Encryption chip

1 Chip features

1.1 User area is **EEPROM**

– There are 4 user partitions

– Multiple write modes: single Byte, multiple Byte and Page write modes– Each partition has access rights **1.2** Configuration area **2K-bit**

– can define Byte unique ID – access rights, authentication **user** and

can - 8 , area define Customers seeds read passwords key writeEncryption has 4 sets of key seeds – Rolling encryption

1.4 Application characteristics

– Voltage range:2.7V-5.5V

– Using 2 wire non-standard I2C interface – Communication frequency up to 1.0 MHz

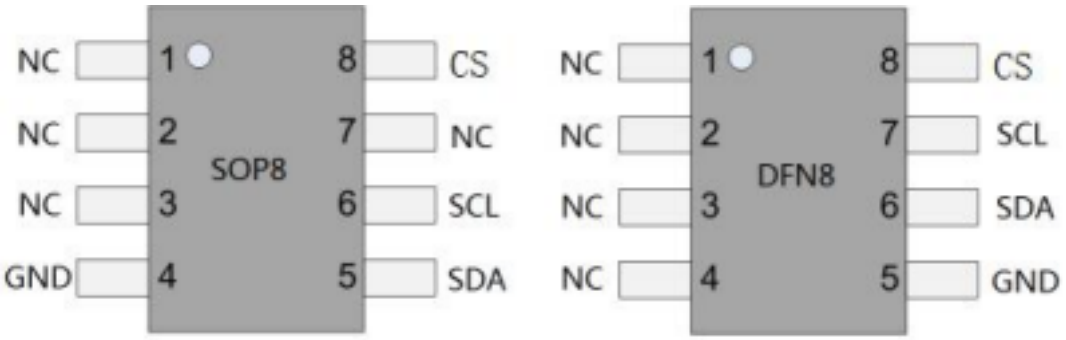
– Standard SOP8 package

1.5 High reliability

– Writeoperations 10 100,000

– data retention up to 2 years

- chip package and pin definitions



The pin definitions are as follows:

Pad	Descri
CS	Contr
GND	Grou
SCL	Seri

SDA	Serial Data Input/Output

3 Configuration Zone Introduction

	$0				
$00	Reserved				
$08		Code I			
$10					
$18		DCR Reser			
$20					
$28					
$30					
$38					
$40					

$48			
$50		AAC0 Ci0	
$58	SK0		
$60		AAC1 Ci1	
$68	SK1		
$70		AAC2 Ci2	
$78	SK2		
$80		AAC3 Ci3	
$88	SK3		
$90			
$98			
$A0			
$A8			
$B0		PAC Write0	
$B8		PAC Write1	
$C0		PAC Write2	
$C8		PAC Write3	
$D0		PAC Write4	
$D8		PAC Write5	
$E0		PAC Write6	
$E8		PAC Write7	

$F0	Reserved	System
$F8		

3.1 Fab Code

16-bit register, the factory value is:"10 10", the customer cannot modify it.

3.2 MTZ

memory test area has a total of 16-bit, which is defined for testing communication, and has permission to read and write MTZ at any time.

3.3 ID Code

can define an 8-Byte unique ID, which can only be read and cannot be modified after leaving the factory.

3.4 **DCR**

Bit7		Bit6	Bit5	Bit4	Bit3	Bit2	Bit1
		UAT		ETA	CS3	CS2	CS1

Bit0

CS0

UAT: If enabled (UAT="0"), it allows numerous false authentications, andAAC invalid.ETA: If enabled (EAT="0"), there are 8 chances of wrong authentication or verification. IfEAT="1",AACand PAC have only 4 chances of error. CS0-CS3: The chip can respond to the default chip select address$B(1011), and can alsoCS0-CS3 correspond to the address value

3.5 Access Register **AR**

Bit7		Bit6	Bit5	Bit4	Bit3	Bit2	Bit1
PM1		PM0	AM1	AM0	ER		

Bit0

PM(1:0)Mode

PM1		PM0 Permission
1		1 No password verification
1		0 Password verification required
0		1 Password verification required
0		

		for both reading and writing Check 0

When PM="11", no password verification is required to access the user area. When PM="10", the write password needs to be verified for writing to the user area, and the read password is not required for reading the user area. When PM="01"or" 00", the read and write user area needs to verify the write password, and the read-only user

area needs to verify the read password.

AM(1:0)mode

		authentication
0		1

AM1		AM0 Permission
1		1 No authentication required
1		0 Writing requires authentication
1		0 Both reading and writing require

When AM="11", no authentication is required to access the user area. When AM="10", authentication is required for writing to the user area, but not for reading the user area.

When AM="01", authentication is required for both reading and writing the user area. ER-encryption required

When ER="0", if the user area is to be read and written correctly, the host needs to enable encryption mode.

When ER="1", the host can start the encryption mode, if not, it can also access the user area, but the communication is not encrypted.

3.6 Password register **PR**

Bit7		Bit6	Bit5	Bit4	Bit3	Bit2	Bit1
AK1		AK0			PW2		PW1

Bit0
PW0

AK(1:0)-Authentication Key, these 2 bits define 4 groups of encryption seeds G0-G3 , this encryption seed is used in the authentication and encryption process.

PW(2:0) -Password setting, these 3 bits define 8 groups of passwords as the password of the user area. 3.7 Security code (**secure code**) The security code corresponds to the , and the configuration area can be modified only after the **is** security **code**

password verified write7 correctly. 3.9 **G0-G3**

encryption authentication seed should be the same as the software authentication seed. 3.10 **Passwords**

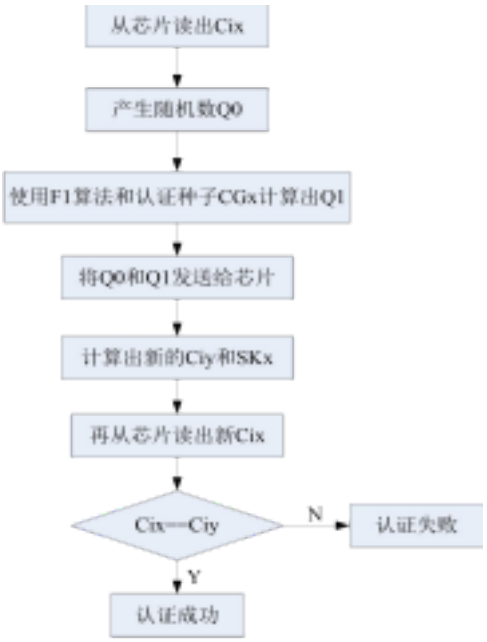
The password can be used to protect the reading and writing of the user area. There are 8 groups of passwords, and one can be selected through thePR register to protect the corresponding user area. If the write password is verified, both reading and writing are possible, and if only the read password is verified, only reading is allowed.

4 Communication Mode

4.1 Standard Mode

The chip is in standard mode by default, any type of data is not encrypted, and the communication data is plaintext. 4.2 The authentication mode

by accessing the registers AR/PR . In this mode, the password in the configuration area is encrypted. If a command is sent to verify the read and write password, it will be done in cipher text. For the user area, the chip must be successfully authenticated before it can access the user area, and the communication is in clear text. The authentication process is as follows:



4.3 The encryption mode

by accessing the register AR . In this mode, the password in the configuration area and the communication in the user area are encrypted and carried out in the form of cipher text. The encryption mode startup process is based on the authentication mode startup, changing the CGx to the calculated SKx and re-authentication. If the authentication is successful, the encryption mode is started.

5 Fuse

The encryption chip has 4 fuses in total,"fuse byte"gives the status of the fuse,"0"means it has been blown.Bits 4 to 7 are reserved bits

Bit7		Bit6	Bit5	Bit4	Bit3	Bit2	Bit1
				SEC		PER	CMA

Bit0
FAB

In order to lock ID Code B, theSEC has been blown when leaving the factory, and the default ID Code B is all"FF". To blowfuses, you must follow the following order: FAB - lock Fab Code
CMA - lock ID Code A
PER - lock the rest of the configuration area
in this order fuses, it must be wrong. Fuse access permission table is as follows:

	W	Sec	Code Se
User		R	AR

Zone		OPFuse		
		SEC=0	FAB=	
	R	F	Fre	
	W	Sec	Code Forbi	
MTZ	R	Free	Fre	
	W			
ID A	R	Code F	Fre	
	W	Sec	Code Se	
ID B	R	Code F	Fre	
	Forbidden	Forbid	Forbic	
Control R	Free	F	Fre	
	Secure	C	Se	Code
AACx Cix	R	F	Fre	
	W	Sec	Code Se	
SKx	R	Secure	Code Se	
	W			
Secret	R	Secure	Code Se	
	W			PW
PW	R	Secure	Code Se	
	W			PW
PAC	R	F	Fre	

Zones		W			

Description: The chip defaults SEC=0 . If the FAB blown,FAB=0 effect. If CMA blown, CMA=0 effect. IfPER blown, then thePER=0The permission corresponding to

6 The chip adopts **2** -wire non-standard **I2C** communication protocol, and the operation commands are as follows:

Item		INS	P1
W		$E	$00
Re	z	$B	$00
W		$E	$00
Wr		$B4	$01
Send ch		$B4	$02
Se	zc	$B4	$03
Re	z	$B	$00
Rea		$B6	$01
Read ch		$B6	$02
v		$B8	$0X
ve		$B8	$1X
Ver		$BA	$0X
Ve		$BA	$1X

pw

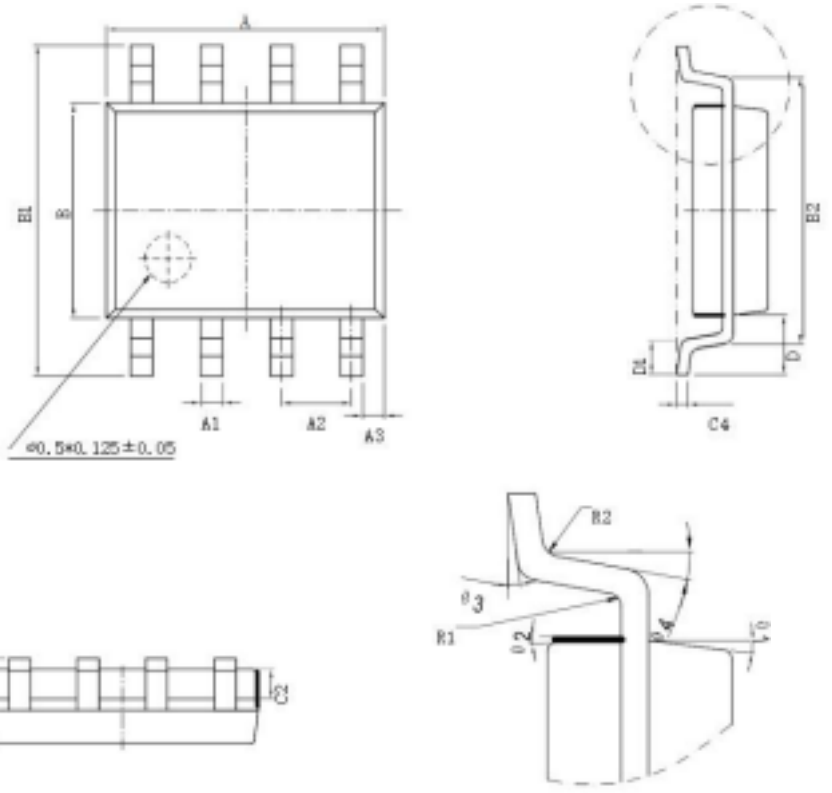
pw

Note:1.After the write operation, a delay of 10ms,verfiy auth and verify Encry a delay20ms.2.,Q0 is 8 bytes bytes a random numberQ1 is F1 calculated by the8 ofdata .3.RW-PW means write password,-PW means read password.

7 Package size

1) SOP8

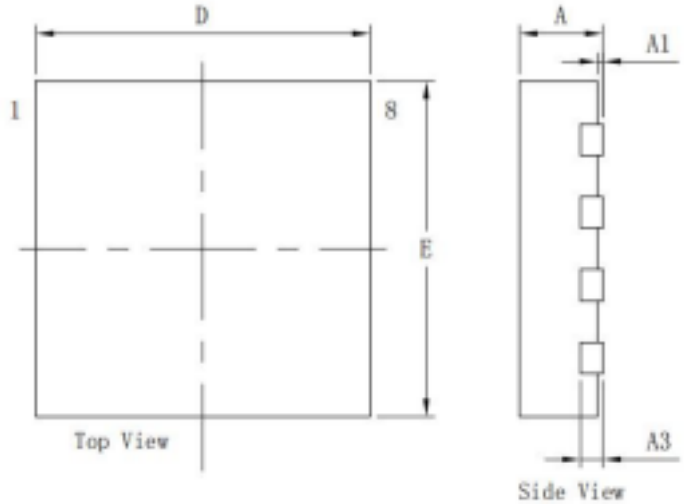
标注 \ 尺寸	最小(mm)	最大(mm)	标注 \ 尺寸	最小(mm)	最大(mm)
A	4.80	5.00	C3	0.05	0.20
A1	0.356	0.456	C4	0.203	0.233
A2	1.27TYP		D	1.05TYP	
A3	0.345TYP		D1	0.40	0.80
B	3.80	4.00	R1	0.20TYP	
B1	5.80	6.20	R2	0.20TYP	
B2	5.00TYP		θ1	17° TYP4	
C	1.30	1.60	θ2	13° TYP4	
C1	0.55	0.65	θ3	0° ~ 8°	
C2	0.55	0.65	θ4	4° ~ 12°	

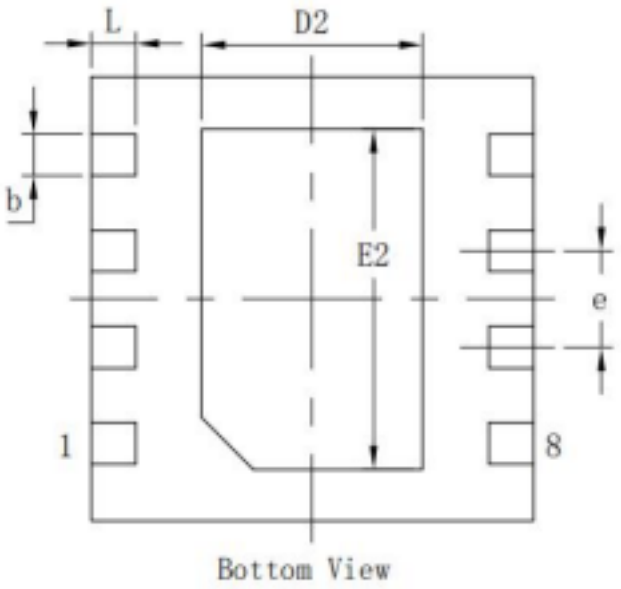


2)

DFN8

标注 \ 尺寸	最小(mm)	标准(mm)	最大(mm)	标注 \ 尺寸	最小(mm)	标准(mm)	最大(mm)
A	0.70	0.75	0.80	E	2.90	3.00	3.10
A1	-	-	0.05	D2	1.40	1.50	1.60
A3	0.203 REF			E2	2.20	2.30	2.40
b	0.23	0.28	0.33	e	0.65 TYP		
D	2.90	3.00	3.10	L	0.25	0.30	0.35




L
D2
b
E2
e
1
8
Bottom View