SHA-256 Battery Authenticator with 34 Bytes User Memory

General Description

The RT9430 battery authenticator uses challenge and response authentication based on SHA-256 (FIPS 180-3) hash algorithm to ensure that the battery pack is certified by the original manufacturer.

The device supports 34 bytes of programmable non-volatile memory for users to access battery information, 4 bytes Device_ID for chip supplier information and system user information, and 8 bytes unique ROM ID for chip identification code. The RT9430 communicates over the single-wire Interface.

Ordering Information

RT9430□-□□□□

- Pin 1 Orientation***
  (2) : Quadrant 2, Follow EIA-481-D
- Key Version Code
- Customer Code
- Package Type
  WTC : TWL-CSP-6B 1.46x1.16 (BSC)

Note :

***Empty means Pin1 orientation is Quadrant 1

Richtek products are :

- ▶ RoHS compliant and compatible with the current requirements of IPC/JEDEC J-STD-020.
- ▶ Suitable for use in SnPb or Pb-free soldering processes.

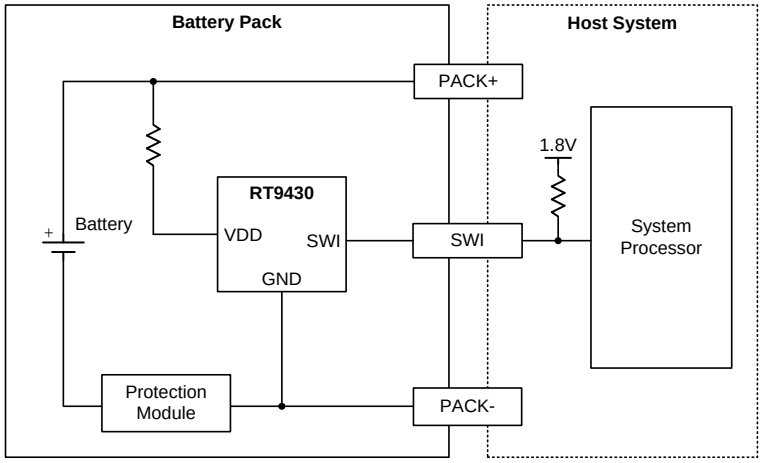
Features

- **SHA-256 FIPS 180-3 Symmetric-Key-Based Secure Authentication Model**
- **34 Bytes of User NVM**
- **32 Bytes of Secret**
- **8 Bytes of ROM_ID**
- **4 Bytes of Device_ID**
- **Support NVM Write and Read Protect**
- **Supports Anonymous Authentication Mode**
- **Single-Wire Interface Bit Rate 50kbps, Supports Normal Mode and Fast Mode**
- **TWL-CSP 1.46x1.16mm Package**

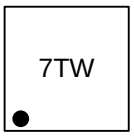
Applications

- Smartphones
- Portable Applications

Simplified Application Circuit



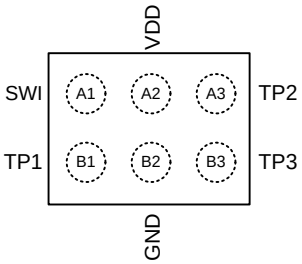
Marking Information



7T : Product Code
W : Date Code

Pin Configuration

(TOP VIEW)

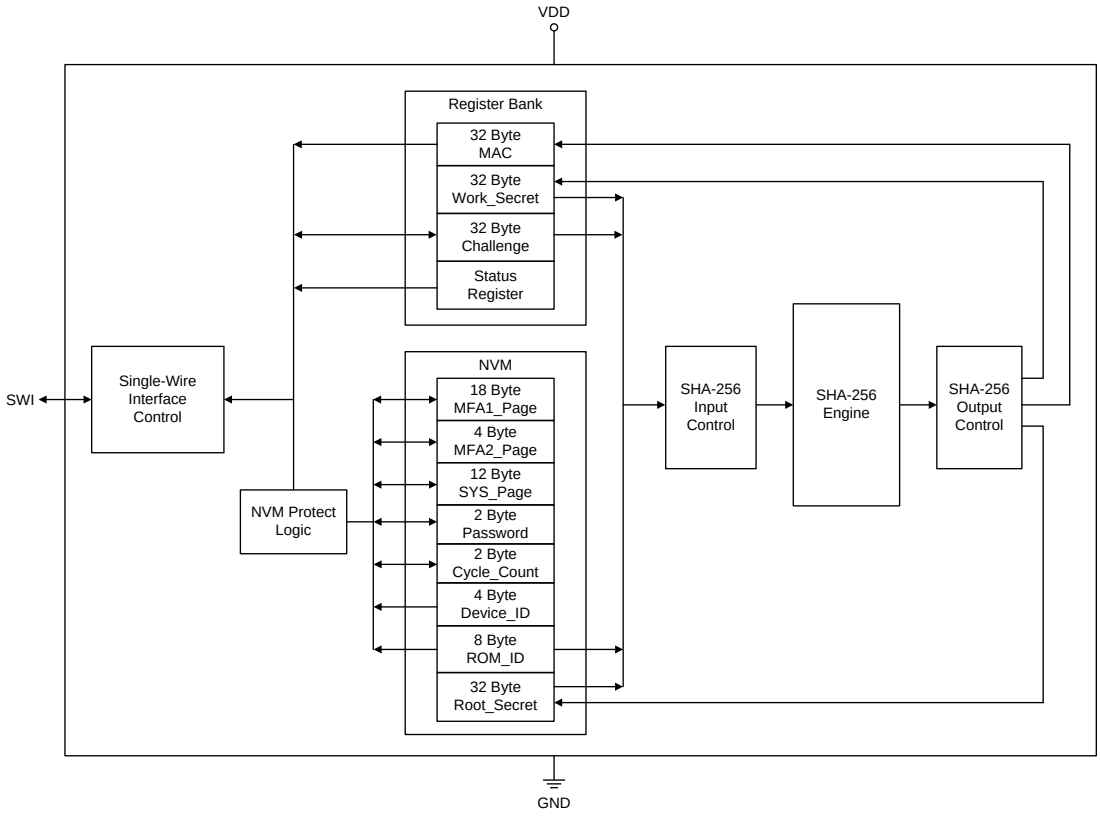


TWL-CSP-6B 1.46x1.16 (BSC)

Functional Pin Description

Pin No.	Pin Name	Pin Function
A1	SWI	Single-wire interface.
A2	VDD	Power supply input.
A3	TP2	Test pin, connect to GND.
B1	TP1	Test pin, connect to SWI.
B2	GND	Device ground.
B3	TP3	Test pin, connect to GND.

Functional Block Diagram



Absolute Maximum Ratings (Note 1)

- Voltage on VDD Pin Relative to GND ---------- –0.3V to 5.5V
- Voltage on SWI Pin Relative to GND ---------- –0.3V to 5.5V
- Power Dissipation, P_D @ T_A = 25°C
  TWL-CSP-6B 1.46x1.16 (BSC) ---------- 2.13W
- Package Thermal Resistance (Note 2)
  TWL-CSP-6B 1.46x1.16 (BSC), θ_{JA} ---------- 46.9°C/W
- Lead Temperature (Soldering, 10 sec.) ---------- 260°C
- Junction Temperature ---------- 150°C
- Storage Temperature Range ---------- –65°C to 150°C
- ESD Susceptibility (Note 3)
  HBM (Human Body Model) ---------- 8kV

Recommended Operating Conditions (Note 4)

- Supply Voltage, VDD ---------- 2.8V to 5.0V
- Ambient Temperature Range ---------- –40°C to 85°C
- Junction Temperature Range ---------- –40°C to 150°C

Electrical Characteristics

(2.8V ≤ V_{DD} ≤ 5.0V, T_A = 25°C, unless otherwise specified)

Parameter	Symbol	Test Conditions	Min	Typ	Max	Unit
Power						
Idle Current	I_{IDLE}	SWI Idle	--	2	5	μA
IO						
SWI Input High	V_{IH}		1.1	--	--	V
SWI Input Low	V_{IL}		--	--	0.4	V
SWI Output Low	V_{OL}	I_{OL} = 5mA	--	--	0.4	V
NVM						
Programming Current	I_{PROG}		--	100	400	μA
Programming Time	t_{PROG}	4 byte	--	7.5	15	ms
Write/Erase Cycling Endurance	N_{CY}	–40°C to 150°C	10k	--	--	Cycles
Data Retention	t_{DR}		10	--	--	Years
SHA-256 Engine						
Computation Current	I_{SHA}		--	1	--	mA
Computation Time	t_{SHA}		--	100	--	μs

Electrical Characteristics : Single-Wire Interface

(2.8V ≤ V_{DD} ≤ 5.0V, T_A = 25°C, unless otherwise specified)

Parameter	Symbol	Test Conditions	Min	Typ	Max	Unit
Fast Mode Timing						
Break Time	t_B		38	--	46	µs
Break Recovery Time	t_{BREC}		15	--	20	µs
Host Write 1	t_{HW1}		2	--	12	µs
Host Write 0	t_{HW0}		16	--	26	µs
Host Write Recovery Time	t_{HREC}		2	--	--	µs
Host Send Start Time	t_{HSTA}		2	--	6	µs
Host Sample Time	t_{HSAM}		14	--	20	µs
Device Write 1 Cycle Time	t_{DW1_CYC}		14	--	--	µs
Device Write 0 Cycle Time	t_{DW0_CYC}		28	--	--	µs
Device Write 1	t_{DW1}		8	--	12	µs
Device Write 0	t_{DW0}		22	--	26	µs
SWI Line Rising Time	t_{RISE}		--	--	100	ns
SWI Line Falling Time	t_{FALL}		--	--	100	ns
Normal Mode Timing						
Break Time	t_B		110	--	130	µs
Break Recovery Time	t_{BREC}		60	--	70	µs
Host Write 1	t_{HW1}		40	--	60	µs
Host Write 0	t_{HW0}		70	--	90	µs
Host Write Recovery Time	t_{HREC}		40	--	--	µs
Host Send Start Time	t_{HSTA}		6	--	46	µs
Host Sample Time	t_{HSAM}		62	--	78	µs
Device Write 1 Cycle Time	t_{DW1_CYC}		62	--	--	µs
Device Write 0 Cycle Time	t_{DW0_CYC}		92	--	--	µs
Device Write 1	t_{DW1}		50	--	60	µs
Device Write 0	t_{DW0}		80	--	90	µs
SWI Line Rising Time	t_{RISE}		--	--	250	ns
SWI Line Falling Time	t_{FALL}		--	--	250	ns
Chip Reset Low Time	t_{CRSTL}	Chip reset	1000	--	--	µs
SWI Reset Low Time	t_{RSTL}	SWI protocol reset	250	--	--	µs
SWI Reset High Time	t_{RSTH}	SWI protocol reset	128	--	--	ms

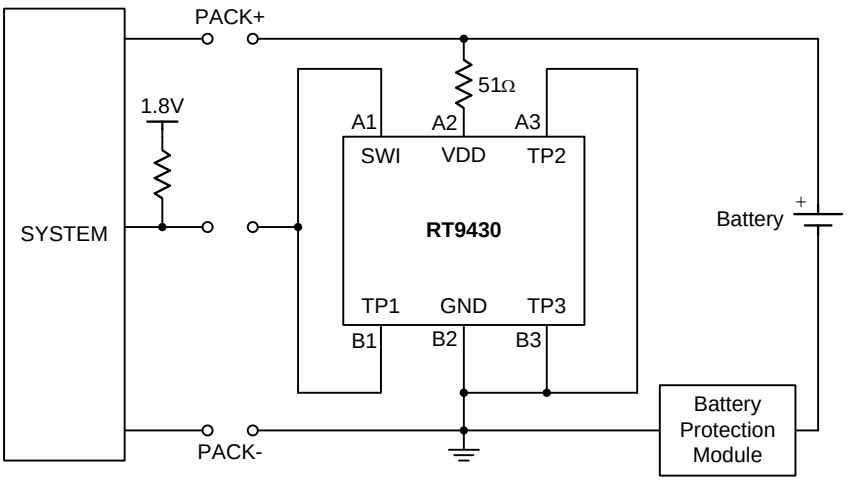
Note 1. Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions may affect device reliability.

Note 2. θ_{JA} is measured under natural convection (still air) at T_A = 25°C with the component mounted on a high effective-thermal-conductivity four-layer test board on a JEDEC 51-7 thermal measurement standard.

Note 3. Devices are ESD sensitive. Handling precaution is recommended.

Note 4. The device is not guaranteed to function outside its operating conditions.

Typical Application Circuit



Application Information

SHA-256 Authentication

The RT9430 supports SHA-256 authentication with 256 bytes Root_Secret to ensure host system uses the certificated battery pack. In order to prevent Root_Secret being revealed, the RT9430 performed a unique authentication that Root_Secret will only exist in the RT9430.

Authentication is using SHA-256 FIPS 180-3 Symmetric-Key-Based secure authentication model. The 64 bytes message block consists of a 32 bytes Root_Secret, a 32 bytes challenge and optional 8 bytes unique ROM_ID to replace challenge block. RT9430 returns a 32 bytes MAC after SHA-256 authentication. If this MAC matches an identical one generated by a host system, the authentication process is successful.

Contact Richtek for detail description.

Memory

The RT9430 battery authenticator supports 34 bytes non-volatile memory for storing user programmable data MFA_Page1, MFA_Page2, SYS_Page.

Each memory space has different access modes and also supports permanently lock function.

Contact Richtek for detail description.

Single-Wire Interface Commands

The RT9430 uses the corresponding commands to perform authentication and access NVM through the Single-Wire Interface protocol. All command lengths are fixed to 2 bytes, and the length of data to be written or read according to the command. The command must be attached by a 1 byte CRC for transmission error detection. The CRC is calculated by passing the command and data through the CRC8, $X^8 + X^2 + X + 1$ equation.

The RT9430 commands divides into Read, Write and CMD only, depends on command attribute. Figure 1 shows the host system command flow, all communication sequence follow this flow.

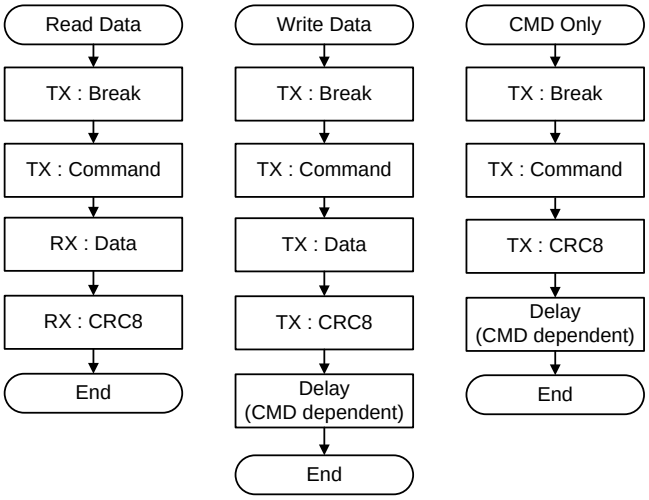


Figure 1. Host System Command Flow

Cycle Count

Cycle count maintains a total count of the battery charge cycles stored in nonvolatile memory.

Host system can increase cycle count by sending a CYCLE_COUNT command to the RT9430.

Device ID

Device_ID include 4 bytes data for chip supplier and system user information. Device_ID is read only data and can be read in every access mode.

ROM ID

8 bytes unique ROM_ID for chip identification code. ROM_ID is read only data and can be read in every access mode

Single-Wire Interface

The RT9430 battery authenticator adopts the SWI (Single-Wire Interface) to perform bidirectional data commination to host system. The MSB of the data is transmitted first, and the data is Big-Endian order. The SWI pin is open-drain and requires an external pull-up resistor.

The command length of the SWI protocol is fixed to 2 bytes. The length of the data to be written or read according to different commands. Finally, a 1 byte CRC code must be attached. The CRC Code is calculated using the equations of CRC8 ($X^8 + X^2 + X + 1$).

Break

The host initiates communication by the Break command. Immediately after the completion of the Break command, the MSB of the command is transmitted. When the RT9430 receives the Break command in the idle state, the chip begins to receive the command transmitted from the host. Please note that the Break command is required to initialize the SWI before all communications begin. In addition, through the pulse width of different Break, it can be determined SWI communication speed is Normal mode or Fast Mode. If the Break does not meet the pulse width specification, the chip will ignore the following received command.

Receiving Break during communication will reset the current SWI communication and proceed to the next command.

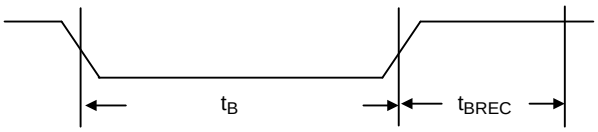


Figure 2. Break

Host Write Bit

Figure 3 and Figure 4 illustrates the waveform of host write bit .The host needs to meet the timing specifications to ensure the correctness of data transmission.

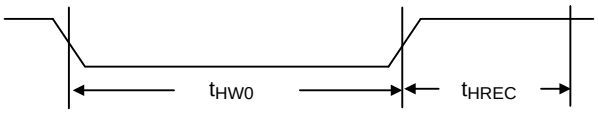


Figure 3. Host Write 1

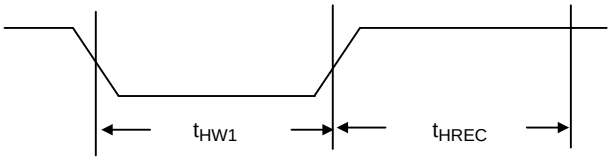


Figure 4. Host Write 0

Host Read Bit

When the host sends a read command, after the 2 bytes command is transmitted, the host needs to continue to read the RT9430 returns data. Each bit is triggered by the host to ensure data integrity.

The receive bit begins after the host pulls the SWI level low, and the host releases SWI after t_{HSTA}. When RT9430 detects the falling edge, it starts to pull down the SWI level at the same time, and releases the SWI according to the transfer bit at the corresponding time (t_{DW1}, t_{DW0}). The host must read the SWI level at t_{HSAM} after pulling down the SWI level, SWI high level for read bit 1 and the low level for bit 0.

When the host receives bit 1, it needs to delay t_{DW1_CYC} then process the next bit; when the host receives bit 0, it needs to delay t_{DW0_CYC} then process the next bit.

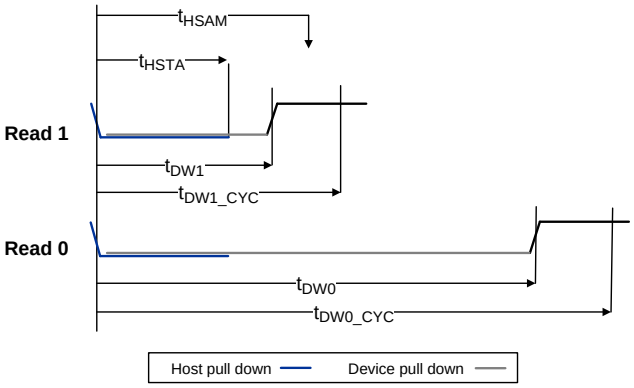


Figure 5. Host Read Bit

SWI Reset

If the SWI is held high for longer than t_{RSTH}; or if the low time is exceeded for t_{RSTL}, the SWI state machine will perform a reset. If the host does not receive the expected response from the chip, or if the host needs to reset the SWI during communication, the host can use SWI to held low time for more than t_{RSTL} to reset the SWI.

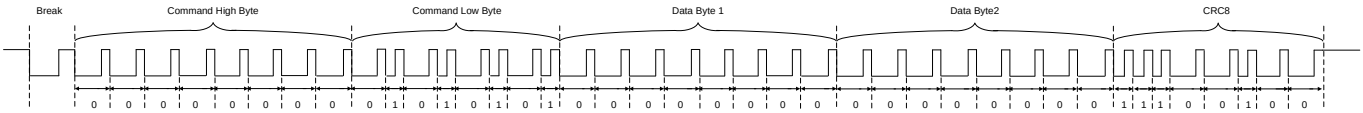


Figure 6. SWI Bit Steam

Thermal Considerations

The junction temperature should never exceed the absolute maximum junction temperature $T_{J(MAX)}$, listed under Absolute Maximum Ratings, to avoid permanent damage to the device. The maximum allowable power dissipation depends on the thermal resistance of the IC package, the PCB layout, the rate of surrounding airflow, and the difference between the junction and ambient temperatures. The maximum power dissipation can be calculated using the following formula :

$P_{D(MAX)} = (T_{J(MAX)} - T_A) / \theta_{JA}$

where $T_{J(MAX)}$ is the maximum junction temperature, T_A is the ambient temperature, and θ_{JA} is the junction-to-ambient thermal resistance.

For continuous operation, the maximum operating junction temperature indicated under Recommended Operating Conditions is 125°C. The junction-to-ambient thermal resistance, θ_{JA}, is highly package dependent. For a TWL-CSP-6B 1.46x1.16 (BSC) package, the thermal resistance, θ_{JA}, is 46.9°C/W on a standard JEDEC 51-7 high effective-thermal-conductivity four-layer test board. The maximum power dissipation at T_A = 25°C can be calculated as below :

$P_{D(MAX)}$ = (125°C - 25°C) / (46.9°C/W) = 2.13W for a TWL-CSP-6B 1.46x1.16 (BSC) package.

The maximum power dissipation depends on the operating ambient temperature for the fixed $T_{J(MAX)}$ and the thermal resistance, θ_{JA}. The derating curves in Figure 7 allows the designer to see the effect of rising ambient temperature on the maximum power dissipation.

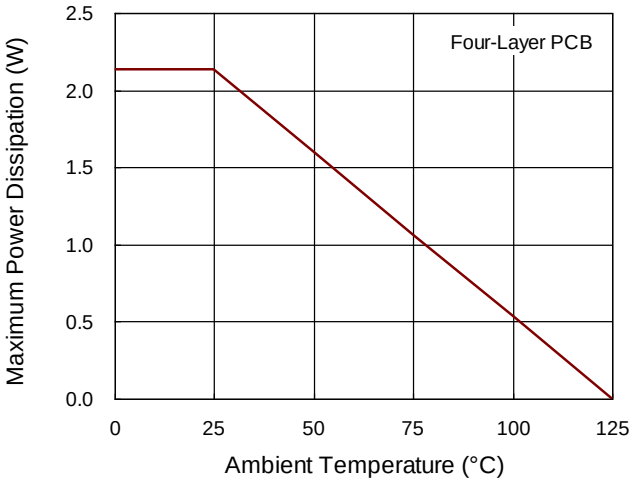


Figure 7. Derating Curve of Maximum Power Dissipation

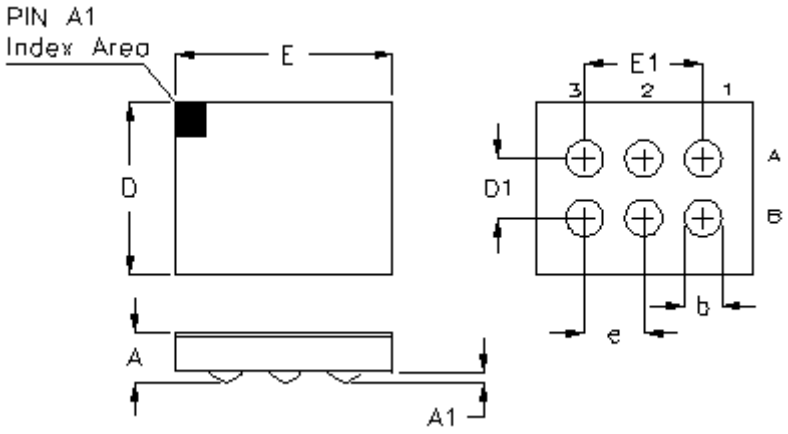
Command Summary Table

Name	Symbol	Command	Data Length	Access Mode		Description
				USER	SYS	
Status	READ_STATUS	0x0055	2	R	R	Status register
	READ_CMD_CRC	0x0051	1	R	R	Read latest received command CRC
Authentication	AUTH_WO_ROM_ID	0x8150	0	W	W	Computes SHA-256 without unique ROM_ID to replace challenge block
	AUTH_WI_ROM_ID	0x8151	0	W	W	Computes SHA-256 with unique ROM_ID to replace challenge block
	GEN_WORK_SECRET	0x8105	0	W	W	Generates new work secret
	WRITE_CHALLENGE	0x8115	32	W	W	Write challenge
	READ_CHALLENGE	0x0115	32	R	R	Read challenge
	READ_MAC	0x0125	32	R	R	Read MAC
	READ_ROM_ID	0x0135	8	R	R	Read unique ROM_ID
Secret Manage	ANONYMOUS_AUTH	0x8215	0	W	W	Anonymous authentication
	LOCK_ROOT_SECRET	0x8235	0	W	W	Permanently lock root secret
	LOCK_MFA1	0x8245	0	W	W	Permanently lock MFA1 page
	LOCK_MFA2	0x8255	0	W	W	Permanently lock MFA2 page
SEAL / UNSEAL	UNSEAL_SYS	0x8410	2	W	W	Unseal SYS mode by SYS_PWD
	SEAL_NVM	0x8480	0	W	W	Seal SYS mode to USER mode
NVM	WRITE_MFA1	0x8800	18	W	W	Write data to the MFA1 page
	WRITE_MFA2	0x8801	4	W	W	Write data to the MFA2 page
	WRITE_SYS	0x8802	12	--	W	Write data to the SYS page
	WRITE_SYS_PWD	0x8804	2	--	W	Change SYS_PWD
	READ_MFA1	0x0800	18	R	R	Read data from MFA1 page
	READ_MFA2	0x0801	4	R	R	Read data from MFA2 page
	READ_SYS	0x0802	12	--	R	Read data from SYS page
	READ_SYS_PWD	0x0804	2	--	R	Read SYS_PWD
	READ_DEVICE_ID	0x0805	4	R	R	Read Device ID
Battery	INC_CYC_CNT	0x9055	0	W	W	Increase cycle count
	READ_CYC_CNT	0x1055	2	R	R	Read cycle count
Reset	RESET	0xA055	0	W	W	Reset the RT9430

Status Register

Bit	Mode	SYMBOL	Definition	Reset
15	R	Reserved	Reserved	0
14	R	MFA2_LCK	MFA_Page2 locked	0
13	R	MFA1_LCK	MFA_Page1 locked	0
12	R	RT_SECRET_LCK	Root_Secret locked	0
11	R	Reserved	Reserved	0
10	R	CHALLENGE_RDY	Challenge ready	0
9	R	MAC_RDY	MAC ready	0
8	R	WK_SECRET_RDY	Work Secret ready	0
7	R/C	SWI_TIMEOUT	SWI timeout occurs	0
6	R/C	SWI_CRC_ERR	Received error CRC	0
5	R	Reserved	Reserved	0
4	R	Reserved	Reserved	0
3	R/C	RI	Reset flag	1
2	R	BUSY	Device is busy with an internal operation.	0
1	R	Reserved	Reserved	0
0	R	SYS_MODE	SYS Mode unsealed	0

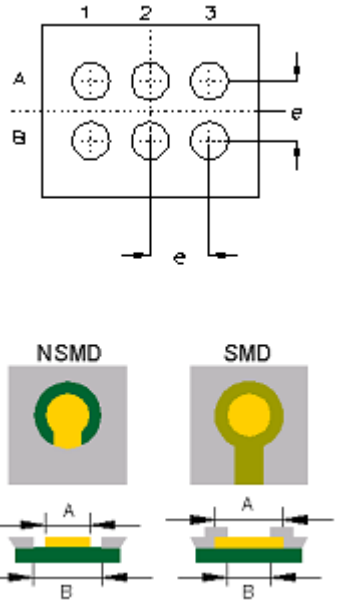
Outline Dimension



Symbol	Dimensions In Millimeters		Dimensions In Inches	
	Min	Max	Min	Max
A	0.310	0.350	0.012	0.014
A1	0.060	0.080	0.002	0.003
b	0.220	0.280	0.009	0.011
E	1.420	1.500	0.056	0.059
E1	0.800		0.031	
D	1.120	1.200	0.044	0.047
D1	0.400		0.016	
e	0.400		0.016	

6B TWL-CSP 1.46x1.16 Package (BSC)

Footprint Information



Package	Number of Pin	Type	Footprint Dimension (mm)			Tolerance
			e	A	B	
TWL-CSP1.46x1.16-6(BSC)	6	NSMD	0.400	0.250	0.350	±0.025
		SMD		0.260	0.250	

Richtek Technology Corporation
14F, No. 8, Tai Yuen 1st Street, Chupei City
Hsinchu, Taiwan, R.O.C.
Tel: (8863)5526789