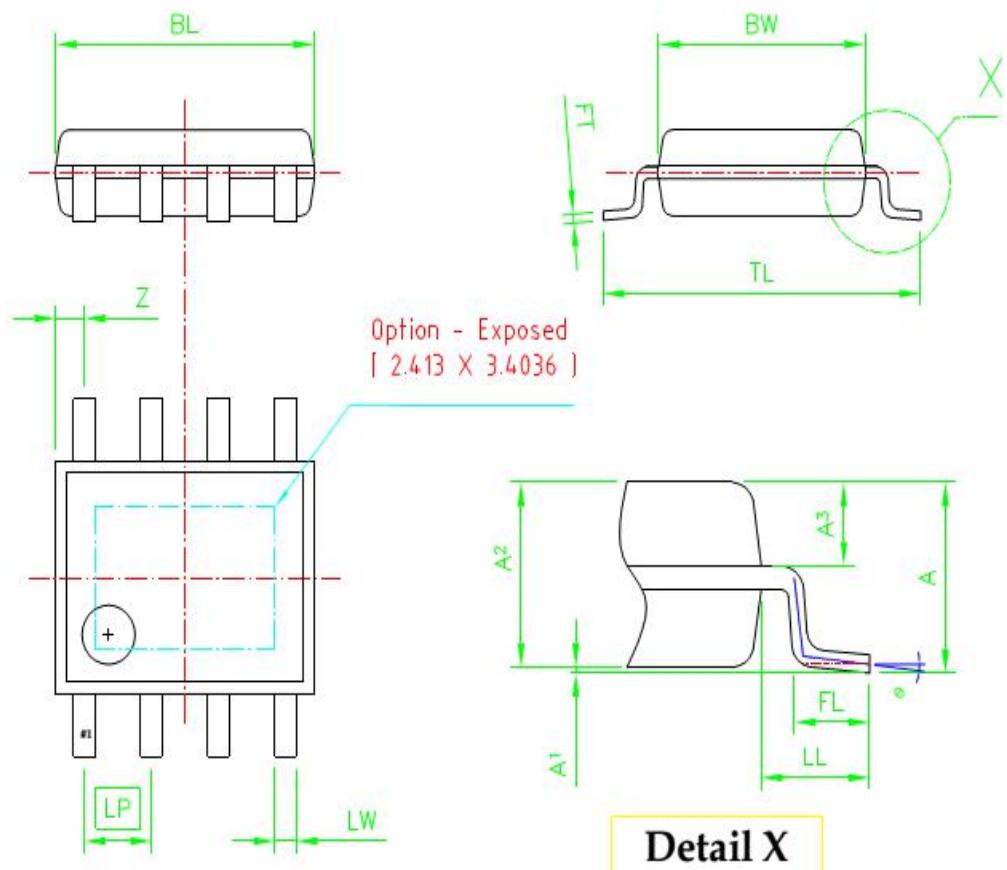
SYMBOL	MILLIMETER		
	MIN	NOM	MAX
A	0.70	0.75	0.80
A1	0	0.02	0.05
b	0.25	0.30	0.35
c	0.18	0.20	0.25
D	1.90	2.00	2.10
D2	1.50	1.60	1.70
e	0.65BSC		
Nd	1.30BSC		
E	1.90	2.00	2.10
E2	0.90	1.00	1.10
K	0.20	–	–
L	0.20	0.25	0.30
h	0.15	0.20	0.25
L/F載体尺寸(MIL)	69X47		

Figure [9.2] package dimension (DFN6L)

8SOP

Option - Exposed
[2.413 X 3.4036]

Detail X

Dimensions

Unit	BL	BW	FT	TL	LP	LW	A max.	A1	A2	A3	LL	FL	θ	Z
mm	5.10 4.70	4.10 3.70	0.210 0.196	6.20 5.80	1.27 BSC	0.432 0.381	1.75	0.05 0.25	1.45 BSC	0.623 BSC	1.05 BSC	0.80 0.50	8 0	0.55

Figure [9.3] package dimension (8SOP)

CHIPSBRAIN GLOBAL