

## **1. Preface**

This manual provides an introduction of the Board ID device with pre-loaded authentication firmware. The authentication firmware supports four use cases with powerful authentication capability. This firmware is designed to minimize the development effort on the Board ID device with its pre-fabricated authentication API so that robust authentication can be implemented mainly by developing the host (authenticator) application.

## **2. The Target Device**

This document is dedicated to the “Authentication Firmware” version of Board ID device (R5H30211) and covers the functional specification including the pin assignment, the I2C host interface, the firmware register set and the authentication procedure. The authentication firmware is not modifiable, due to the nature of a secure device.

This document also covers the necessary tasks on the host (authenticator) application

### 3. Feature List

The authentication firmware utilizes a X.509 digital certificate including the RSA 1024/2048bit device public key.

#### Anti Cloning

The authenticator (host) can verify the integrity of the digital certificate with the public key from root CA.

The authenticator (host) can verify the ownership of the digital certificate with the challenge/response process.

#### Usage Control

Additional Usage Counter can limit the number of positive authentication. Preset value (1 to 4294967295 = 0xFFFFFFFF) will be programmed at the provisioning stage.

Once the number of authentication reaches to the pre-set limit, the authentication result becomes negative / expired.

#### Secure Tracking

4 bytes (0 to 4294967295 = 0xFFFFFFFF) of secure tracking information enables a region control or a country code type of restriction.

This can also be used for classifying product type or version for example.

#### IP Protection

4 bytes (0 to 4294967295 = 0xFFFFFFFF) of IP protection information enables a “Feature control” type of usage.

#### Secure Storage

The authentication firmware features 512bytes (64 × 8pages) of storage area. This area can be either designated as “one-time programmable” or “rewritable”. Rewrite (or write unlocking) to this area may be enabled by following the procedures described in Section 7.

### 4. Authentication Outline

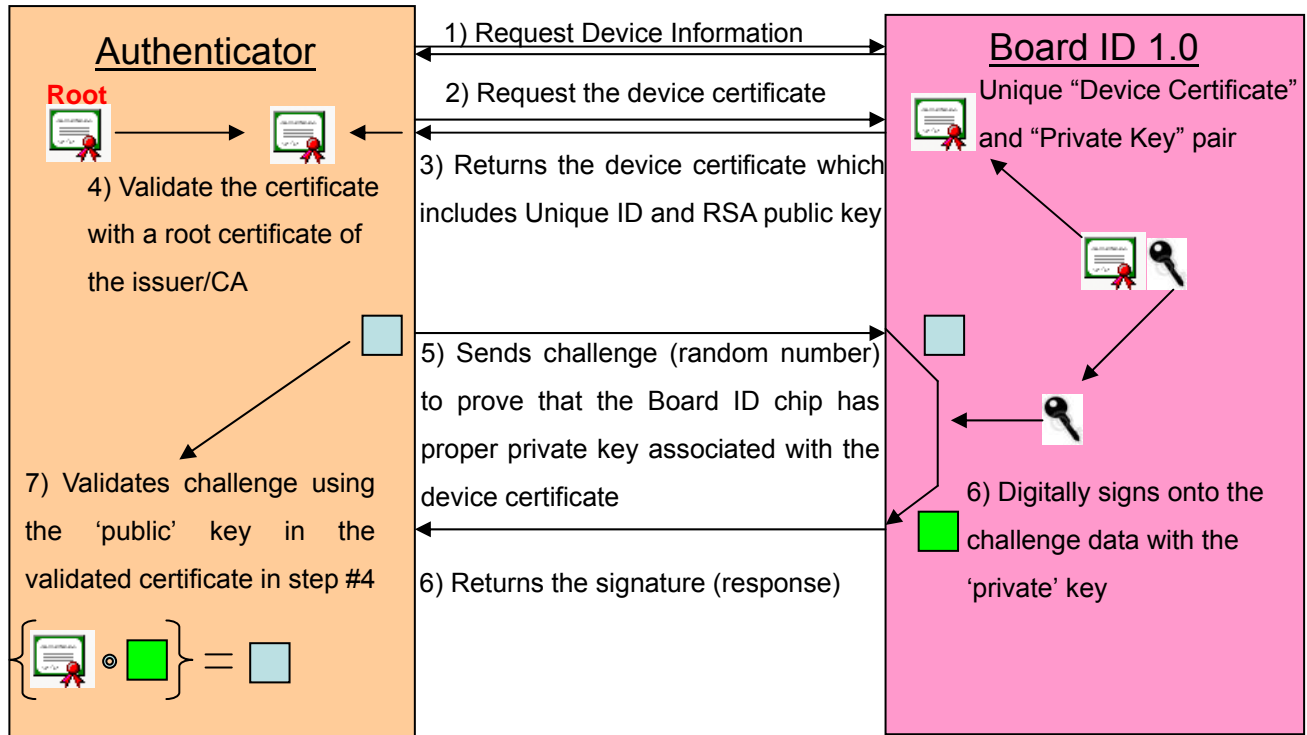


Fig. 4.1 Authentication Outline

### 5. Hardware Specification

#### 5.1. R5H30211 Device Pin Assignment

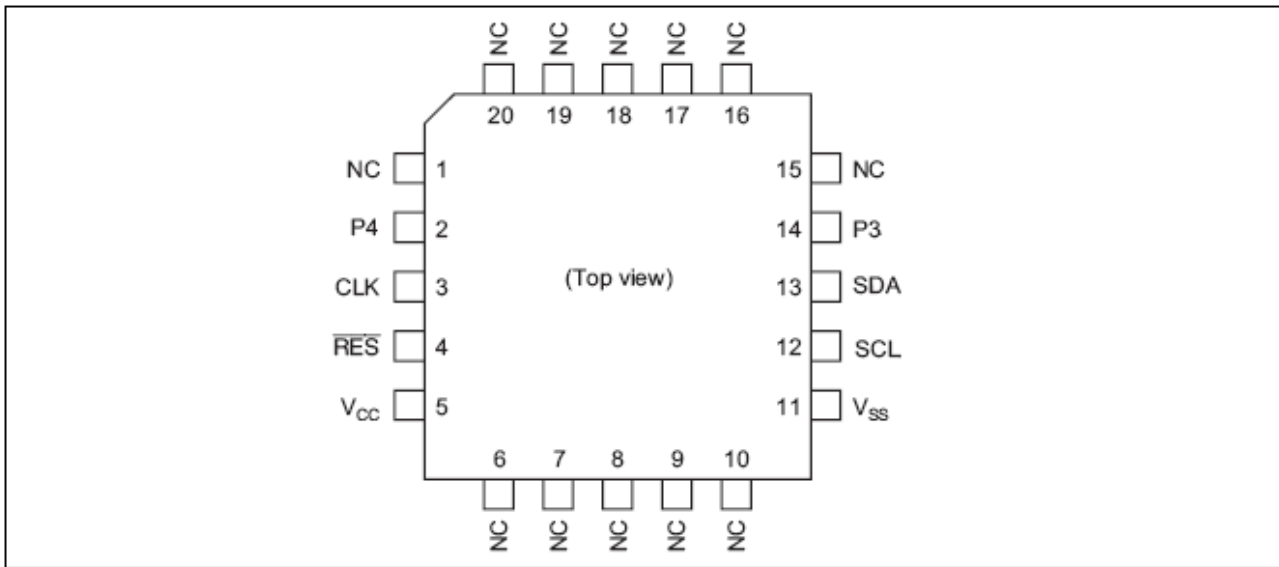


Fig. 5.1 Device Pin Arrangement      Package: QFN20 4.2mmX4.2mm

Pin	Signal	Pin	Signal
1	N/C	11	VSS
2	P4	12	SCL
3	/RES	13	SDA
4	CLK	14	P3
5	VCC	15	N/C
6-10	N/C	16-20	N/C

Table 5.1 Device Pin Assignment

### 5.2. Package Dimensions

Unit:mm

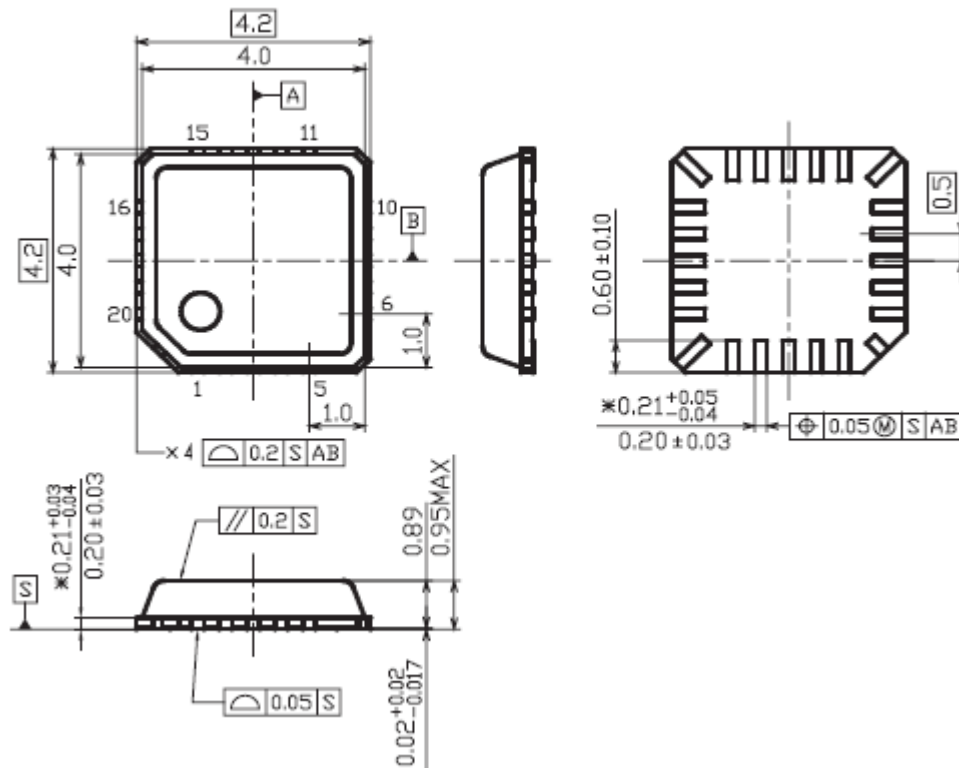
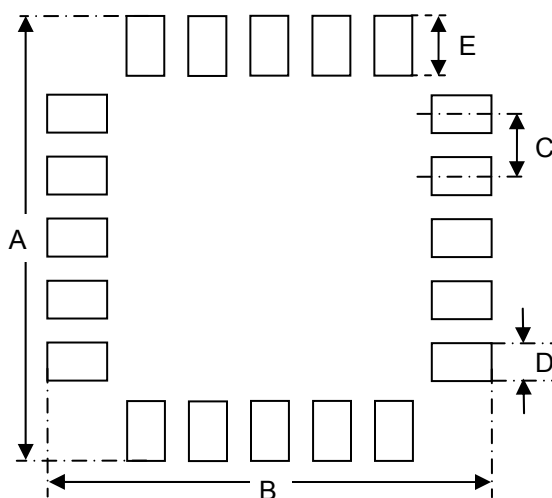


Fig 5.2 Package Dimensions

### 5.3. Sample PCB Land Layout



Footprint (mm)	
A	4.6
B	4.6
C	0.5
D	0.25
E	1.0

Fig. 5.3 Sample PCB Layout

### 5.4. Typical Operating Circuit

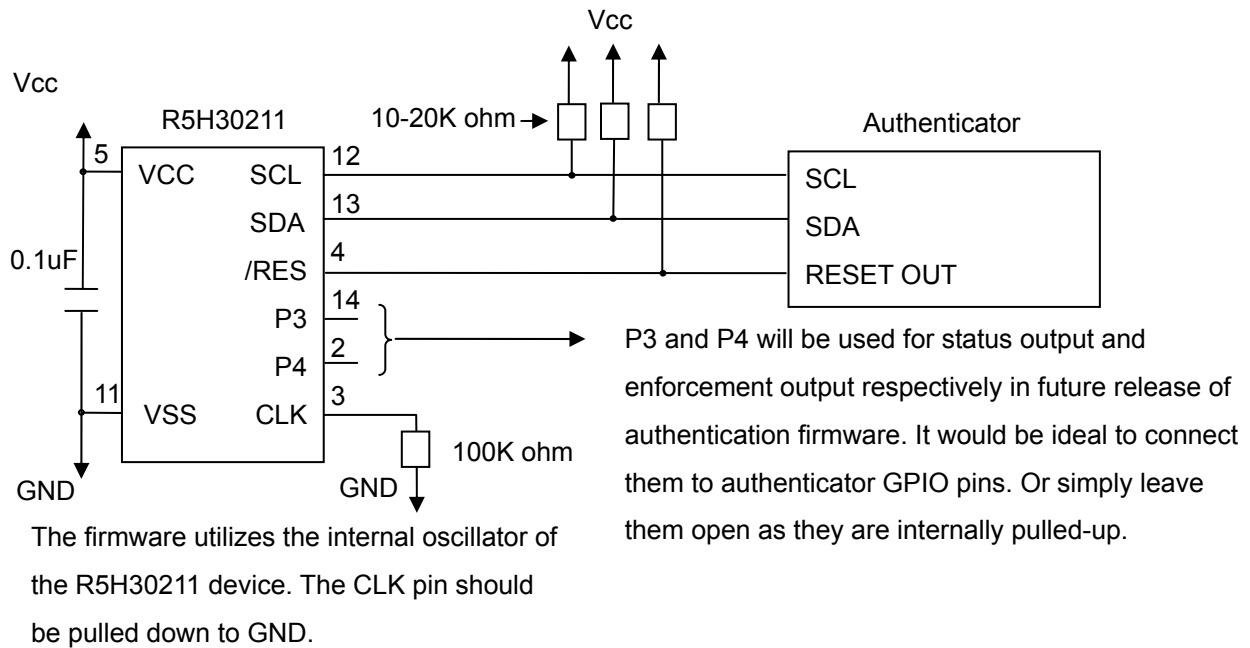


Fig. 5.4 Typical Circuit

### 5.5. Board ID Mini-module Connector Pinouts

Pin	Signal	Pin	Signal
1	SCL	2	GND
3	SDA	4	VCC
5	N/C	6	/RES
7	P3	8	CLK
9	P4	10	GND

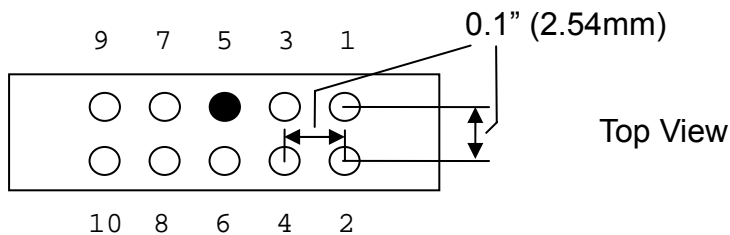


Fig. 5.5 Board ID mini-module Pin-outs

## 5.6. Absolute Maximum Ratings

Item	Symbol	Condition
Power Supply Voltage	$V_{CC}$	-0.3V to +7.0V
Input voltage	$V_{IN}$	-0.3V to $V_{CC}+0.3V$
Operating Temperature	$T_{OPR}$	-20 to +75 °C
Storage Temperature	$T_{STG}$	-55 to +75°C

Table 5.2 Absolute Maximum Ratings

Note: Permanent damage may occur to the device if any of the maximum ratings are exceeded. Normal operation should be under the recommended operation conditions. Exceeding these conditions could affect the reliability of the chip.

## 5.7. DC Characteristics

Item	Symbol	Condition	Min	Typ.	Max
Input high voltage	$V_{IH}$	$V_{CC}=3.0V$ to 3.6V	$V_{CC}\times 0.7V$	-	$V_{CC}+0.3V$
Input low voltage	$V_{IL}$	$V_{CC}=3.0V$ to 3.6V	-0.3V	-	$V_{CC}\times 0.2V$
Output high voltage	$V_{OH}$	$V_{CC}=3.0V$ to 3.6V	-0.3V	-	$V_{CC}+0.3V$
Output low voltage	$V_{OL}$	$V_{CC}=3.0V$ to 3.6V	$V_{CC}\times 0.7$	-	$V_{CC}+0.3V$
Input leakage current	$I_{IN}$	$V_{IN}=0.5V$ to $V_{CC} - 0.5V$	0V	-	0.4V
Input pull-up MOS current	$-I_P$	$V_{IN}=0V$	-	-	150 $\mu$ A
Supply current	$I_{CC}$		-	-	10mA
Pin capacitance	$C_P$	$V_{IN}=0V$	-	-	$V_{CC}+0.3V$

Table 5.3 DC Characteristics

**5.8. AC Characteristics**

Item	Symbol	Condition	Min	Typ.	Max
System clock	$t_{cyc}$	Fig. 4.1	139ns	166ns	208ns
Cold reset pulse width	$t_{RWL1}$	Fig. 4.2	500 $\mu$ s	-	-
Warm reset pulse width	$t_{RWL2}$	Fig. 4.2	400 $t_{cyc}$	-	-
EEPROM write time	$t_{EPW}$	Rewrite	-	-	3ms
EEPROM erase time	$t_{EPW}$	Erase	-	-	1.5ms
Power-on reset effective voltage	$V_{POR1}$	Fig. 4.3	-	-	0.1V
Power-on reset release voltage rise time	$t_{PWON1}$	Fig. 4.3 $t_{POR1} \geq 1s$ Fig. 4.3 $t_{POR1} \geq 10s$	- -	- -	0.5ms 1ms
Power-on reset release time	$t_{PRST}$	Fig. 4.3	-	-	500 $\mu$ s
SCL input cycle time	$t_{SCL}$	Fig. 4.4	12 $t_{cyc}+600ns$	-	-
SCL input cycle time	$t_{SCLH}$	Fig. 4.4	3 $t_{cyc}+300ns$	-	-
SCL input cycle time	$t_{SCLL}$	Fig. 4.4	5 $t_{cyc}+300ns$	-	-
SCL/SDA input fall time	$t_{sf}$	Fig. 4.4	-	-	300ns
SCL/SDA input spike pulse removal time	$t_{SP}$	Fig. 4.4	-	-	1 $t_{cyc}$
SDA input bus free time	$t_{BUF}$	Fig. 4.4	5 $t_{cyc}$	-	-
Start condition input hold time	$t_{STAH}$	Fig. 4.4	3 $t_{cyc}$	-	-
Repeated start condition input setup time	$t_{STAS}$	Fig. 4.4	3 $t_{cyc}$	-	-
Stop condition input setup time	$t_{STOS}$	Fig. 4.4	3 $t_{cyc}$	-	-
Data input setup time	$t_{SDAS}$	Fig. 4.4	1 $t_{cyc} + 20ns$	-	-
Data input hold time	$t_{SDAH}$	Fig. 4.4	0ns	-	-

Table 5.4 AC Characteristics

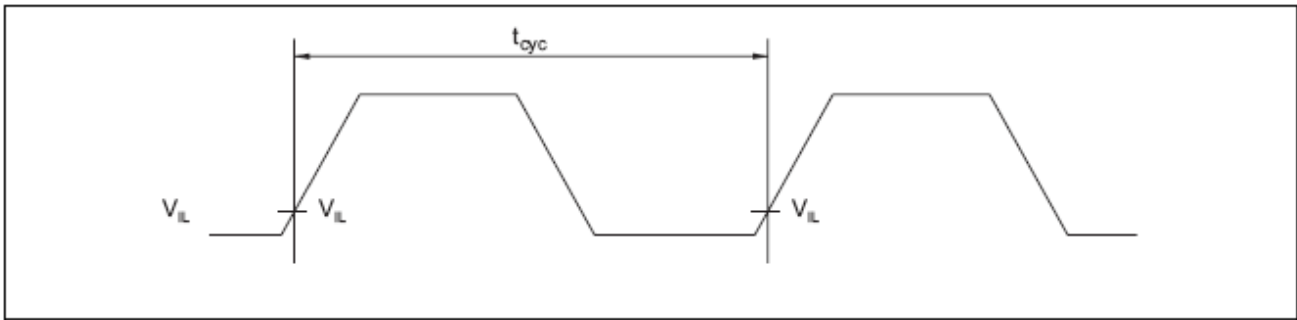


Fig. 5.6 System Clock (Internal)

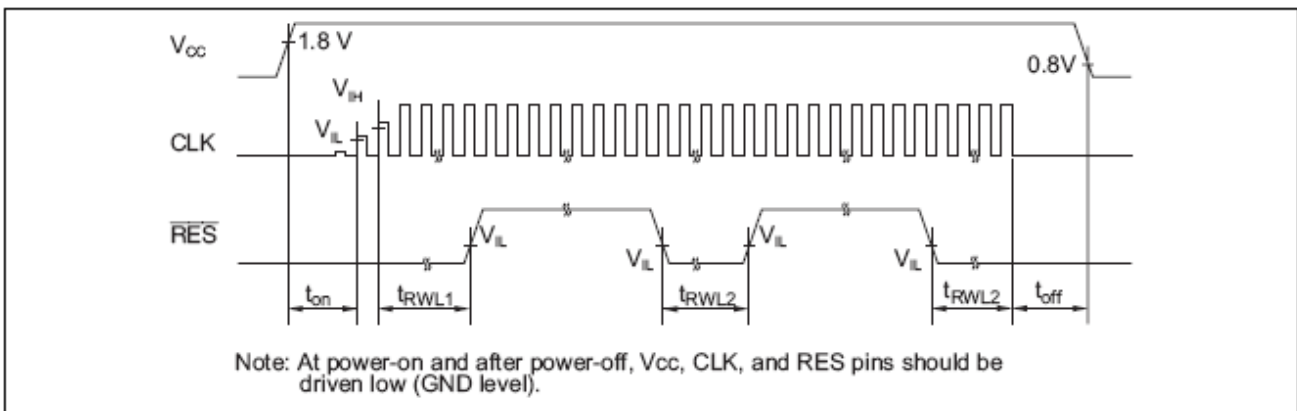


Fig. 5.7 Power ON/OFF and /RES Input Timing

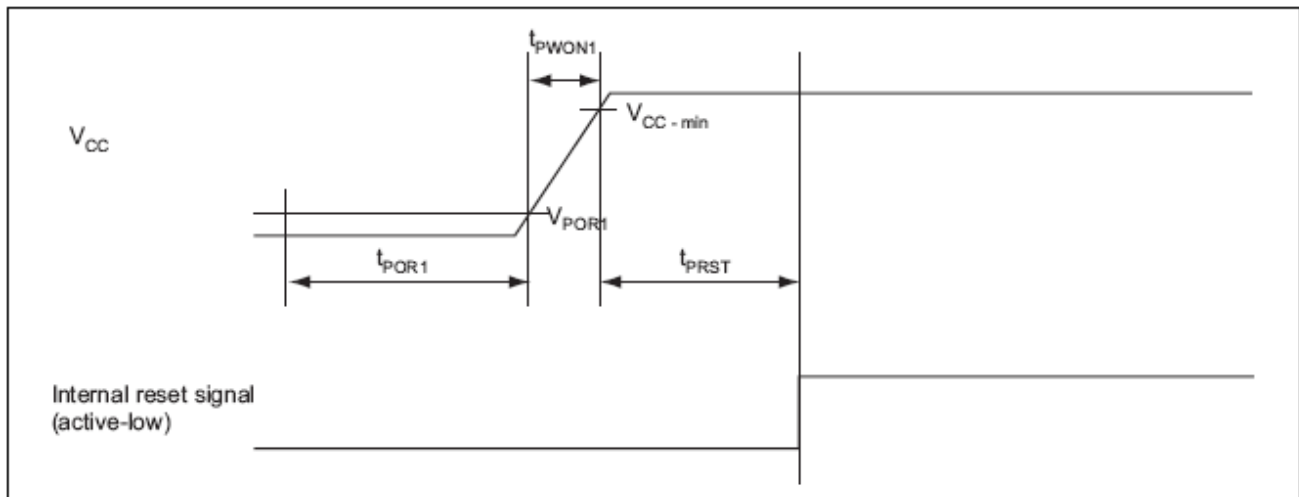


Fig. 5.8 Power-on Reset Timing

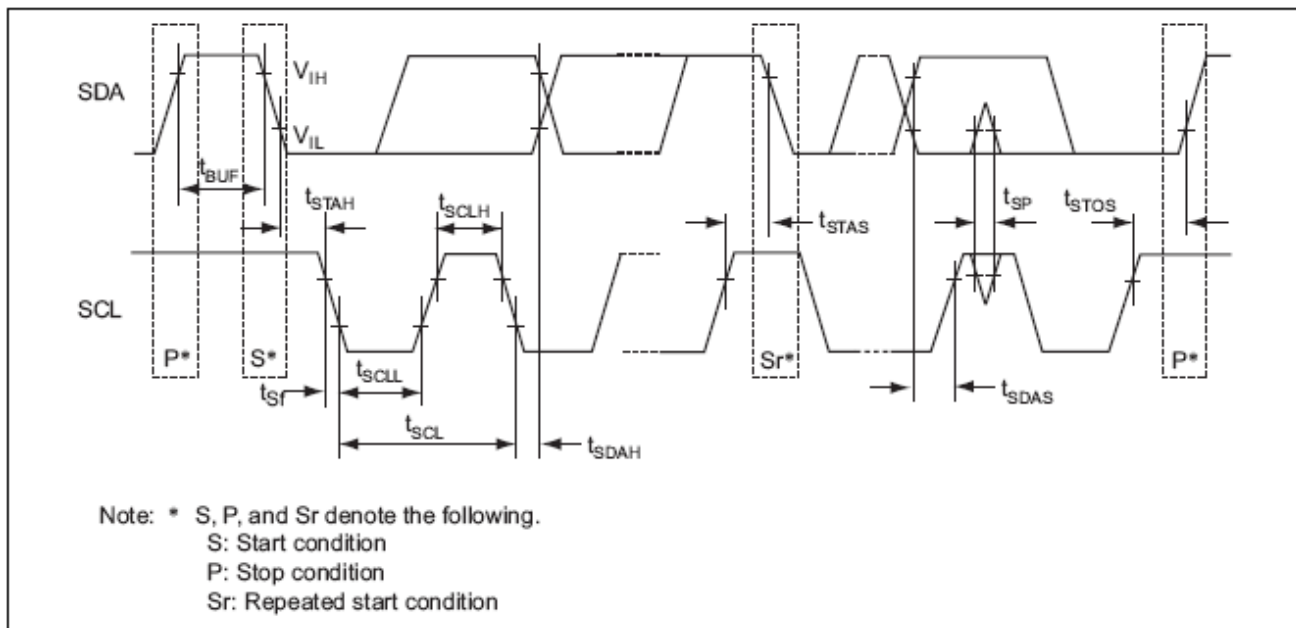


Fig. 5.9 I2C Bus Interface

### 5.9. Reflow Soldering Conditions

Reflowing must be performed under following condition:

	Condition	Reflowing time (230 - 260°C)
Maximum temperature	260°C	
Reflowing temperature	230°C	30 to 50 seconds
Maximum Reflowing Count	3 times	

### 5.10. Storage and Handling

The device must be kept within the following condition after opening dry packing:

	Condition	Note
Storage Temperature	5°C – 30°C	
Storage Humidity	60% RH or less	

Note 1: It is recommended to complete the final reflow soldering process within 168 hours after opening the dry packing.

Note 2: **Do not bake the device under any circumstance or the device may be permanently damaged.**

## 6. Ordering Information

As described in section 3, the Board ID has two versions – sample and production version. Once the use case and its conditions are determined, the production version of device is ready to be ordered. Unlike the sample device with pre-installed ‘sample’ certificate, the production devices will hold individual ‘device’ certificate and mating ‘private’ key, along with the use case/parameter information.

These information need to be provided to the provisioning authority by filling the customer ordering form as shown in the next page. Necessary information to be filled is as follows:

Item:	Example
Authentication related:	
Usage Allowance:	0 – 4294967295 (0xFFFFFFFF)
Secure Tracking Information:	0 – 4294967295 (0xFFFFFFFF)
IP Protection Information:	0 – 4294967295 (0xFFFFFFFF)
I2C slave address:	1 – 127 (7 bit, default: 80 = 0x50)
Customer related:	
CA Distinguished Name	
Country code:	US
State/Province:	CA
City:	San Jose
Company (Organization) name:	YourCompanyName
Unit name (optional)	YourDivision
Email address (optional)	YourName@YourCompanyName.com
Device Distinguished Name	
Country code:	US
State/Province:	CA
City:	San Jose
Company (Organization) name:	YourCompanyName
Unit name (optional):	YourDivision
Email address (optional):	YourName@YourCompanyName.com

Filled information will be stored in the device certificate and provisioning authority will insert the device certificate and authentication conditions to the Board ID device.

Provisioning authority strictly controls the ordering and provisioning process so that no other entity can obtain the Board ID devices with other company’s device certificate installed.

Board ID 1.0 Customer Data Form February, 2010	data size	comments	examples	customer data
<b>Certificate setting</b>				
Usage Control Allowed Authentication Count	4 Bytes	Allowed Authentication Count	Eg. 1000 Enter a 4-byte integer in decimal format	(*)
Secure Tracking / Location	4 Bytes	Location Field	Eg. 1234567890 Enter a 32-bit decimal number	(*)
IP Protection	4 Bytes	IP Protection Field	Eg. 8192 Enter the desired 7-bit Slave Address (decimal format)	(*)
I2C Slave Address	1 Byte	I2C Slave Address	Eg. 32	
Certificate validity period	Expiry date or expiry period	format YYYY/MM/DD/HH/MM/SS format XXXX	Eg. 2010/06/30/12/00/00 Eg. 365 days	(**)
<b>Certificate Authority Distinguished Name</b>				
Country Code	2 Bytes	Country Code	Enter the 2 character country code Eg. US	
State or Province Name	16 Bytes max	State Name	Enter the state or province name Eg. California	
Locality (or City) Name	32 Bytes max	Locality (or City) Name	Eg. San Jose	
Organization Name	32 Bytes max	Company Name	Eg. XYZ Inc	
Organizational Unit Name (optional)	32 Bytes max			
E-mail Address (optional)	32 Bytes max			
<b>Fixed Applet Device Distinguished Name</b>				
Country Code	2 Bytes	Country Code	Enter the 2 character country code Eg. US	
State or Province Name	16 Bytes max	State Name	Enter the state or province name Eg. California	
Locality (or City) Name	32 Bytes max	Locality (or City) Name	Eg. San Jose	
Organization Name	32 Bytes max	Company Name	Eg. XYZ Inc	
Organizational Unit Name (optional)	32 Bytes max			
E-mail Address (optional)	32 Bytes max			
<b>RSA key length</b>	2 Bytes	1024 bits or 2048 bits	Eg. 1024 bits	
<b>Optional: Secure data storage</b>				
EEPROM Storage Data	512 Bytes max	Optional customer data in binary format	A binary file of size 512 bytes containing the customer data	
Authentication Key	24 Bytes	HMAC User Authentication Key	Binary file of size 24 bytes	
<b>Note:</b>				
(*) if these 3 fields are left blank, the device will perform a simple authentication				
(**) cannot exceed year 2049				

Fig. 6.1 Board ID 1.0 Order Form

## 7. Additional Information

Please visit <http://america.renesas.com/boardid/> for more information. More details are provided in the Board ID 1.0 User Manual available under NDA.