

---

# iPod Authentication Coprocessor 2.0B Specification

Release R5



2009-07-27



Apple Inc.  
© 2009 Apple Inc.  
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, electronic, photocopying, recording, or otherwise, without prior written permission of Apple Inc., with the following exceptions: Any person is hereby authorized to store documentation on a single computer for personal use only and to print copies of documentation for personal use provided that the documentation contains Apple's copyright notice.

The Apple logo is a trademark of Apple Inc.

Use of the "keyboard" Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

No licenses, express or implied, are granted with respect to any of the technology described in this document. Apple retains all intellectual property rights associated with the technology described in this document. This document is intended to assist application developers to develop applications only for Apple-labeled or Apple-licensed computers.

Every effort has been made to ensure that the information in this document is accurate. Apple is not responsible for typographical errors.

Apple Inc.  
1 Infinite Loop  
Cupertino, CA 95014  
408-996-1010

Apple, the Apple logo, iPod, and Pages are trademarks of Apple Inc., registered in the United States and other countries.

Simultaneously published in the United States and Canada.

**Even though Apple has reviewed this document, APPLE MAKES NO WARRANTY OR REPRESENTATION, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT, ITS QUALITY, ACCURACY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. AS A RESULT, THIS DOCUMENT IS PROVIDED "AS IS," AND YOU, THE READER, ARE ASSUMING THE**

**ENTIRE RISK AS TO ITS QUALITY AND ACCURACY.**

**IN NO EVENT WILL APPLE BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY DEFECT OR INACCURACY IN THIS DOCUMENT, even if advised of the possibility of such damages.**

**THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED. No Apple dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty.**

**Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.**

# Contents

## **Chapter 1**    **Introduction**    7

---

- Overview    7
- Authentication Protocol    7
- Terminology Used in This Document    8
- Related Documents    9

## **Chapter 2**    **Signal Descriptions and Reference Circuits**    11

---

- CP Signals and Pinouts    11
- Communication Mode Selection    12
- I2C Reference Circuit    13
- SPI Reference Circuit    14

## **Chapter 3**    **Hardware Configuration and Interface**    15

---

- System Voltage    15
- Reset    15
- Communication Modes    15
- Low-Power Sleep Mode    16

## **Chapter 4**    **Coprocessor Registers**    17

---

- Register Addresses    17
- Register Descriptions    19
  - Device Version    19
  - Firmware Version    20
  - Authentication Protocol Major and Minor Versions    20
  - Device ID    20
  - Error Code    20
  - Authentication Control and Status    21
  - Signature Data Length    22
  - Signature Data    22
  - Challenge Data Length    23
  - Challenge Data    23
  - Accessory Certificate Data Length    23
  - Accessory Certificate Data    23
  - Self-Test Control and Status    23

iPod Certificate Data Length 24  
 iPod Certificate Data 25

**Chapter 5**      **Authentication Data Flows** 27

---

iPod Authentication of Accessory 27  
 Accessory Authentication of iPod 28

**Chapter 6**      **I2C Communication Protocol** 31

---

Slave Selection and Reset 31  
 Coprocessor Busy 31  
 Writing to the Coprocessor 31  
 Reading from the Coprocessor 32

**Chapter 7**      **SPI Communication Protocol** 33

---

Slave Selection and Reset 33  
 Timing and Polarity 34  
 Coprocessor Busy 34  
 Writing to the Coprocessor 35  
 Reading from the Coprocessor 36

**Chapter 8**      **CP Device Characteristics** 39

---

Maximum Environmental Conditions 39  
 Recommended Operating Conditions 39  
 DC Electrical Characteristics 40  
 Timing Characteristics 41  
 Mechanical Package Characteristics 42

Document Revision History 47

---

# Figures and Tables

## Chapter 1 Introduction 7

---

Table 1-1 Document-specific terminology 8

## Chapter 2 Signal Descriptions and Reference Circuits 11

---

Figure 2-1 CP chip pinouts, top view 11  
Figure 2-2 Reference circuit for CP as I2C slave 13  
Figure 2-3 Reference circuit for CP as SPI slave 14  
Table 2-1 CP signals 11  
Table 2-2 Mode selection signals 13

## Chapter 3 Hardware Configuration and Interface 15

---

Figure 3-1 I<sup>2</sup>C slave write address 16  
Figure 3-2 I<sup>2</sup>C slave read address 16

## Chapter 4 Coprocessor Registers 17

---

Figure 4-1 Authentication Control/Status register, read-only bits 21  
Figure 4-2 Authentication Control/Status register, write-only bits 22  
Figure 4-3 Self-test Control/Status register, write-only bits 23  
Figure 4-4 Self-test Control/Status register, read-only bits 24  
Table 4-1 iPod Authentication Coprocessor 2.0B register map 17  
Table 4-2 Error codes 20  
Table 4-3 Authentication ERR\_SET values 21  
Table 4-4 Authentication PROC\_RESULTS values 21  
Table 4-5 Authentication PROC\_CONTROL values 22  
Table 4-6 Self-test PROC\_CONTROL values 24  
Table 4-7 Self-test result bits 24

## Chapter 5 Authentication Data Flows 27

---

Table 5-1 Sequence of interactions by which an iPod authenticates an accessory 27  
Table 5-2 Sequence of interactions by which an accessory authenticates an iPod 28

**Chapter 7**      **SPI Communication Protocol**    33

---

Figure 7-1      SPI\_nSS timing    33  
 Figure 7-2      SPI data transmission timing    35  
 Figure 7-3      Command byte that starts an SPI write action to the CP    35  
 Figure 7-4      Coprocessor write timing    36  
 Figure 7-5      Command byte that starts a read action from the CP    36  
 Figure 7-6      Coprocessor read timing    37  
 Table 7-1      Maximum SPI transaction delay times    34

**Chapter 8**      **CP Device Characteristics**    39

---

Figure 8-1      Typical power-on reset timing and voltage limits    41  
 Figure 8-2      Typical external reset timing and voltage limits    42  
 Figure 8-3      Typical I/O port input waveform    42  
 Figure 8-4      2.0B iPod Authentication Coprocessor QFN-20 package    43  
 Figure 8-5      2.0B iPod Authentication Coprocessor SOP-8 package    44  
 Table 8-1      Maximum electrical and temperature ranges    39  
 Table 8-2      Recommended operating conditions    39  
 Table 8-3      Supply current into  $V_{CC}$ , excluding external current    40  
 Table 8-4      Inputs    40  
 Table 8-5      Outputs    40  
 Table 8-6      Values for Figure 8-1    41  
 Table 8-7      Values for Figure 8-2    42  
 Table 8-8      Values for Figure 8-3    42  
 Table 8-9      QFN-20 package dimensions in millimeters    43  
 Table 8-10      SOP-8 package dimensions in millimeters    44

# Introduction

---

NOTICE OF PROPRIETARY PROPERTY: THE INFORMATION CONTAINED HEREIN IS THE PROPRIETARY PROPERTY OF APPLE INC. THE POSSESSOR AGREES TO THE FOLLOWING: (I) TO MAINTAIN THIS DOCUMENT IN CONFIDENCE, (II) NOT TO REPRODUCE OR COPY IT, (III) NOT TO REVEAL OR PUBLISH IT IN WHOLE OR IN PART, (IV) ALL RIGHTS RESERVED. ACCESS TO THIS DOCUMENT AND THE INFORMATION CONTAINED THEREIN IS GOVERNED BY THE TERMS OF THE MADE FOR IPOD LICENSE AGREEMENT AND/OR THE IPOD TECHNOLOGY EVALUATION LICENSE AND CONFIDENTIALITY AGREEMENT. ALL OTHER USE SHALL BE AT APPLE'S SOLE DISCRETION.

## Overview

---

An Apple iPod verifies whether a device attached to it is an authorized accessory by issuing an authentication challenge to the device. The device must respond to the iPod's challenge, and it can do so only with the assistance of an **iPod Authentication Coprocessor (CP)** chip located in the device. Conversely, the accessory device can use its CP chip to authenticate the iPod. Certain control and reporting functions of the iPod are made available externally only after it has authenticated an attached device as an authorized accessory.

Earlier versions of the iPod Authentication Coprocessor (1.0 and 2.0A) were implemented in a QFN-40 package. The current version, 2.0B, is available in two smaller and more efficient industry-standard packages: the QFN-20 (20-pin Quad Flat No-lead) package and the SOP-8 (8-pin Small Outline) package. This document describes the configuration, usage, and specifications of Apple's iPod Authentication Coprocessor 2.0B in both packages.

## Authentication Protocol

---

The authentication protocol supported by the iPod Authentication Coprocessor 2.0B is based on standard X.509 version 3 certification. Each certificate is generated and signed by a recognized certificate authority and has a unique serial number. Information about the X.509 standard can be found at the IETF website <http://tools.ietf.org/html/3280>.

For information about the iAP General lingo commands required to perform authentication using the iPod Authentication Coprocessor 2.0B, see Apple's *iPod Accessory Protocol Interface Specification*, Release R36.

The iPod Authentication Coprocessor 2.0B supports iAP General lingo commands 0x14 through 0x1F, providing five authentication-related services:

**For iPod authentication of the accessory:**

- **Certificate delivery:** To initiate authentication of the accessory that contains it, the CP supplies an X.509 digital certificate for public key verification by the attached iPod.
- **Signature generation:** To complete authentication of the accessory that contains it, the CP generates a valid digital signature in response to a challenge from an attached iPod. This signature authorizes the iPod to respond to messages and commands from the accessory.

**For accessory authentication of the iPod:**

- **iPod certificate validation:** To initiate the authentication of an iPod attached to an accessory, the CP verifies that the X.509 certificate supplied by iPod has been signed by the proper certificate authority.
- **Challenge generation:** To continue the authentication of an iPod attached to an accessory, the accessory's CP can generate a challenge to be sent to the iPod.
- **Signature verification:** To complete the authentication of an iPod attached to the accessory, the CP can verify the signature returned by the iPod in response to the previous challenge.

## Terminology Used in This Document

---

Certain technical terms specific to this document are defined in Table 1-1.

**Table 1-1** Document-specific terminology

Term	Definition
Accessory controller	The microcontroller in an iPod accessory responsible for implementing application-specific logic.
Authentication coprocessor	A device in an accessory controller that provides iPod-related digital signature creation and verification services.
Challenge	A random number sent via iAP from an iPod to an accessory controller, or vice versa. The device being challenged must perform a digital signature computation on the offered challenge and return the resulting digital signature to the challenging device for verification.
Digital signature	The result obtained by performing a digital signing process on an offered challenge.
iAP	iPod Accessory Protocol. See Apple's <i>iPod Accessory Protocol Interface Specification</i> .



Term	Definition
I <sup>2</sup> C bus	A 2-wire serial bus designed by Philips to allow easy communication between components that reside on the same circuit board. The I <sup>2</sup> C specification is located at <a href="http://www.semiconductors.philips.com/acrobat_download/literature/9398/39340011.pdf">http://www.semiconductors.philips.com/acrobat_download/literature/9398/39340011.pdf</a> .
SPI bus	A 4-wire serial communications interface used by many microprocessor peripheral chips.
STD configuration	The standard temperature range configuration of the 2.0B coprocessor chip.
WTR configuration	The wide temperature range configuration of the 2.0B coprocessor chip.
X.509 certification	A standard defined by the International Telecommunication Union (ITU) that governs the format of certificates used for authentication and sender identity verification in public-key cryptography. X.509 certificates contain the public keys used in the iPod's accessory authentication process.

Parts of this document contain specification requirements that are incorporated by reference into legal agreements between Apple Inc. and its licensees. The use of the words “must,” “should,” “may,” and “reserved” in these specifications have the following meanings:

- “Must” means that the specification is an absolute requirement.
- “Must not” means that the specification is an absolute prohibition.
- “Should” means that there may be valid reasons in particular circumstances to ignore the specification, but their full implications must be understood and carefully weighed before choosing to do so.
- “Should not” means that there may be valid reasons in particular circumstances that make the specified action or feature acceptable, but their full implications must be understood and carefully weighed before choosing to include it.
- “May” means that the indicated action or feature does not contravene this specification.
- When a data field is marked “reserved,” accessories writing to it must set it to 0 and accessories reading it must ignore its value.

## Related Documents

---

For further information about authenticating iPods and their attached accessories, see the *iPod Accessory Protocol Interface Specification*, Release R36.



# Signal Descriptions and Reference Circuits

This chapter defines the pinout, signals, and reference circuitry of the iPod Authentication Coprocessor 2.0B supplied by Apple, Inc.

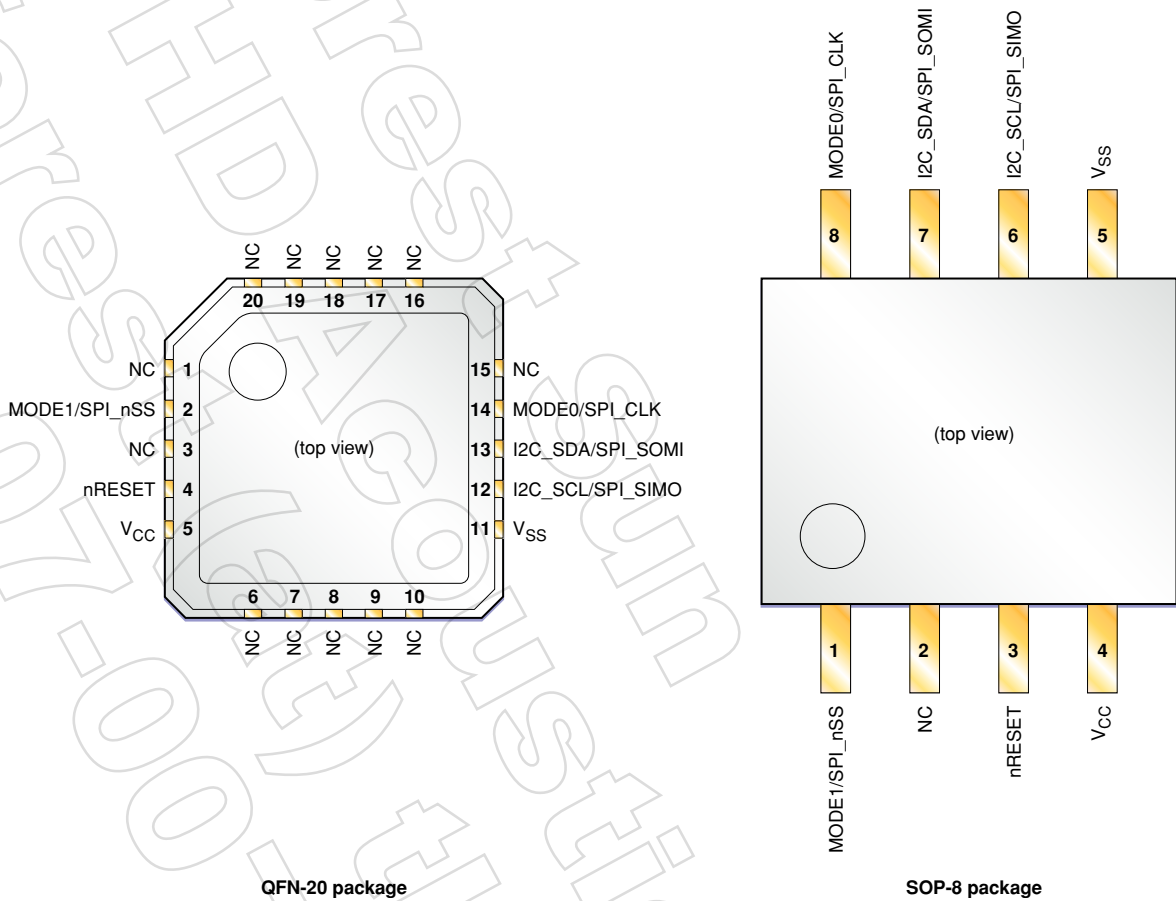
## CP Signals and Pinouts

The 2.0B CP chip signal descriptions are given in Table 2-1 and its pinouts for both QFN-20 and SOP-8 packages are shown in [Figure 2-1](#) (page 11).

**Table 2-1** CP signals

Signal name	QFN-20 pin	SOP-8 pin	I/O	Description
V <sub>CC</sub>	5	4	I	Supply voltage, positive terminal
V <sub>SS</sub>	11	5	I	Supply voltage, negative terminal
nRESET	4	3	I	CP reset (active low)
I2C_SDA SPI_SOMI	13	7	I/O O	I2C mode: I2C data SPI mode: slave-to-master data
I2C_SCL SPI_SIMO	12	6	I/O I	I2C mode: I2C clock SPI mode: master-to-slave data
MODE0 SPI_CLK	14	8	I I	Reset: selects communication mode SPI mode: SPI clock
MODE1 SPI_nSS	2	1	I I	Reset: selects communication mode SPI mode: SPI slave select (active low)
NC	1, 3, 6–10, 15–20	2		Do not connect

Figure 2-1 CP chip pinouts, top view



**Note:** The MODE0 and MODE1 inputs must not be left unconnected. The next section describes their usage.

## Communication Mode Selection

When nRESET is driven low to initiate a CP reset cycle, the states of MODE0 and MODE1 must be set to select the CP's communication mode, as shown in Table 2-2 (page 13). After nRESET goes high, the states of these and the other CP inputs must be held static for at least 30 ms to complete the reset cycle (see "Reset" (page 15)). After reset completion, if SPI mode has been selected, the MODE0 input switches its functionality to SPI\_CLK and the MODE1 input switches to SPI\_nSS.

**Table 2-2** Mode selection signals

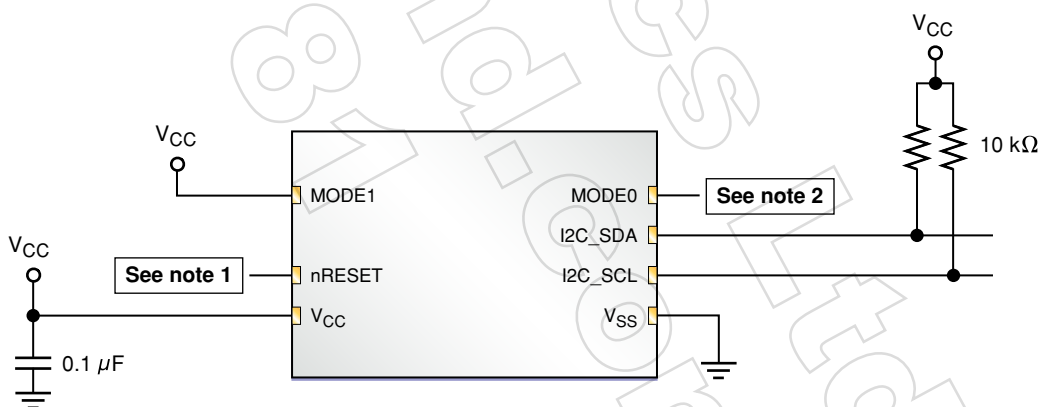
Signal state		Communication mode	I2C addresses	
MODE1	MODE0		Write	Read
0	0	SPI slave mode		
0	1	Reserved		
1	0	I <sup>2</sup> C slave mode	0x20	0x21
1	1		0x22	0x23

See “[Communication Modes](#)” (page 15) for interface details of the communication modes listed in Table 2-2.

## I2C Reference Circuit

The 2.0B CP may be used either as an I<sup>2</sup>C slave or an SPI slave, but not as both. The alternate uses of QFN-20 pins 2, 12, 13, and 14 (SOP-8 pins 1, 6, 7, and 8) are shown in [Table 2-1](#) (page 11). When the CP chip is being reset, the states of QFN-20 pins 2 and 14 (SOP-8 pins 1 and 8) set its communication mode to I<sup>2</sup>C or SPI, as described in “[Communication Mode Selection](#)” (page 12).

The reference circuit for I<sup>2</sup>C operation of the CP is shown in Figure 2-2.

**Figure 2-2** Reference circuit for CP as I2C slave

The following notes apply to Figure 2-2:

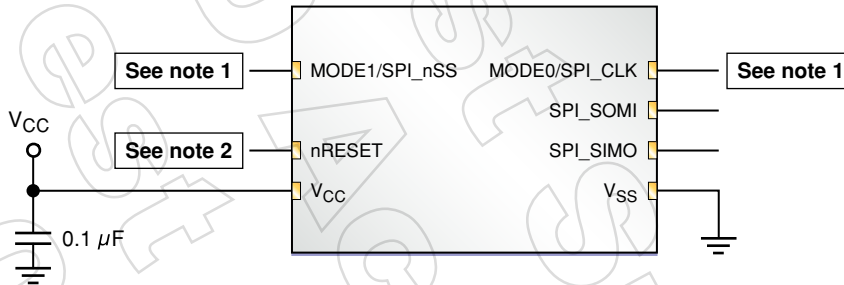
- Note 1: An active-low voltage supervisor (not shown) is recommended. nRESET should be connected either to a GPIO on the accessory's controller or to the active-low voltage supervisor.
- Note 2: The MODE0 pin should be tied to either V<sub>CC</sub> or GND to select the desired I<sup>2</sup>C slave read/write addresses, as shown in [Table 2-2](#) (page 13).

## SPI Reference Circuit

---

The reference circuit for SPI operation of the CP is shown in [Figure 2-3](#) (page 14).

**Figure 2-3** Reference circuit for CP as SPI slave



The following notes apply to Figure 2-3:

- Note 1: Hold MODE1 and MODE0 low at reset time (see [“Communication Mode Selection”](#) (page 12)). This selects SPI mode, after which the low signal on SPI\_nSS addresses the CP as an SPI slave.
- Note 2: An active-low voltage supervisor (not shown) is recommended. nRESET should be connected either to a GPIO on the accessory’s controller or to the active-low voltage supervisor.

Further details of external connections to the CP are given in [“Hardware Configuration and Interface”](#) (page 15).

# Hardware Configuration and Interface

---

This chapter describes the operating modes of the iPod Authentication Coprocessor 2.0B and the ways that it interacts with other circuitry.

## System Voltage

---

The 2.0B CP may be used either in an iPod-powered accessory or in a device that has its own power source.

## Reset

---

The nRESET pin may be used to force a reset of the CP. While nRESET is low, the CP does not operate. After nRESET goes high, the states of all I/O pins must remain the same for at least 30 ms. After that time, the CP is in its reset state and ready to operate.

The CP is available in both standard (STD) and wide temperature range (WTR) configurations (see [“Recommended Operating Conditions”](#) (page 39)). If an attempt is made to operate either configuration outside its specified temperature or voltage range, internal sensors will force it to its reset state. If this happens, or if any unexpected error condition occurs, the CP should be brought back to its specified operating environment and then externally reset.

**Note:** The nRESET pin must not be left unconnected and must be tied to  $V_{CC}$  if not actively driven by the accessory controller or another component, such as a voltage supervisor (the use of which is recommended).

## Communication Modes

---

The CP may be addressed using either I<sup>2</sup>C or SPI. In both cases, the CP is the slave device. The communication mode is set by the states of MODE1 and MODE0 when nRESET goes high, as described in [“Communication Mode Selection”](#) (page 12).

When operating, the 2.0B CP chip is internally clocked at a nominal rate of 6 MHz.

When used in I<sup>2</sup>C mode, the CP is addressed as a standard 7-bit I<sup>2</sup>C slave. The I<sup>2</sup>C slave address is configured upon reset and is based on the MODE0 input. The I<sup>2</sup>C effective slave address for writing is shown in Figure 3-1 (page 16) and the corresponding read address in Figure 3-2 (page 16).

**Figure 3-1** I<sup>2</sup>C slave write address

A6	A5	A4	A3	A2	A1	A0	R/nW
0	0	1	0	0	0	MODE0	0

**Figure 3-2** I<sup>2</sup>C slave read address

A6	A5	A4	A3	A2	A1	A0	R/nW
0	0	1	0	0	0	MODE0	1

In I<sup>2</sup>C mode, the CP has both a write address and a read address, as is typical for an I<sup>2</sup>C device. The I<sup>2</sup>C write address of the CP consists of the seven bits [A6:A0] followed by 0 for the R/nW bit. The I<sup>2</sup>C read address of the CP consists of the seven bits [A6:A0] followed by 1 for the R/nW bit. If the MODE0 input is connected to ground, the write and read addresses of the CP are 0x20 and 0x21 respectively; if it is pulled high, the write and read addresses of the CP are 0x22 and 0x23.

In SPI mode, the CP does not have a protocol-level slave address. Instead, as is typical for an SPI device, the CP is addressed by means of its slave-select pin (SPI\_nSS).

## Low-Power Sleep Mode

The 2.0B CP does not automatically enter a low-power mode. It can be forced to sleep by using the Authentication Control/Status register. See “Authentication Control and Status” (page 21) for details. Once it has gone into Sleep mode, the CP must be reset to resume normal operation. See “Reset” (page 15).

**Note:** To optimize accessory power usage, the CP should be put into Sleep mode whenever it is not being used for authentication.



# Coprocessor Registers

Registers within the iPod Authentication Coprocessor 2.0B (CP) are accessed via either I<sup>2</sup>C or SPI transport, as discussed in “[Communication Modes](#)” (page 15). Also see “[I2C Communication Protocol](#)” (page 31) and “[SPI Communication Protocol](#)” (page 33) for register addressing details and telegram formats.

## Register Addresses

Registers and their addresses in the CP are listed in Table 4-1. Each register is discussed in the sections that follow.

**Note:** Registers in the same block with consecutive addresses may be read from sequentially in increasing numerical order. With the exception of the iPod certificate data registers (addresses 0x51-0x5F), registers in the same block with consecutive addresses may also be written to sequentially in increasing numerical order. Multibyte numeric values are stored in big-endian order; for example, the first byte in a two-byte register is the MSB of the stored value and the second byte is its LSB.

**Table 4-1** iPod Authentication Coprocessor 2.0B register map

Register address	Block	Register name	Length in bytes	Contents after reset	Access mode
0x00	0	Device Version	1	0x03	Read-only
0x01	0	Firmware Version	1	0x01	Read-only
0x02	0	Authentication Protocol Major Version	1	0x02	Read-only
0x03	0	Authentication Protocol Minor Version	1	0x00	Read-only
0x04	0	Device ID	4	0x00000200	Read-only
0x05	0	Error Code	1	0x00	Read-only (cleared on read)

Register address	Block	Register name	Length in bytes	Contents after reset	Access mode
0x10	1	Authentication Control/Status	1	0x00	Read/write
0x11	1	Signature Data Length	2	128	Read/write
0x12	1	Signature Data	128	Undefined	Read/write
0x20	2	Challenge Data Length	2	20	Read/write
0x21	2	Challenge Data	20	Undefined	Read/write
0x30	3	Accessory Certificate Data Length	2	≤1920	Read-only
0x31	3	Accessory Certificate Data (Page 1)	128	Certificate	Read-only
0x32	3	Accessory Certificate Data (Page 2)	128	Certificate	Read-only
0x33	3	Accessory Certificate Data (Page 3)	128	Certificate	Read-only
0x34	3	Accessory Certificate Data (Page 4)	128	Certificate	Read-only
0x35	3	Accessory Certificate Data (Page 5)	128	Certificate	Read-only
0x36	3	Accessory Certificate Data (Page 6)	128	Certificate	Read-only
0x37	3	Accessory Certificate Data (Page 7)	128	Certificate	Read-only
0x38	3	Accessory Certificate Data (Page 8)	128	Certificate	Read-only
0x39	3	Accessory Certificate Data (Page 9)	128	Certificate	Read-only
0x3A	3	Accessory Certificate Data (Page 10)	128	Certificate	Read-only
0x3B	3	Accessory Certificate Data (Page 11)	128	Certificate	Read-only

Register address	Block	Register name	Length in bytes	Contents after reset	Access mode
0x3C	3	Accessory Certificate Data (Page 12)	128	Certificate	Read-only
0x3D	3	Accessory Certificate Data (Page 13)	128	Certificate	Read-only
0x3E	3	Accessory Certificate Data (Page 14)	128	Certificate	Read-only
0x3F	3	Accessory Certificate Data (Page 15)	128	Certificate	Read-only
0x40	4	Self-test Control/Status	1	0x00	Read/write
0x50	5	iPod Certificate Data Length	2	Undefined	Read/write
0x51	5	iPod Certificate Data (Page 1)	128	Undefined	Read/write
0x52	5	iPod Certificate Data (Page 2)	128	Undefined	Read/write
0x53	5	iPod Certificate Data (Page 3)	128	Undefined	Read/write
0x54	5	iPod Certificate Data (Page 4)	128	Undefined	Read/write
0x55	5	iPod Certificate Data (Page 5)	128	Undefined	Read/write
0x56	5	iPod Certificate Data (Page 6)	128	Undefined	Read/write
0x57	5	iPod Certificate Data (Page 7)	128	Undefined	Read/write
0x58	5	iPod Certificate Data (Page 8)	128	Undefined	Read/write

## Register Descriptions

---

This section describes the ways that the CP registers listed in Table 4-1 are used.

### Device Version

---

The Device Version read-only register contain the version number of the coprocessor device. The current Authentication 2.0B coprocessor is designated as device version 0x03. The previous 2.0A CP is device version 0x02 and the 1.0 CP is device version 0x01.

## Firmware Version

---

The Firmware Version read-only register contains the version number of the coprocessor firmware. Firmware version numbers advance by whole integers.

## Authentication Protocol Major and Minor Versions

---

The Authentication Protocol Major Version and Authentication Protocol Minor Version read-only registers provide the version number of the authentication protocol that the CP supports. This information is accessed by the iAP command `RetDevAuthenticationInfo` during accessory authentication.

## Device ID

---

The Device ID read-only register identifies the accessory and is accessed by the iAP command `SetFIDTokenValues` during accessory identification.

## Error Code

---

The Error Code read-only register stores the most recent communication or authentication process error code generated since the register was last cleared. The error code register is cleared after it is read. The possible error codes are listed in Table 4-2.

**Table 4-2** Error codes

Code	Description
0x00	No error
0x01	Invalid register for read
0x02	Invalid register for write
0x03	Invalid signature length
0x04	Invalid challenge length
0x05	Invalid certificate length
0x06	Internal process error during signature generation
0x07	Internal process error during challenge generation
0x08	Internal process error during signature verification
0x09	Internal process error during certificate validation
0x0A	Invalid process control

Code	Description
0x0B–0xFF	Reserved

If a single communication operation happens to produce multiple errors (for example, by writing an invalid signature length during a multiregister write that also attempts to continue past the end of the corresponding block) then only the highest-numbered error code is stored.

## Authentication Control and Status

The Authentication Control/Status read/write register provides control and status information for the CP's authentication processes.

When read from, the Authentication Control/Status register provides the status of the most recently requested CP process, as shown in Figure 4-1 and Tables 4-3 and 4-4.

**Figure 4-1** Authentication Control/Status register, read-only bits

7	6	5	4	3	2	1	0
ERR_SET	PROC_RESULTS			0	0	0	0

**Table 4-3** Authentication ERR\_SET values

Value	Description
0	No process or communication error is currently stored in the Error Code register
1	The Error Code register contains the most recent process or communication error. Both this bit and the Error Code register itself are cleared after the Error Code register is next read.

**Table 4-4** Authentication PROC\_RESULTS values

Value	Description
0	Most recent process did not produce valid results.
1	Accessory signature successfully generated.
2	Challenge successfully generated.
3	iPod signature successfully verified.
4	iPod certificate successfully validated.
5-7	Reserved

When written to, the Authentication Control/Status register controls the start of CP processes, as shown in Figure 4-2 and Table 4-5.

**Figure 4-2** Authentication Control/Status register, write-only bits



**Note:** Attempts to write to other bits are ignored.

**Table 4-5** Authentication PROC\_CONTROL values

Value	Description
0	No effect
1	Start new signature-generation process
2	Start new challenge-generation process
3	Start new signature-verification process
4	Start new certificate-validation process
5	Force CP to sleep
6-7	Reserved

## Signature Data Length

The Signature Data Length read/write register holds the length in bytes of the results of the most recent signature-generation process (if the iPod is authenticating an accessory) or signature-verification process (if the accessory is authenticating the iPod).

Before a signature-generation process begins, this register should contain 0x80, the maximum allowable signature length. After completion of the signature-generation process, the CP updates this register to contain the actual length of the generated signature. This updated value should be read in order to determine how much of the Signature Data register contains valid signature bytes.

Before a signature-verification process begins, this register should hold the actual length of the signature being verified.

## Signature Data

In the case of a signature-generation process, the Signature Data read/write register holds the newly generated signature. In the case of a signature-verification process, it holds the signature to be verified.

## Challenge Data Length

---

The Challenge Data Length read/write register holds the length, in bytes, of the current challenge. This challenge may either be written into the CP, during iPod authentication of an accessory, or generated by the CP during accessory authentication of an iPod.

Before starting a signature-generation process on the current challenge during iPod authentication of an accessory, this register should contain the length of the challenge.

Before starting a new challenge-generation process during accessory authentication of an iPod, this register should contain the requested challenge length.

The required length of a challenge, whether offered by the iPod or by an accessory, is 20 bytes. This length requirement may not hold in future versions of the authentication protocol.

## Challenge Data

---

The Challenge Data read/write register holds the current challenge. This challenge may either be written into the CP (during iPod authentication of an accessory) or generated by the CP (during accessory authentication of an iPod).

## Accessory Certificate Data Length

---

The Accessory Certificate Data Length read-only register holds the length of the X.509 certificate that the iPod uses to authenticate an accessory. The length of a certificate varies but is always less than or equal to 1920 bytes. This length limit may not hold for future versions of the authentication protocol.

## Accessory Certificate Data

---

The Accessory Certificate Data read-only register holds the X.509 Certificate that the iPod uses to authenticate an accessory. The Accessory Certificate may be read from the coprocessor in 128-byte pages starting at any Accessory Certificate Data Page address, or it may be read in a continuous stream starting at Page 1. Since the length of the Accessory Certificate varies, fewer than all of the pages may be used. The Accessory Certificate Data Length value can be read to determine which Accessory Certificate Data Pages contain the certificate data.

## Self-Test Control and Status

---

The Self-test Control/Status read/write register provides access to the built-in self-test functions of the coprocessor. When it is set to a value of 1, the Self-test Control/Status register initiates a self-test process, as shown in Figure 4-3 and Table 4-6.

**Figure 4-3** Self-test Control/Status register, write-only bits

7	6	5	4	3	2	1	0
0	0	0	0	0	PROC_CONTROL		

**Note:** Attempts to write to other bits are ignored.

**Table 4-6** Self-test PROC\_CONTROL values

Value	Test process to be run
0	None
1	Run X.509 certificate and private key tests
2-7	Reserved

When read from, bits 7–4 of the Self-test Control/Status register report the results of the X.509 certificate and private key tests, as shown in Figure 4-4 and Table 4-7. The CP detects a read cycle and resets the control/status register to 0x00 after it; hence bits 7–4 must all be retrieved in one operation.

**Figure 4-4** Self-test Control/Status register, read-only bits

7	6	5	4	3	2	1	0
Self-Test results				0	0	0	0

**Table 4-7** Self-test result bits

Bit	Test	Bit value	
		0	1
7	X.509 certificate	Certificate not found	Certificate found in memory (see note below)
6	Private key	Private key not found	Private key found in memory (see note below)
5-4	Reserved		

**Note:** The X.509 and private key tests only verify that these elements are present in Flash memory; no authentication is performed.

## iPod Certificate Data Length

The iPod Certificate Data Length register holds the length of the X.509 certificate supplied by the attached iPod. An accessory uses this certificate to authenticate an iPod in both the certificate validation and signature verification processes. The length of an iPod certificate varies but is always less than or equal to 1024 bytes. This length limit may not hold for future versions of the authentication protocol.



## iPod Certificate Data

---

The iPod Certificate Data register holds the X.509 Certificate that an accessory uses to authenticate an iPod in both the certificate validation and signature verification processes. The iPod Certificate may be written to the coprocessor in 128-byte pages starting at any iPod Certificate Data Page address, but it may not be written in a multipage stream. Since the length of the iPod Certificate varies, not all of the pages need to be used. The iPod Certificate Data Length value determines which iPod Certificate Data Pages contain valid certificate data.



# Authentication Data Flows

Authentication involves communication between the accessory controller (AC), the Authentication Coprocessor (CP) in the accessory, and the iPod attached to the accessory.

Communication between the accessory controller and the CP takes place via the transport mode (I<sup>2</sup>C or SPI) described in “[Communication Modes](#)” (page 15). Communication between the accessory controller and the iPod takes place via the iPod Accessory Protocol. See the *iPod Accessory Protocol Interface Specification*, Release R36, for full details.

This chapter summarizes the kinds of information that pass between the AC, the CP, and the attached iPod.

## iPod Authentication of Accessory

The sequence of interactions by which an iPod authenticates an accessory is shown in [Table 5-1](#) (page 27). At the beginning of this process the accessory controller is granted access by iPod to the iAP lingo or lingo; however, if the process does not finish successfully that access is terminated.

**Table 5-1** Sequence of interactions by which an iPod authenticates an accessory

Command or action	Direction	Comments
Read Authentication Protocol Version and Device ID	CP → AC	Accessory controller reads authentication protocol version and device ID from CP
StartIDPS (iAP)	AC → iPod	The accessory controller initiates and completes the Identify Device Preferences and Settings (IDPS) process. It sends the iPod a set of ID tokens, one of which includes the device ID returned by the CP. See <i>iPod Accessory Protocol Interface Specification</i> , Release R36, “Device Signaling and Initialization” in Chapter 5 and “Sample Identification Sequences” in Chapter 6.
SetFIDTokenValues (iAP)	AC → iPod	
EndIDPS (iAP)	AC → iPod	
GetDevAuthenticationInfo (iAP)	iPod → AC	iPod requests device authentication info

Command or action	Direction	Comments
Read Accessory Certificate Length and Data	CP → AC	Accessory controller reads Accessory certificate from CP
RetDevAuthenticationInfo (iAP)	AC → iPod	Accessory controller returns information needed for authentication process, using the authentication protocol version number and X.509 certificate returned by the CP
AckDevAuthenticationInfo (iAP)	iPod → AC	The status of the authentication version comparison is returned to the accessory controller. The returned status includes information about the validity of the X.509 certificate.
GetDevAuthentication-Signature (iAP)	iPod → AC	iPod sends accessory controller a challenge and requests that it provide corresponding digital signature
Write Challenge Length and Challenge Data	AC → CP	Accessory controller writes challenge into CP
Write Authentication Control: PROC_CONTROL = 1	AC → CP	Accessory controller starts signature-generation process in CP
Wait for process completion	CP → AC	Accessory controller waits for CP to finish processing
Read Authentication Status	CP → AC	Accessory controller reads Authentication Status and checks PROC_RESULTS field
Read Signature Data Length and Signature Data	CP → AC	Accessory controller reads signature from CP
RetDevAuthentication-Signature (iAP)	AC → iPod	Accessory controller returns signature to iPod
AckDevAuthenticationStatus (iAP)	iPod → AC	Resulting success or failure of signature verification sent to accessory controller by iPod

## Accessory Authentication of iPod

The sequence of interactions by which an accessory authenticates an iPod is shown in [Table 5-2](#) (page 28).

**Table 5-2** Sequence of interactions by which an accessory authenticates an iPod

Command or action	Direction	Comments
Read Authentication Protocol Version and Device ID	CP → AC	Accessory controller reads authentication protocol version and device ID from CP

Command or action	Direction	Comments
<p>The accessory controller performs the accessory identification and authentication processes listed in <a href="#">Table 5-1</a> (page 27).</p> <p>These processes, by which the iPod authenticates the accessory, must finish successfully before the sequence by which the accessory authenticates the iPod can continue.</p>		
GetiPodAuthenticationInfo (iAP)	AC → iPod	Accessory controller requests iPod authentication information
RetiPodAuthenticationInfo (iAP)	iPod → AC	iPod returns its authentication version and certificate
Write iPod Certificate length and data	AC → CP	Accessory controller writes iPod Certificate into CP
Write Authentication Control: PROC_CONTROL = 4	AC → CP	Accessory controller starts certificate validation process in CP
Wait for process completion	CP → AC	Accessory controller waits for CP to finish processing
Read Authentication Status	CP → AC	Accessory controller reads Authentication Status and checks PROC_RESULTS field
AckiPodAuthenticationInfo (iAP)	AC → iPod	Results of the authentication information comparison are returned to iPod
Write Authentication Control: PROC_CONTROL = 2	AC → CP	Accessory controller starts challenge-generation process in CP to calculate new challenge
Wait for process completion	CP → AC	Accessory controller waits for CP to finish processing
Read Authentication Status	CP → AC	Accessory controller reads the authentication status and checks PROC_RESULTS field
Read Challenge Length and Challenge Data	CP → AC	Accessory controller reads challenge from CP
GetiPodAuthentication-Signature (iAP)	AC → iPod	Accessory controller sends challenge to iPod and requests that iPod calculate digital signature
RetiPodAuthentication-Signature (iAP)	iPod → AC	iPod returns digital signature to Accessory controller
Write Signature Data Length and Signature Data	AC → CP	Accessory controller writes digital signature into CP

Command or action	Direction	Comments
Write Challenge Length and Challenge	AC → CP	Accessory controller writes challenge into CP (it needs to write this into the CP only if the challenge has been changed in the meantime)
Write Authentication Control: PROC_CONTROL = 3	AC → CP	Accessory controller starts signature-verification process in CP
Wait for process completion	CP → AC	Accessory controller waits for CP to finish processing
Read Authentication Status	CP → AC	Accessory controller reads authentication status and checks PROC_RESULTS field
Ack iPodAuthenticationStatus (iAP)	AC → iPod	Signature verification status is returned to iPod.

# I2C Communication Protocol

---

When configured for I<sup>2</sup>C mode, the iPod Authentication Coprocessor (CP) acts as an I<sup>2</sup>C slave.

I2C\_SCL is the I<sup>2</sup>C clock line and is usually driven by the accessory controller. I2C\_SDA is the I<sup>2</sup>C data line and is driven by whichever device is currently sending data. The CP may perform I<sup>2</sup>C slave clock synchronization by stretching I2C\_SCL, so the accessory controller must allow for this possibility.

The maximum supported I<sup>2</sup>C clock rate is 50 kHz. If the I<sup>2</sup>C bus is shared with other devices, the CP must either be put in Sleep mode or held in reset status during any communication that exceeds this rate.

## Slave Selection and Reset

---

During reset, the MODE1 pin must be held high for at least 30 ms to select I<sup>2</sup>C operation, as described in [“Communication Mode Selection”](#) (page 12). As an I<sup>2</sup>C slave, the CP is then selected in-band via its I<sup>2</sup>C address. The least significant bit of the I<sup>2</sup>C slave address controls whether a write or a read operation is to be performed, as described in [“Communication Modes”](#) (page 15).

## Coprocessor Busy

---

When the CP is busy processing it is unable to handle incoming communication attempts. If the coprocessor does not ACK its slave address during an attempted I<sup>2</sup>C communication, then the coprocessor is busy. The accessory controller must repeatedly attempt communication until the coprocessor sends an ACK after receiving its slave address.

## Writing to the Coprocessor

---

To write data to the coprocessor, follow these steps:

1. Send the I<sup>2</sup>C start sequence.
2. Send the I<sup>2</sup>C write address of the CP.
3. Check for an ACK from the slave; if it is not received, loop back to Step 1.
4. Send the register address at which to begin writing.
5. Send the data bytes.
6. Send the I<sup>2</sup>C stop sequence.

## Reading from the Coprocessor

---

To read data from the coprocessor, follow these steps:

1. Send the I<sup>2</sup>C start sequence.
2. Send the I<sup>2</sup>C write address of the CP.
3. Check for an ACK from the slave; if it is not received, loop back to Step 1.
4. Send the register address at which to begin reading.
5. Optional: send the I<sup>2</sup>C stop sequence.
6. Send the I<sup>2</sup>C start sequence.
7. Send the I<sup>2</sup>C read address of the CP.
8. Check for an ACK from the slave; if it is not received, loop back to Step 6.
9. Read the data bytes.
10. Send the I<sup>2</sup>C stop sequence.

Any additional reads after an I<sup>2</sup>C read stop sequence continue with the byte following the previous byte read until an invalid register address or an end of block is reached, at which point the slave returns 0xFF in response to all further reads.



# SPI Communication Protocol

When configured for SPI mode, the iPod Authentication Coprocessor (CP) acts as an SPI slave.

The SPI clock (SPI\_CLK) controls data transfer on the master-to-slave (SPI\_SIMO) and slave-to-master (SPI\_SOMI) data lines; it must be driven by the accessory controller.

The maximum supported SPI\_CLK rate is 75 kHz.

## Slave Selection and Reset

To select SPI mode, both the MODE1 and MODE0 pins must be held low for at least 30 ms during reset, as described in “Communication Mode Selection” (page 12).

Before attempting to communicate with the CP via SPI, the accessory controller must ensure that the SPI slave-select pin (SPI\_nSS) is low.

When SPI\_nSS is low, the CP drives SPI\_SOMI. When SPI\_nSS is high, the CP leaves SPI\_SOMI undriven and ignores any activity on SPI\_CLK and SPI\_SIMO.

After completing a transaction, the accessory controller may return SPI\_nSS high, but it is not required to do so. A rising-edge signal on SPI\_nSS causes the CP to reset its SPI module. If the CP is the only SPI slave in the accessory, SPI\_nSS may be tied directly to ground.

If SPI\_nSS is not tied to ground, its timing relations with SPI\_SOMI during a typical SPI transaction are as shown in Figure 7-1. The  $T_{\text{SOMI\_READY}}$  and  $T_{\text{SOMI\_RELEASE}}$  times are shown in Table 7-1.

**Figure 7-1** SPI\_nSS timing

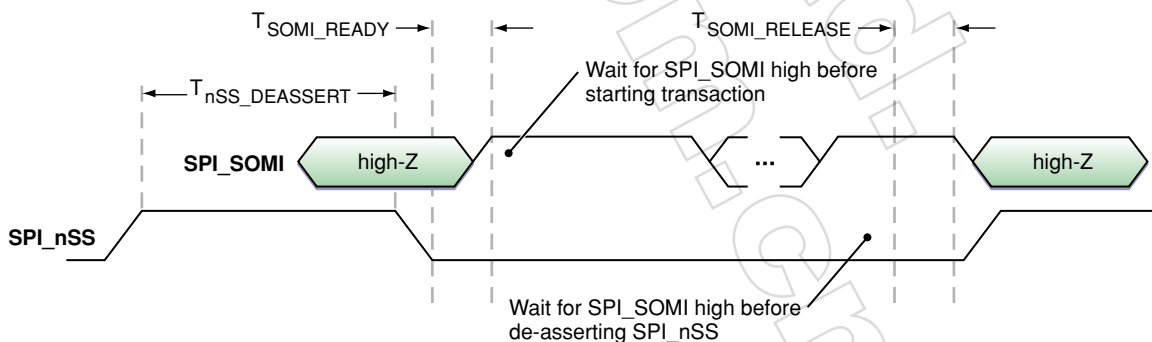


Table 7-1 lists the maximum values of various delays during SPI transactions by the CP. The accessory controller should wait for at least these times at the appropriate stages of each transaction.

**Table 7-1** Maximum SPI transaction delay times

Name	Time	Description
T <sub>SOMI_READY</sub>	50 $\mu$ s	Delay before SPI_SOMI indicates the ready status of the coprocessor
T <sub>SOMI_RELEASE</sub>	50 $\mu$ s	Delay between deasserting SPI_nSS and SPI_SOMI becoming a high-impedance input
T <sub>nSS_DEASSERT</sub>	300 $\mu$ s	Minimum time between de-asserting and re-asserting SPI_nSS.

## Timing and Polarity

---

The CP latches the state of SPI\_SIMO on the falling edge of SPI\_CLK. The accessory controller should update SPI\_SIMO on the rising edge of SPI\_CLK.

When SPI\_nSS is low, the CP updates SPI\_SOMI on the rising edge of SPI\_CLK. The accessory controller should latch SPI\_SOMI on the falling edge of SPI\_CLK.

For both SPI\_SIMO and SPI\_SOMI, the most significant bit of a data byte is the first to be transmitted.

## Coprocessor Busy

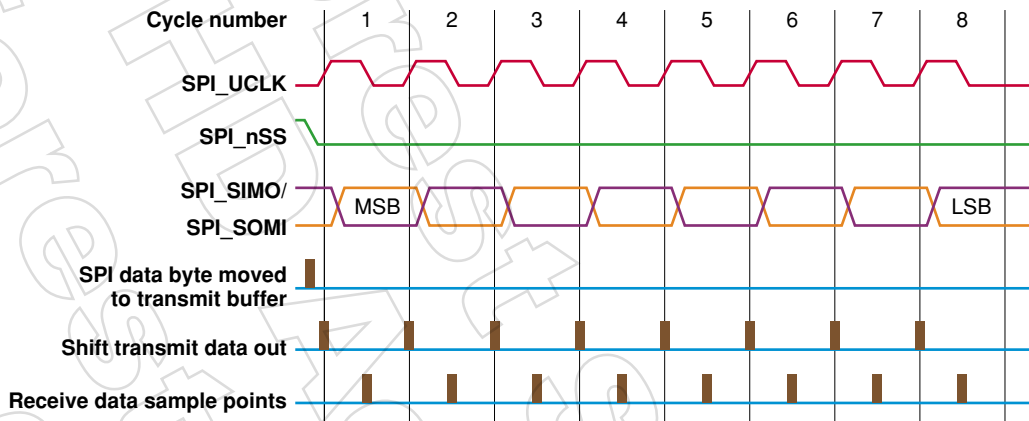
---

When the coprocessor is busy processing it is unable to handle incoming communication attempts. In SPI mode, the coprocessor uses its SPI\_SOMI line to indicate when it is ready to communicate. SPI\_SOMI is set low when the coprocessor is busy and set high when the coprocessor is ready for further communication.

Before starting a new SPI transaction, the accessory controller must wait for SPI\_SOMI to be set high. Once SPI\_SOMI has been set high, the accessory controller may transmit the command and length bytes. After receiving the command and length bytes, the coprocessor will be busy preparing for the transaction. The coprocessor sets the SPI\_SOMI line high when it is ready to continue with the data byte portion of the transaction.

The overall SPI data transmission timing is shown in [Figure 7-2](#) (page 35).

**Figure 7-2** SPI data transmission timing

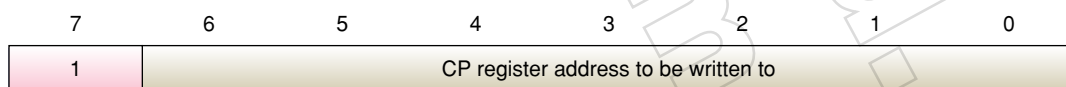


## Writing to the Coprocessor

To write data to the CP using SPI, follow these steps:

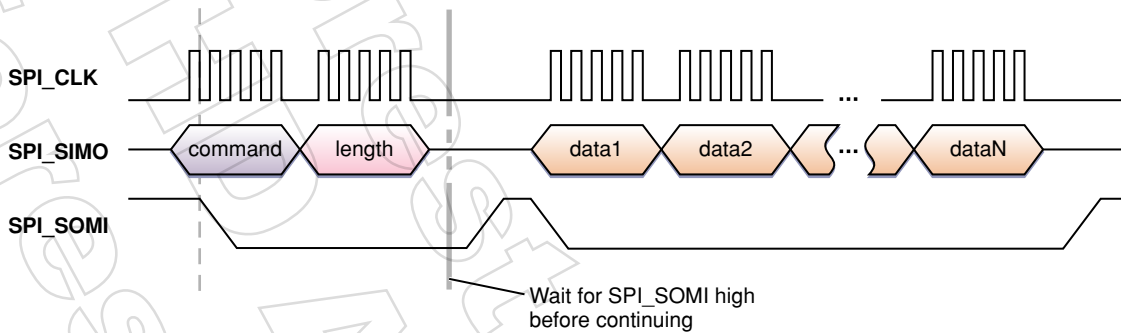
1. Set SPI\_nSS low and wait for the  $T_{SOMI\_READY}$  delay time before continuing (see [Table 7-1](#) (page 34)).
2. Wait for SPI\_SOMI to go high.
3. Send the command byte on SPI\_SIMO. This byte consists of a write bit plus the register address; see [Figure 7-3](#). SPI\_SOMI goes low after the first bit.
4. Send the length byte on SPI\_SIMO.
5. Wait for SPI\_SOMI to go high.
6. Send the data bytes on SPI\_SIMO; SPI\_SOMI goes low after the first bit.
7. Wait for the  $T_{SOMI\_READY}$  delay time before continuing (see [Table 7-1](#) (page 34)).
8. Wait for SPI\_SOMI to go high.
9. Optional: set SPI\_nSS high.

**Figure 7-3** Command byte that starts an SPI write action to the CP



The overall timing of an SPI write transaction is shown in [Figure 7-4](#) (page 36).

**Figure 7-4** Coprocessor write timing



## Reading from the Coprocessor

To read data from the CP using SPI, follow these steps:

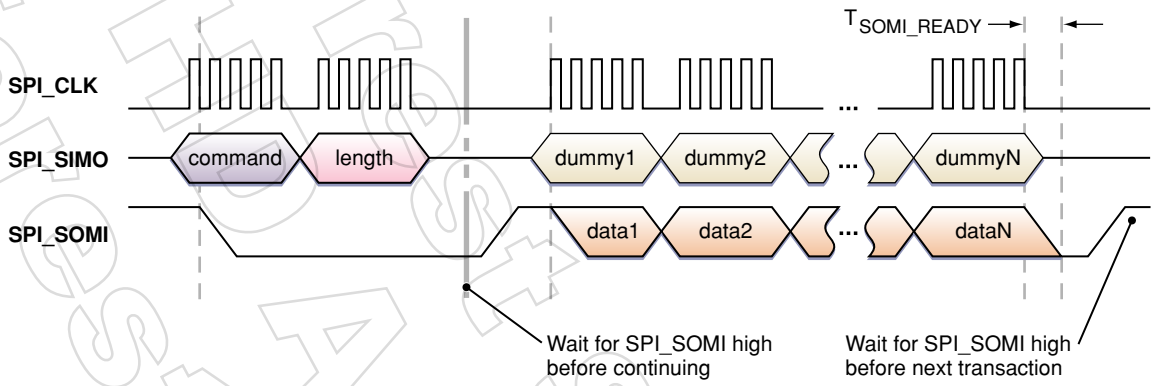
1. Set SPI\_nSS low and wait for the  $T_{\text{SOMI\_READY}}$  delay time before continuing (see [Table 7-1](#) (page 34)).
2. Wait for SPI\_SOMI to go high.
3. Send the command byte on SPI\_SIMO. This byte consists of a read bit plus the register address; see [Figure 7-5](#). SPI\_SOMI goes low after the first bit.
4. Send the length byte on SPI\_SIMO.
5. Wait for SPI\_SOMI to go high.
6. Send a number of dummy bytes on SPI\_SIMO equal to the number of data bytes to be read. While the dummy bytes are being clocked out, read the incoming data bytes on SPI\_SOMI.
7. Wait for the  $T_{\text{SOMI\_READY}}$  delay time before continuing (see [Table 7-1](#) (page 34)).
8. Wait for SPI\_SOMI to go high.
9. Optional: set SPI\_nSS high.

**Figure 7-5** Command byte that starts a read action from the CP



The overall timing of an SPI read transaction is shown in [Figure 7-6](#) (page 37).

Figure 7-6 Coprocessor read timing





# CP Device Characteristics

This chapter provides technical details and tolerances for the Apple iPod Authentication Coprocessor 2.0B (CP) chip.

## Maximum Environmental Conditions

Table 8-1 lists the CP's absolute maximum electrical and free-air temperature ranges. Stresses to the CP chip beyond the ranges listed in Table 8-1 may cause permanent damage. Exposure to either end of any range for extended periods may affect device reliability.

**Table 8-1** Maximum electrical and temperature ranges

Condition	Maximum range
Voltage applied at $V_{CC}$ relative to $V_{SS}$	-0.3 V to +7.0 V
Voltage applied to any pin	-0.3 V to $V_{CC} + 0.3$ V
Storage temperature	-55 °C to +85 °C

## Recommended Operating Conditions

The CP is available in both standard (STD) and wide temperature range (WTR) configurations. Internal sensors force it to its reset state if any of the conditions listed in Table 8-2 are exceeded. Attempting to operate the CP in this state is not recommended and may lead to device failure or unreliability.

**Table 8-2** Recommended operating conditions

Condition	Minimum	Maximum	Unit
STD configuration operating free-air temperature	-25	+85	°C
WTR configuration operating free-air temperature	-40	+85	°C
Supply voltage during program execution, STD or WTR	1.8	3.6	V

## DC Electrical Characteristics

Tables 8-3 through 8-5 show the DC electrical characteristics of the CP chip over its recommended voltage and temperature ranges. Unless otherwise specified in these tables,  $V_{CC} = 1.8$  to  $3.6$  V; for the STD configuration,  $T_A = -25$  °C to  $+85$  °C and for the WTR configuration,  $T_A = -40$  °C to  $+85$  °C.

**Table 8-3** Supply current into  $V_{CC}$ , excluding external current

Parameter	Test conditions	Minimum	Typical	Maximum	Unit
$I_{(AM)}$ Active mode (authentication process running)				7.5	mA
$I_{(sleep)}$ Sleep mode	$T_A \leq 50$ °C			100	$\mu$ A
	$T_A > 50$ °C			200	

**Table 8-4** Inputs

Symbol	Parameter	Test conditions	Minimum	Typical	Maximum	Unit
$V_{IH}$	High-level input voltage	$V_{CC} = 2.2$ to $3.6$	$V_{CC} \times 0.7$		$V_{CC} + 0.3$	V
		$V_{CC} = 1.8$ to $2.2$	$V_{CC} \times 0.85$			
$V_{IL}$	Low-level input voltage	$V_{CC} = 2.2$ to $3.6$	-0.3		$V_{CC} \times 0.2$	
		$V_{CC} = 1.8$ to $2.2$		0.2		
$I_p$	nRESET pullup	$V_{IN} = 0$ V			150	$\mu$ A
$I_{lkg}$	Leakage current	$V_{IN} = 0.5$ to $V_{CC} - 0.5$ V			10	

**Table 8-5** Outputs

Symbol	Parameter	Test conditions	Minimum	Typical	Maximum	Unit
$V_{OH}$	High-level output voltage	$I_{OH} = +200$ $\mu$ A;	$V_{CC} \times 0.7$		$V_{CC}$	V
$V_{OL}$	Low-level output voltage	$I_{OL(max)} = -1$ mA;	$V_{SS}$		$V_{SS} + 0.4$	



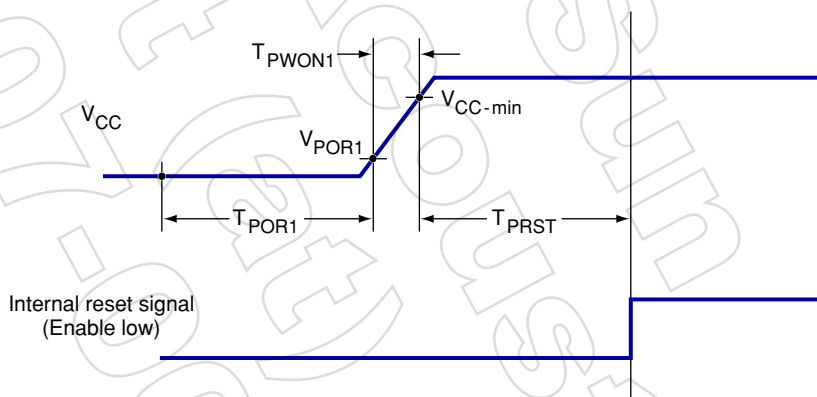
## Timing Characteristics

This section documents the typical timing characteristics of the CP's internal and external resets and its I/O inputs. In all cases,  $V_{CC} = 1.8$  to  $3.6$  V; for the STD configuration,  $T_A = -25$  °C to  $+85$  °C and for the WTR configuration,  $T_A = -40$  °C to  $+85$  °C.

Figure 8-1 illustrates the timing of the CP's internal reset during a typical power-on sequence. In the diagram,  $T_{POR1}$  represents the minimum time during which external power is held below  $V_{POR1}$ .

Table 8-6 lists the parameter values in Figure 8-1.

**Figure 8-1** Typical power-on reset timing and voltage limits

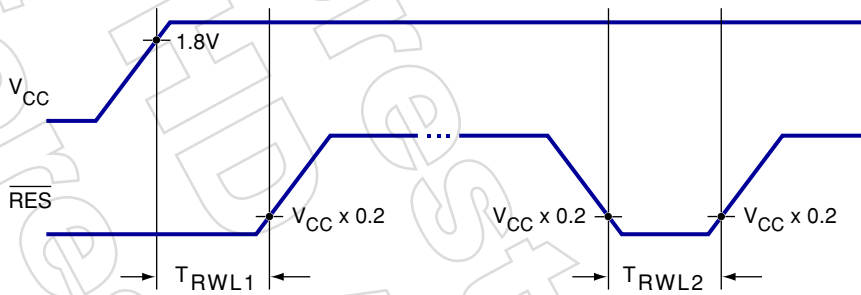


**Table 8-6** Values for Figure 8-1

Symbol	Description	Maximum value	Test condition
$V_{POR1}$	Power-on reset valid voltage	0.1 V	
$T_{PWON1}$	Supply voltage rise time when power-on reset is cancelled	0.5 ms	$T_{POR1} \geq 1$ sec
		1 ms	$T_{POR1} \geq 10$ sec
$T_{PRST}$	Internal reset signal release time	500 $\mu$ s	

Figure 8-2 illustrates a typical externally-controlled reset sequence, both immediately after power-up and at an arbitrary later time while power is on. Table 8-7 lists the parameter values in Figure 8-2.

**Figure 8-2** Typical external reset timing and voltage limits

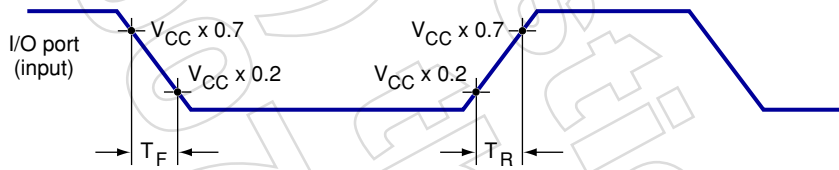


**Table 8-7** Values for Figure 8-2

Symbol	Description	Minimum value
$T_{RLW1}$	Reset pulse width, cold reset	500 $\mu$ s
$T_{RLW2}$	Reset pulse width, warm reset	200 $\mu$ s

Figure 8-3 illustrates the CP's typical I/O port input signal timing and voltage limits. Table 8-8 lists the parameter values in Figure 8-3.

**Figure 8-3** Typical I/O port input waveform



**Table 8-8** Values for Figure 8-3

Symbol	Description	Maximum value
$T_F$	Fall time	1.0 $\mu$ s
$T_R$	Rise time	1.0 $\mu$ s

## Mechanical Package Characteristics

The 2.0B CP is available in two packages: no-lead QFN-20 and SOP-8. The QFN-20 package is shown in [Figure 8-4](#) (page 43) and its dimensions in millimeters are listed in [Table 8-9](#) (page 43). The SOP-8 package is shown in [Figure 8-5](#) (page 44) and its dimensions in millimeters are listed in [Table 8-10](#) (page 44). These drawings and their dimensions are subject to change without notice.

Figure 8-4 2.0B iPod Authentication Coprocessor QFN-20 package

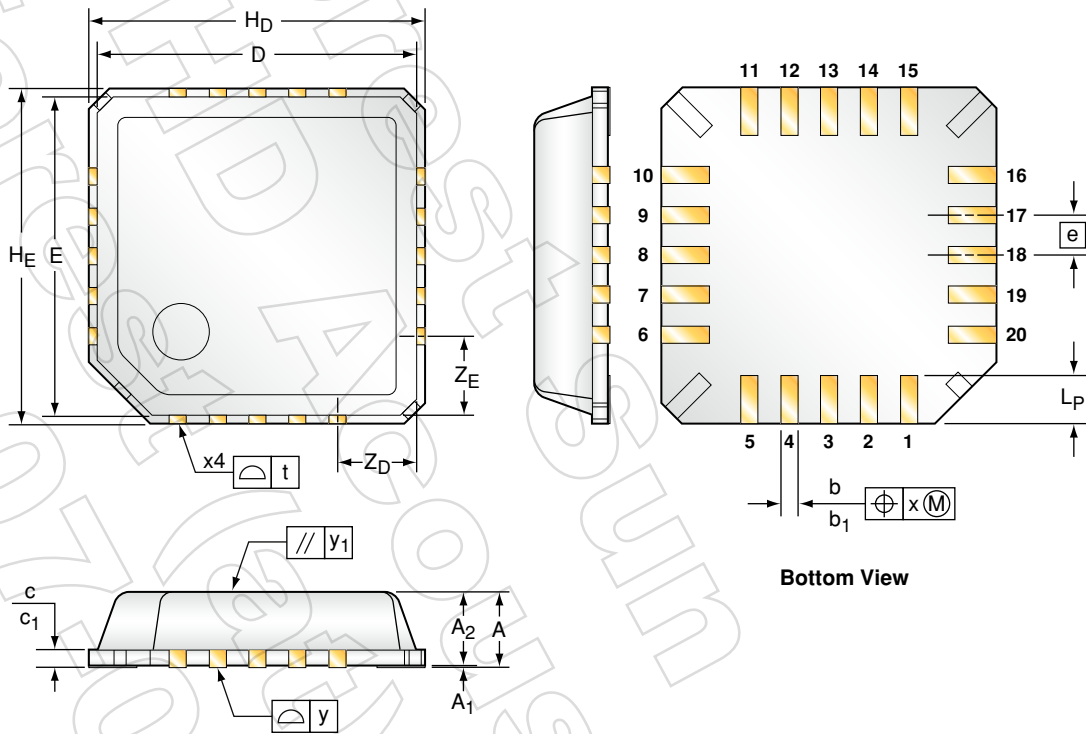


Table 8-9 QFN-20 package dimensions in millimeters

Symbol	Minimum	Nominal	Maximum	Notes
D		4.0		
E		4.0		
A <sub>2</sub>		0.89		
A			0.95	
A <sub>1</sub>	0.005	0.02	0.04	
b	0.17	0.22	0.27	Including plating thickness
b <sub>1</sub>	0.17	0.20	0.23	Base material dimension
e		0.5		
L <sub>p</sub>	0.50	0.60	0.70	
x			0.05	
y			0.05	
y <sub>1</sub>			0.20	
t			0.20	

Symbol	Minimum	Nominal	Maximum	Notes
$H_D$		4.2		
$H_E$		4.2		
$Z_D$		1.0		
$Z_E$		1.0		
c	0.17	0.22	0.25	Including plating thickness
$c_1$	0.17	0.20	0.23	Base material dimension
Mass		0.04 g		

Figure 8-5 2.0B iPod Authentication Coprocessor SOP-8 package

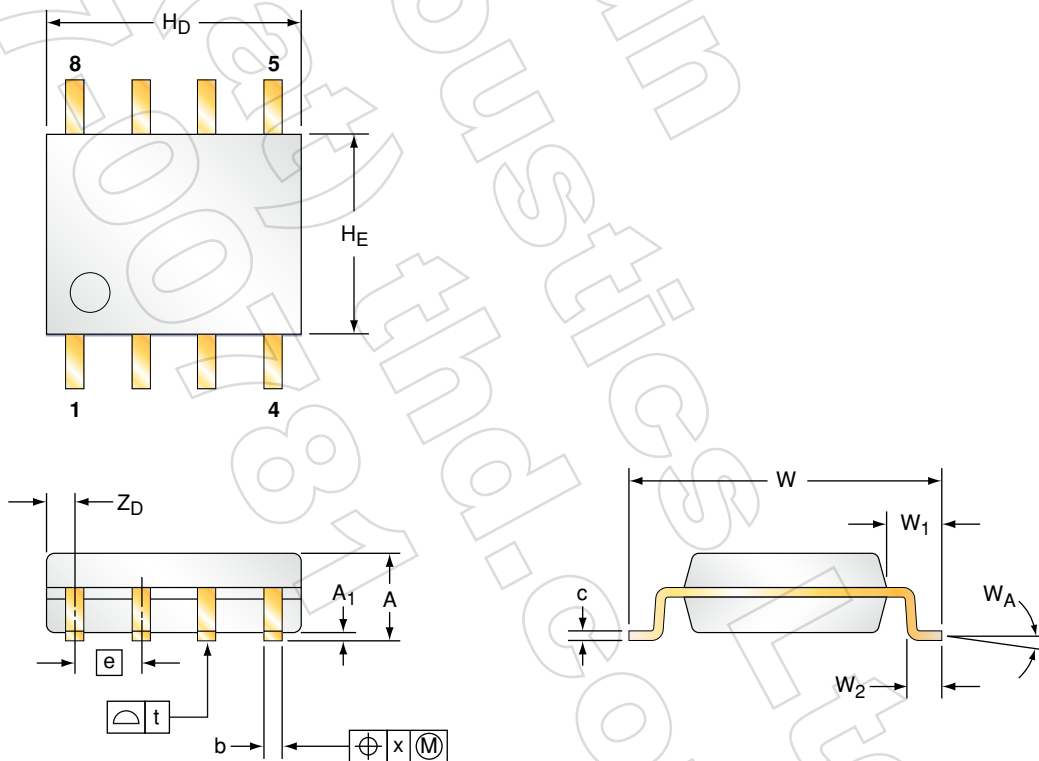


Table 8-10 SOP-8 package dimensions in millimeters

Symbol	Minimum	Nominal	Maximum	Notes
A			1.73	
$A_1$	0.102	0.14	0.154	
b	0.35	0.40	0.45	Palladium plated

**C H A P T E R 8**  
**CP Device Characteristics**

Symbol	Minimum	Nominal	Maximum	Notes
e		1.27		
x		0.25		
t		0.10		
H <sub>D</sub>		4.89	5.15	
H <sub>E</sub>		3.90		
Z <sub>D</sub>			0.69	
c	0.15	0.20	0.25	Palladium plated
W	5.84	6.02	6.20	
W <sub>1</sub>		1.06		
W <sub>A</sub>	0°		8°	
W <sub>2</sub>	0.406	0.60	0.889	
Mass		0.08 g		

Apple  
Acoustics  
Sun  
Apple.com

# Document Revision History

This table describes the changes to *iPod Authentication Coprocessor 2.0B Specification*.

Date	Notes
2009-07-27	<i>Release R5:</i>
	Updated <a href="#">Table 5-1</a> (page 27) and <a href="#">Table 5-2</a> (page 28) to conform to current IDPS and authentication processes (see <i>iPod Accessory Protocol Interface Specification</i> , Release R36, Chapter 5 and Appendix B).
2008-01-16	<i>Release R4:</i>
	Added documentation for the SOP-8 package and WTR (wide temperature range) configurations of the CP.
	Added T <sub>nSS_DEASSERT</sub> timing to <a href="#">“Slave Selection and Reset”</a> (page 33).
	Increased the maximum supported I <sup>2</sup> C and SPI clock rates.
2007-05-21	<i>Release R3:</i>
	Removed references to Verification/Validation Status register (no longer used).
2007-05-14	<i>Release R2:</i>
	Added Device Version register (Table 4-1).
	Renamed communication mode selection and configuration pins (now MODE1 and MODE0).
	Added new section <a href="#">“Communication Mode Selection”</a> (page 12).
	Added sleep function to Authentication Control/Status Register.
	Limited iPod certificate data to 1024 bytes (8 pages).
	Modified process for accessory authentication of iPod.
	Provided values for maximum SPI transaction delay times (Table 7-1).

# REVISION HISTORY

## Document Revision History

Date	Notes
	Widened storage temperature range (Table 8-1).
	Changed maximum supply current values (Table 8-3).
2007-03-29	<i>Release R1</i> : Initial publication.