# 3. Apple Authentication Coprocessor 2.0C

## 3.1 Coprocessor 2.0C Overview

An Apple device verifies whether a third-party accessory attached to it is authorized for use with the Apple device by issuing an authentication challenge to the accessory. The accessory must respond to the Apple device's challenge, and it can do so only with the assistance of an Apple Authentication Coprocessor (CP) chip located in the accessory. Conversely, the accessory can use its CP chip to authenticate the Apple device.

Earlier versions of the Apple Authentication Coprocessor (1.0, 2.0A, and 2.0B) were implemented in QFN-40, QFN-20, and SOP-8 packages. The current version, 2.0C, is supplied in a smaller and more efficient PG-USON-8-1 package.

The Export Classification Control Number (ECCN) of the Apple Authentication Coprocessor 2.0C is 5A992 NLR.

## 3.2 Coprocessor 2.0C Authentication Protocol

The authentication protocol supported by the Apple Authentication Coprocessor 2.0C 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 accessory authentication of the Apple device, refer to Accessory Authentication (page 261).

For information about Apple device authentication of the accessory, refer to Device Authentication (page 523).

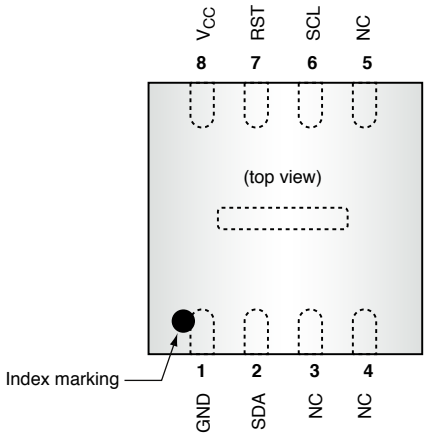
## 3.3 Coprocessor 2.0C Signals and Pinouts

The 2.0C CP chip signal descriptions are given in Table 3-1 (page 67) and its pinouts are shown in Figure 3-1 (page 67).

**Table 3-1** Coprocessor signals

| Signal name | Pin | I/O | Description |
|---|---|---|---|
| GND | 1 | | Supply voltage, negative terminal |
| SDA | 2 | I/O | I2C data |
| NC | 3-5 | | Must not be connected |
| SCL | 6 | I | I2C clock |
| RST | 7 | I | At reset: selects I2C slave address. During operation: CP warm reset |
| $V_{CC}$ | 8 | | Supply voltage, positive terminal |

**Figure 3-1** Coprocessor pinout, top view




**PG-USON-8-1 package**

The thermal pad on the bottom of the CP may be left unconnected or connected to GND.

## 3.4 Coprocessor 2.0C Address Selection

After power-up or in response to a warm reset, the state of RST is used to select the CP's I2C slave addresses, as shown in Table 3-2 (page 67).

**Table 3-2** Coprocessor address selection signals

| RST state | I2C write address | I2C read address |
|---|---|---|
| 0 | 0x20 | 0x21 |

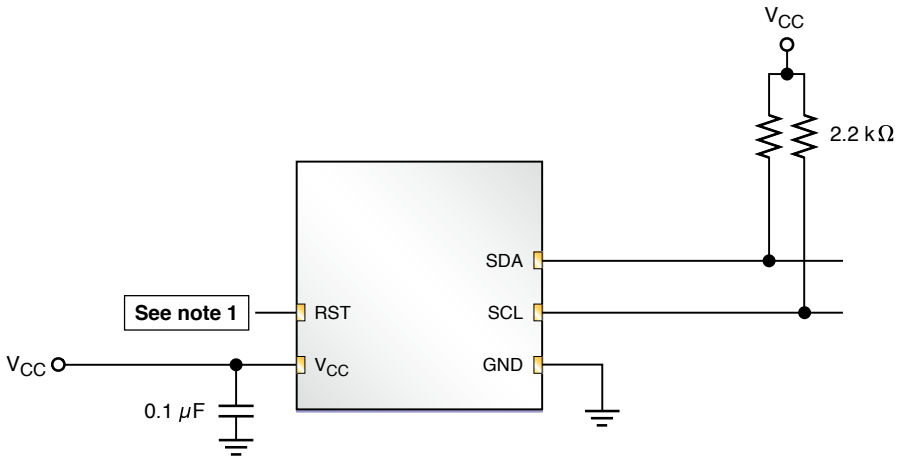
| RST state | I2C write address | I2C read address |
|---|---|---|
| 1 | 0x22 | 0x23 |

See I2C Communications Process (page 71) for the interface requirements of the CP's I2C slave communication transport.

## 3.5 Coprocessor 2.0C Reference Circuit

The reference circuit for I2C operation of the CP is shown in Figure 3-2 (page 68).

**Figure 3-2** Coprocessor reference circuit diagram




**Note:** If the CP's warm reset function is not needed, RST can be tied to either $V_{CC}$ or GND, depending on which of the addressing modes shown in Table 3-2 (page 67) is used. If the warm reset function is needed, RST should be connected to a general-purpose I/O line on the accessory's controller. For further details, see I2C Startup On Warm Reset (page 70).

## 3.6 Coprocessor 2.0C System Voltage

The 2.0C CP may be used either in an accessory powered by an attached Apple device or in an accessory that has its own power source.

# 3.7 Coprocessor 2.0C I2C Interface

The CP's I2C communication interface can be started up either by supplying power to the $V_{CC}$ line or by performing a warm reset on the RST line. The accessory actions required for these two procedures are specified in the next sections.

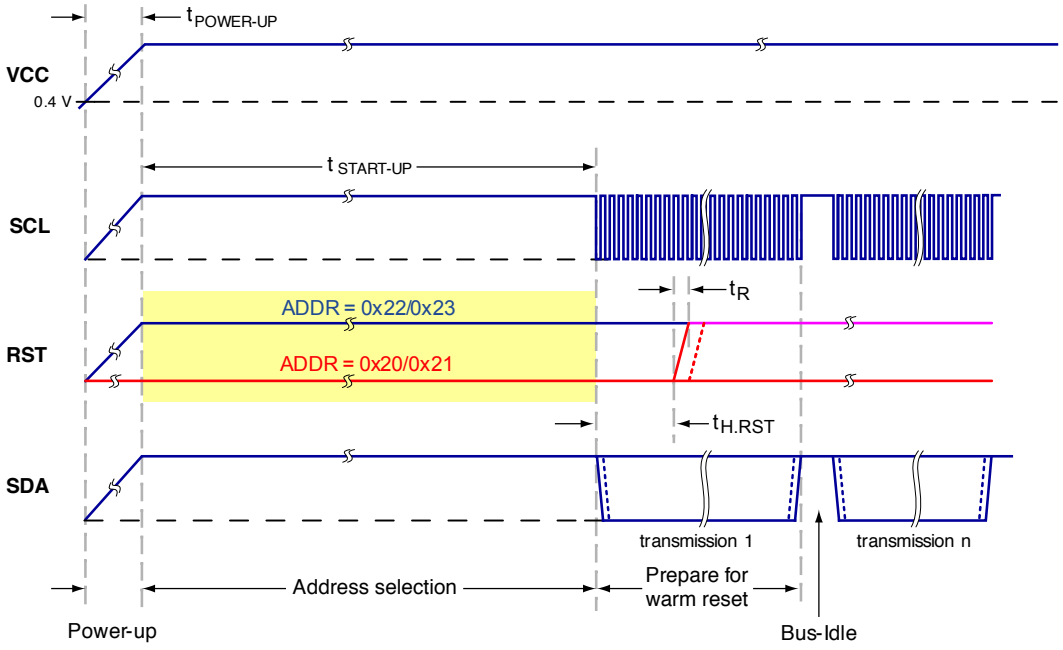
## 3.7.1 I2C Startup On Power On

To activate the I2C interface by supplying power to the $V_{CC}$ line, the accessory must perform the following startup procedure. This procedure is required both to support address selection by means of the RST line and to support the option of a warm reset later.

- The $V_{CC}$ line must be supplied with power and the SDA and SCL lines must be set high during the entire procedure.
- The RST line, used to select addressing as described in Coprocessor 2.0C Address Selection (page 67), must be kept either low or high during the entire procedure. If the RST line is kept low during the procedure, the accessory must set it high not earlier than 10 *ms* after the $V_{CC}$ line goes high but before the first data transmission occurs.
- The first data transmission may start not earlier than 10 *ms* after the $V_{CC}$ line goes high. If the RST line has been kept low and the accessory might need to perform a warm reset of the CP chip later, the accessory must set the RST line high not earlier that 1 *ms* after the start of the first data transmission ($t_{H.RST}$ interval in Figure 3-3 (page 70)). If the option of a warm reset later is not needed, the accessory may tie RST directly to either $V_{CC}$ or GND.

Figure 3-3 (page 70) diagrams the timing of the I2C interface when it is started up by turning power on.

**Figure 3-3** Coprocessor I2C power on timing




In this diagram, $t_{STARTUP} \geq 10\ ms$ and $t_{H.RST} \geq 1\ ms$. The rise time of $t_R$ and the fall time of $t_F$ are both $< 1\ \mu s$ from 10% to 90% of the signal amplitude, and $t_{POWER\text{-}UP} < 200\ \mu s$ from $V_{CC} = 0.4$ V until $V_{CC} = 90\%$ of the target supply voltage.

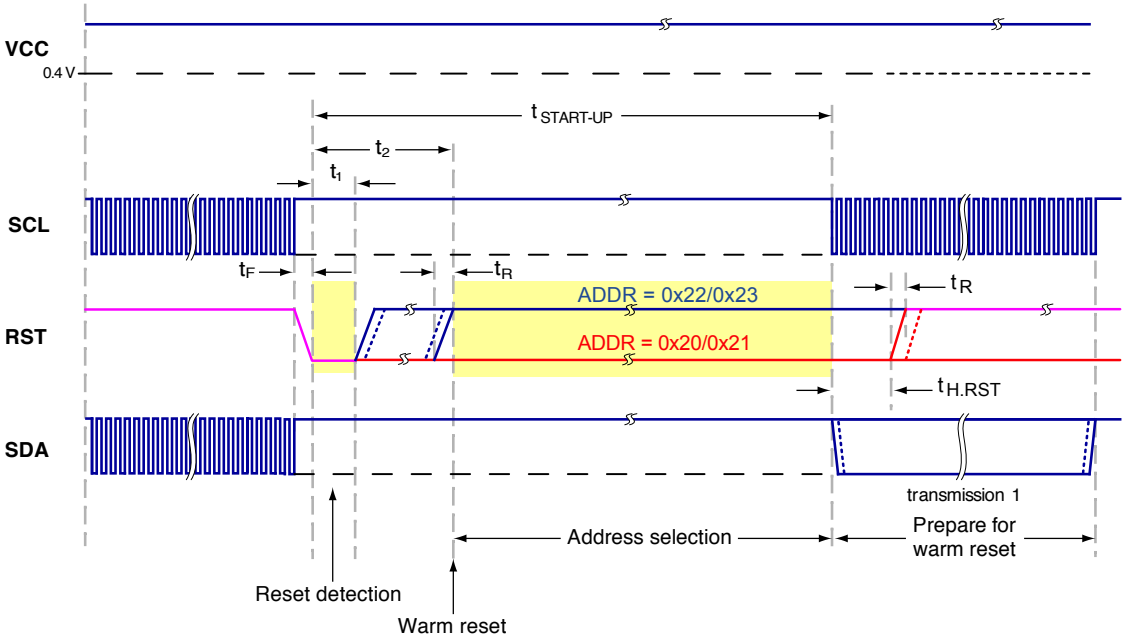
## 3.7.2 I2C Startup On Warm Reset

To reset the I2C interface through the RST line, after activating it through power-up as specified in I2C Startup On Power On (page 69), the accessory must perform the following procedure:

- The $V_{CC}$ line must be supplied with power during the entire procedure.
- The terminal must halt I2C communication, and the SDA and SCL lines must be set high before the RST line is set low.
- The RST line must be set low and kept low for at least 10 µs. Not later than 1 *ms* after the falling edge of the RST signal, the accessory must finish its I2C address selection by either keeping RST low or driving RST high. If the RST line is kept low during the warm reset, the accessory must set it high not earlier than 10 *ms* after the $V_{CC}$ line goes high but before the first data transmission occurs.
- The first data transmission may start not earlier than 10 *ms* after the falling edge of the RST signal. If the RST line has been kept low during the warm reset, the accessory must set it high not earlier that 1 *ms* after the start of the first data transmission ($t_{H.RST}$ interval in Figure 3-4 (page 71)).

Figure 3-4 (page 71) diagrams the timing of the I2C interface when it is reset by software toggling the RST line without a power off/on cycle.

**Figure 3-4** Coprocessor I2C warm reset timing




In this diagram, $t_{STARTUP} \geq 10$ ms, $t_{H.RST} \geq 1$ ms, $t_1 > 10\ \mu s$, and $t_2 = 3\ ms$. The rise time of $t_R$ and the fall time of $t_F$ are both $< 1\ \mu s$ from 10% to 90% of the signal amplitude.

## 3.7.3 I2C Communications Process

When the CP is addressed using I2C, it acts as a standard 7-bit I2C slave. The I2C slave address is configured upon reset and is based on the RST input. The I2C effective slave address for writing is shown in Figure 3-5 (page 71) and the corresponding read address in Figure 3-6 (page 71).

**Figure 3-5** Coprocessor I2C slave write address

| A6 | A5 | A4 | A3 | A2 | A1 | A0 | R/nW |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | RST | 0 |

**Figure 3-6** Coprocessor I2C slave read address

| A6 | A5 | A4 | A3 | A2 | A1 | A0 | R/nW |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | RST | 1 |

In I2C mode, the CP has both a write address and a read address, as is typical for an I2C device. The I2C write address of the CP consists of the seven bits [A6:A0] followed by 0 for the R/nW bit. The I2C read address of the CP consists of the seven bits [A6:A0] followed by 1 for the R/nW bit. If the RST 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.

### 3.7.4 I2C Sleep Mode

The 2.0C CP conserves power by entering a Sleep mode. It enters this mode automatically and cannot be forced to it externally. When in Sleep mode, the CP automatically wakes in response to any I2C communications sent to its address.

## 3.8 Coprocessor 2.0C Registers

Registers within the Apple Authentication Coprocessor 2.0C (CP) are accessed via I2C transport, as described in I2C Communications Process (page 71). This section specifies the CP's register addressing details and telegram formats.

### 3.8.1 Register Addresses

Registers and their addresses in the CP are listed in Table 3-3 (page 72). 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. Registers must not be written to sequentially except as noted. 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 3-3** Coprocessor register map

| Address | Block | Name | Bytes | Reset Value | Access |
|---|---|---|---|---|---|
| 0x00 | 0 | Device Version | 1 | 0x05 | Read-only |
| 0x01 | 0 | Firmware Version | 1 | 0x01 | Read-only |
| 0x02 | 0 | Authentication Protocol Major Version | 1 | 0x02 | Read-only |

| Address | Block | Name | Bytes | Reset Value | Access |
|---|---|---|---|---|---|
| 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 |
| 0x10 | 1 | Authentication Control and Status | 1 | 0x00 | Read/write |
| 0x11 | 1 | Challenge Response Data Length | 2 | 128 | Read/write |
| 0x12 | 1 | Challenge Response Data | 128 | Undefined | Read/write |
| 0x20 | 2 | Challenge Data Length | 2 | 20 | Read/write |
| 0x21 | 2 | Challenge Data | 128 | Undefined | Read/write |
| 0x30 | 3 | Accessory Certificate Data Length | 2 | ≤ 1280 | Read-only |
| 0x31 | 3 | Accessory Certificate Data (Part 1) | 128 | Certificate | Read-only |
| 0x32 | 3 | Accessory Certificate Data (Part 2) | 128 | Certificate | Read-only |
| 0x33 | 3 | Accessory Certificate Data (Part 3) | 128 | Certificate | Read-only |
| 0x34 | 3 | Accessory Certificate Data (Part 4) | 128 | Certificate | Read-only |
| 0x35 | 3 | Accessory Certificate Data (Part 5) | 128 | Certificate | Read-only |
| 0x36 | 3 | Accessory Certificate Data (Part 6) | 128 | Certificate | Read-only |
| 0x37 | 3 | Accessory Certificate Data (Part 7) | 128 | Certificate | Read-only |
| 0x38 | 3 | Accessory Certificate Data (Part 8) | 128 | Certificate | Read-only |

| Address | Block | Name | Bytes | Reset Value | Access |
|---|---|---|---|---|---|
| 0x39 | 3 | Accessory Certificate Data (Part 9) | 128 | Certificate | Read-only |
| 0x3A | 3 | Accessory Certificate Data (Part 10) | 128 | Certificate | Read-only |
| 0x40 | 4 | Self-Test Control and Status | 1 | 0x00 | Read/write |
| 0x41-0x4C | 4 | Reserved | | | |
| 0x4D | 4 | System Event Counter (SEC) | 1 | Undefined | Read-only |
| 0x4E | 4 | Accessory Certificate Serial Number | 31 | Null-terminated string | Read-only |
| 0x50 | 5 | Apple Device Certificate Data Length | 2 | 0x0000 | Read-only |
| 0x51 | 5 | Apple Device Certificate Data (Part 1) | 128 | Undefined | Read/write |
| 0x52 | 5 | Apple Device Certificate Data (Part 2) | 128 | Undefined | Read/write |
| 0x53 | 5 | Apple Device Certificate Data (Part 3) | 128 | Undefined | Read/write |
| 0x54 | 5 | Apple Device Certificate Data (Part 4) | 128 | Undefined | Read/write |
| 0x55 | 5 | Apple Device Certificate Data (Part 5) | 128 | Undefined | Read/write |
| 0x56 | 5 | Apple Device Certificate Data (Part 6) | 128 | Undefined | Read/write |
| 0x57 | 5 | Apple Device Certificate Data (Part 7) | 128 | Undefined | Read/write |
| 0x58 | 5 | Apple Device Certificate Data (Part 8) | 128 | Undefined | Read/write |

**Note:** Normally, reading register 0x05 will clear it. However, register 0x05 can be read sequentially only as part of a sequence that begins with a register in the range 0x00-0x04, in which case the read operation does not clear it.

**Note:** Registers 0x11 and 0x20 may each be written sequentially with registers 0x12 and 0x21, respectively.

## 3.8.2 Register Descriptions

This section describes the ways that the CP registers listed in Table 3-3 (page 72) are used.

### 3.8.2.1 Device Version

The Device Version read-only register contains the version number of the coprocessor device. The current Authentication 2.0C coprocessor is designated as device version 0x05.

### 3.8.2.2 Firmware Version

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

### 3.8.2.3 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.

### 3.8.2.4 Device ID

The Device ID read-only register is not used by accessories that implement iAP2.

### 3.8.2.5 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 3-4 (page 76).

If a single communication operation happens to produce multiple errors (for example, by writing an invalid challenge response 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.

**Table 3-4** Coprocessor error codes

| Error Code | Description |
|---|---|
| 0x00 | No error |
| 0x01 | Invalid register for read |
| 0x02 | Invalid register for write |
| 0x03 | Invalid challenge response length |
| 0x04 | Invalid challenge length |
| 0x05 | Invalid certificate length |
| 0x06 | Internal process error during challenge response generation |
| 0x07 | Internal process error during challenge generation |
| 0x08 | Internal process error during challenge response verification |
| 0x09 | Internal process error during certificate validation |
| 0x0A | Invalid process control |
| 0x0B | Process control out of sequence |
| 0x0C-0xFF | Reserved |

### 3.8.2.6 Authentication Control and Status

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

When read from, the Authentication Control and Status register provides the status of the most recently requested CP process, as shown in Figure 3-7 (page 76), Table 3-5 (page 77) and Table 3-6 (page 77).

**Figure 3-7** Coprocessor Authentication Control and Status register, read-only bits

**Table 3-5** Coprocessor Authentication ERR_SET values

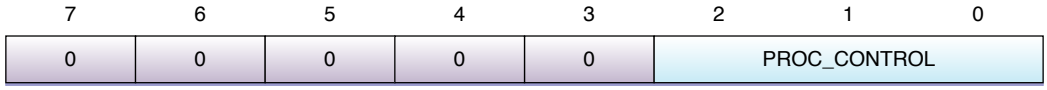
| ERR_SET Value | Description |
|---|---|
| 0 | The Error Code register does not contain a code generated by the most recent command execution. However, it may still contain the most recent error code (greater than 0x00) generated by an earlier command. |
| 1 | The Error Code register contains the most recent process or communication error. Both this bit and the Error Code register contents are cleared after the Error Code register is next read. This bit is also cleared after every successful command execution. |

**Table 3-6** Coprocessor Authentication PROC_RESULTS values

| PROC_RESULTS Value | Description |
|---|---|
| 0 | Most recent process did not produce valid results. |
| 1 | Accessory challenge response successfully generated. |
| 2 | Challenge successfully generated. |
| 3 | Apple device challenge response successfully verified. |
| 4 | Apple device certificate successfully validated. |
| 5-7 | Reserved. |

When written to, the Authentication Control and Status register controls the start of CP processes, as shown in Figure 3-8 (page 77) and Table 3-7 (page 78).

**Figure 3-8** Coprocessor Authentication Control and Status register, write-only bits




**Note:** Attempts to write to other bits in the Coprocessor Authentication Control and Status register are ignored.

**Table 3-7** Coprocessor Authentication PROC_CONTROL values

| PROC_CONTROL Value | Description | Notes |
|---|---|---|
| 0 | No operation | This control does nothing and always reports success (ERR_SET = 0; PROC_RESULTS = 0). |
| 1 | Start new challenge response-generation process | |
| 2 | Start new challenge-generation process | The length of the challenge to be generated is defined by the Challenge Data Length register and ranges from 1 to 128 bytes. |
| 3 | Start new challenge response-verification process | |
| 4 | Start new certificate-validation process | Do not attempt to read the accessory certificate after writing the Apple device certificate but before validating it by this control. |
| 5 | No operation | This control does nothing and always reports success (ERR_SET = 0; PROC_RESULTS = 0). |
| 6-7 | Reserved. | |

### 3.8.2.7 Challenge Response Data Length

The Challenge Response Data Length read/write register holds the length in bytes of the results of the most recent challenge response-generation process (if the Apple device is authenticating an accessory) or challenge response-verification process (if the accessory is authenticating the Apple device).

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

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

### 3.8.2.8 Challenge Response Data

In the case of a challenge response generation process, the Challenge Response Data register holds the newly-generated data. In the case of a challenge response verification process, it holds the challenge response to be verified.

### 3.8.2.9 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 Apple device authentication of an accessory, or generated by the CP during accessory authentication of an Apple device.

Before starting a challenge response-generation process on the current challenge during Apple device authentication of an accessory, this register must contain the length of the challenge.

Before starting a new challenge-generation process during accessory authentication of an Apple device, this register should contain the requested challenge length. The length must be in the range of 1 to 128 bytes, thus writing any other value will cause an error.

The required length of an authentication challenge is 20 bytes.

### 3.8.2.10 Challenge Data

The Challenge Data register holds the current challenge data. This data is either written into the CP or generated by the CP depending on the specific operation. The number of bytes used or generated is determined by the value of the Challenge Length Data register.

### 3.8.2.11 Accessory Certificate Data Length

The Accessory Certificate Data Length read-only register holds the length of the X.509 certificate that the Apple device uses to authenticate an accessory. The length of a certificate varies but is always less than or equal to 1280 bytes. This length limit may not hold for future versions of the authentication protocol.

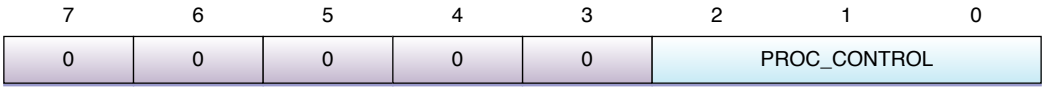
### 3.8.2.12 Accessory Certificate Data

The Accessory Certificate Data read-only register holds the PKCS#7-wrapped X.509 certificate that the Apple device 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.

### 3.8.2.13 Self-Test Control and Status

The Self-Test Control and 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 and Status register initiates a self-test process, as shown in Figure 3-9 (page 80) and Table 3-8 (page 80).

**Figure 3-9** Coprocessor Self-Test Control and Status register, write-only bits




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

**Table 3-8** Coprocessor Self-Test PROC_CONTROL values

| PROC_CONTROL Value | Description |
|---|---|
| 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 and Status register report the results of the X.509 certificate and private key tests, as shown in Figure 3-10 (page 80) and Table 3-9 (page 80). The CP detects a read cycle and resets the Control and Status register to 0x00 after it; hence bits 7-4 must all be retrieved in one operation.

**Figure 3-10** Coprocessor Self-Test Control and Status register, read-only bits


**Table 3-9** Coprocessor Self-Test Results bits

| Self-Test Results Bit | Test | Meaning If 0 | Meaning If 1 |
|---|---|---|---|
| 7 | X.509 Certificate | Certificate not found | Certificate found in memory |
| 6 | Private key | Private key not found | Private key found in memory |
| 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.

### 3.8.2.14 System Event Counter

The System Event Counter (SEC) is a non-volatile register that holds the current value of the CP's event counter. The event counter automatically decrements one count per second while the CP is powered, stopping at 0. If the accessory controls power to the CP, it must wait until the SEC has decremented to 0 before removing power.

### 3.8.2.15 Accessory Certificate Serial Number

The Accessory Certificate Serial Number register holds the serial number of the X.509 certificate that the Apple device uses to authenticate an accessory. The certificate serial number is a null-terminated string, with a maximum length of 31 bytes (inclusive of the null character).

### 3.8.2.16 Apple Device Certificate Data Length

The Apple Device Certificate Data Length register holds the length of the X.509 certificate supplied by the attached Apple device. An accessory uses this certificate to authenticate an Apple device in both the certificate validation and challenge response verification processes. The length of an Apple device 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.

Writing a value in a range greater than 0 and less than or equal to 1024 will cause the CP to validate the data contained in the iPod Certificate Data registers. If the CP invalidates the iPod Certificate Data, it sets this register to 0.

### 3.8.2.17 Apple Device Certificate Data

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

# 3.9 Coprocessor 2.0C I2C Protocol

The Apple Authentication Coprocessor (CP) supports the I2C communication protocol, acting as an I2C slave. Its SCL signal is the I2C clock line and is driven by the accessory. Its SDA signal is the I2C data line and is driven by whichever device is currently sending data.

Unlike the Apple Authentication Coprocessor version 2.0B, CP 2.0C does not perform clock synchronization by stretching SCL. It may, however, not-acknowledge (NACK) a requested register operation if busy, so the I2C master should expect retry operations as a normal part of CP 2.0C use.

The maximum supported I2C clock rate is 400 kHz.

## 3.9.1 Slave Selection and Reset

During reset, the RST signal must specify the CP's I2C slave address and must be held stable for at least 10 *ms* after power-up or reset, as described in I2C Communications Process (page 71). As an I2C slave, the CP is then selected in-band via its I2C address. The least significant bit of the I2C slave address controls whether a write or a read operation is to be performed, as described in Coprocessor 2.0C Address Selection (page 67).

## 3.9.2 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 I2C communication, then the coprocessor is busy. The accessory must repeatedly attempt communication until the coprocessor sends an ACK after receiving its slave address.

## 3.9.3 Writing to the Coprocessor

To write data to the coprocessor, follow these steps:

1. Send the I2C start sequence.
2. Send the I2C write address of the CP.
3. Check for an ACK from the slave; if a NACK is received, wait 500 µ*s* and then loop back to Step 1.
4. Send the register address at which to begin writing.
5. Send the data bytes.
6. Send the I2C stop sequence.

## 3.9.4 Reading from the Coprocessor

To read data from the coprocessor, follow these steps:

1. Send the I2C start sequence.
2. Send the I2C write address of the CP.
3. Check for an ACK from the slave; if a NACK is received, wait 500 µs and then loop back to Step 1.
4. Send the register address at which to begin reading.
5. Optional: send the I2C stop sequence.
6. Send the I2C start sequence.
7. Send the I2C read address of the CP.
8. Check for an ACK from the slave; if a NACK is received, wait 500 µs and then loop back to Step 6.
9. Read the data bytes.
10. Send the I2C stop sequence.

Any additional reads after an I2C 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.

## 3.10 Coprocessor 2.0C Device Characteristics

This section provides technical details and tolerances for the Apple Authentication Coprocessor 2.0C (CP) chip.

### 3.10.1 Physical Configuration

Figure 3-11 (page 84) shows the CP package's layout, pin locations, and dimensional tolerances.

**Figure 3-11** Coprocessor package

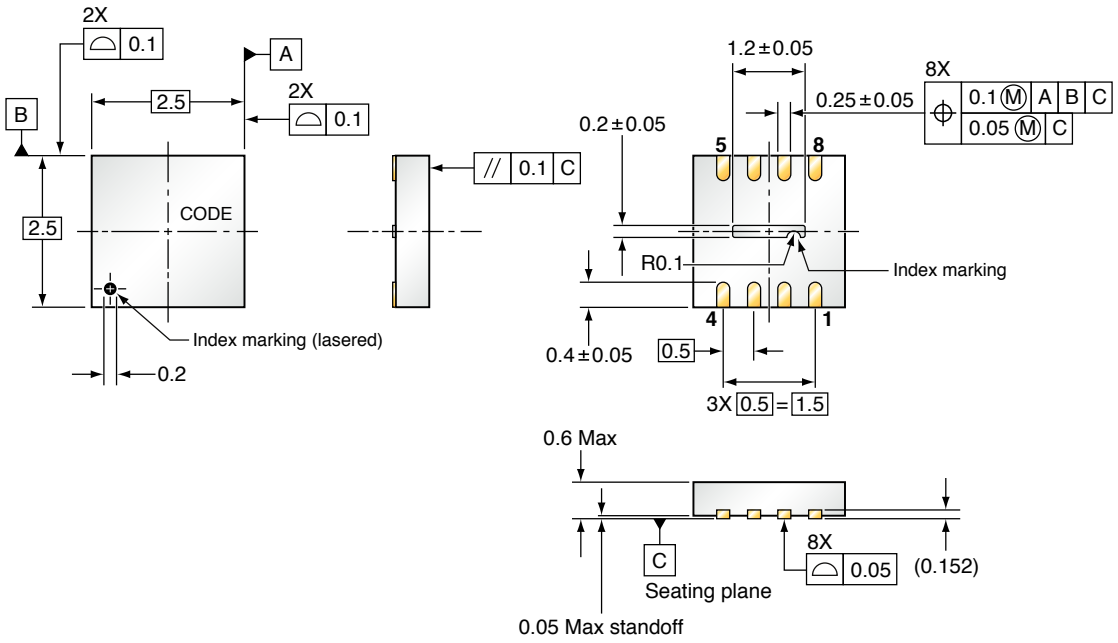



Figure 3-12 (page 85), Figure 3-13 (page 86), Figure 3-14 (page 87), Figure 3-15 (page 88), and Figure 3-16 (page 89) describe how the CP is delivered to accessory manufacturing facilities.

**Figure 3-12** Coprocessor Packing Carrier Tape

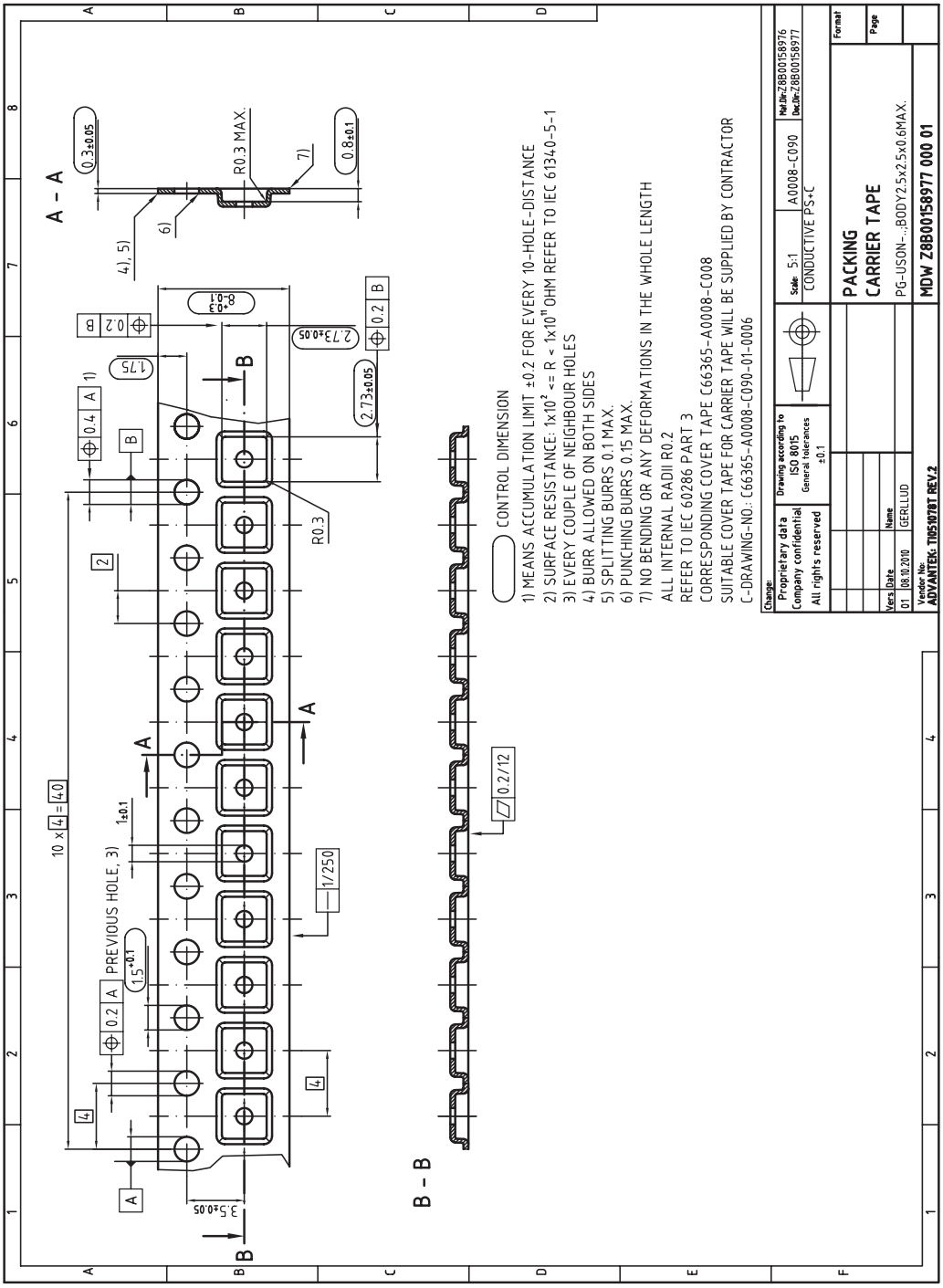


**Figure 3-13** Coprocessor Packing Reel (1,000 unit)

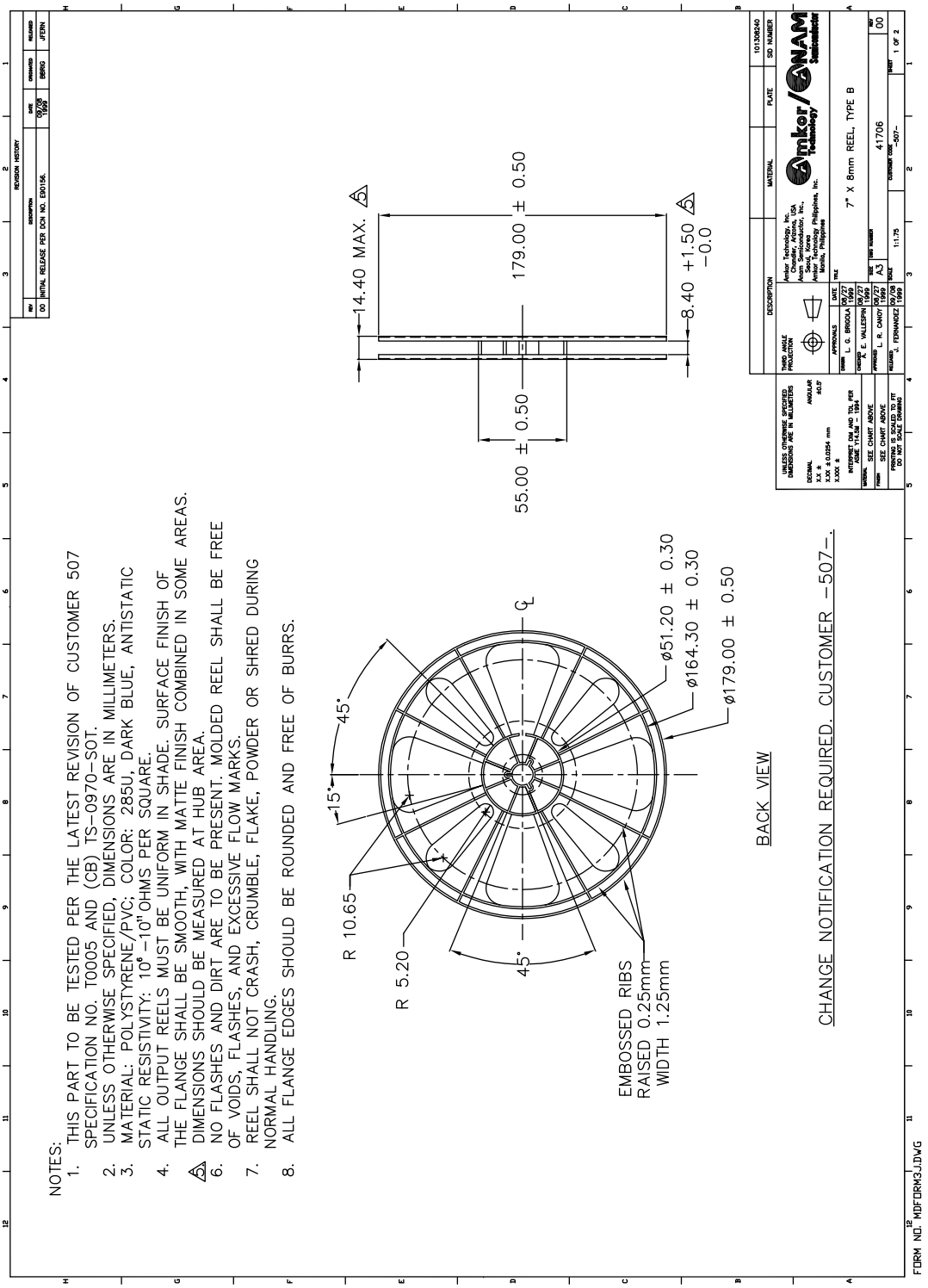


**Figure 3-14** Coprocessor Packing Reel (1,000 unit) details

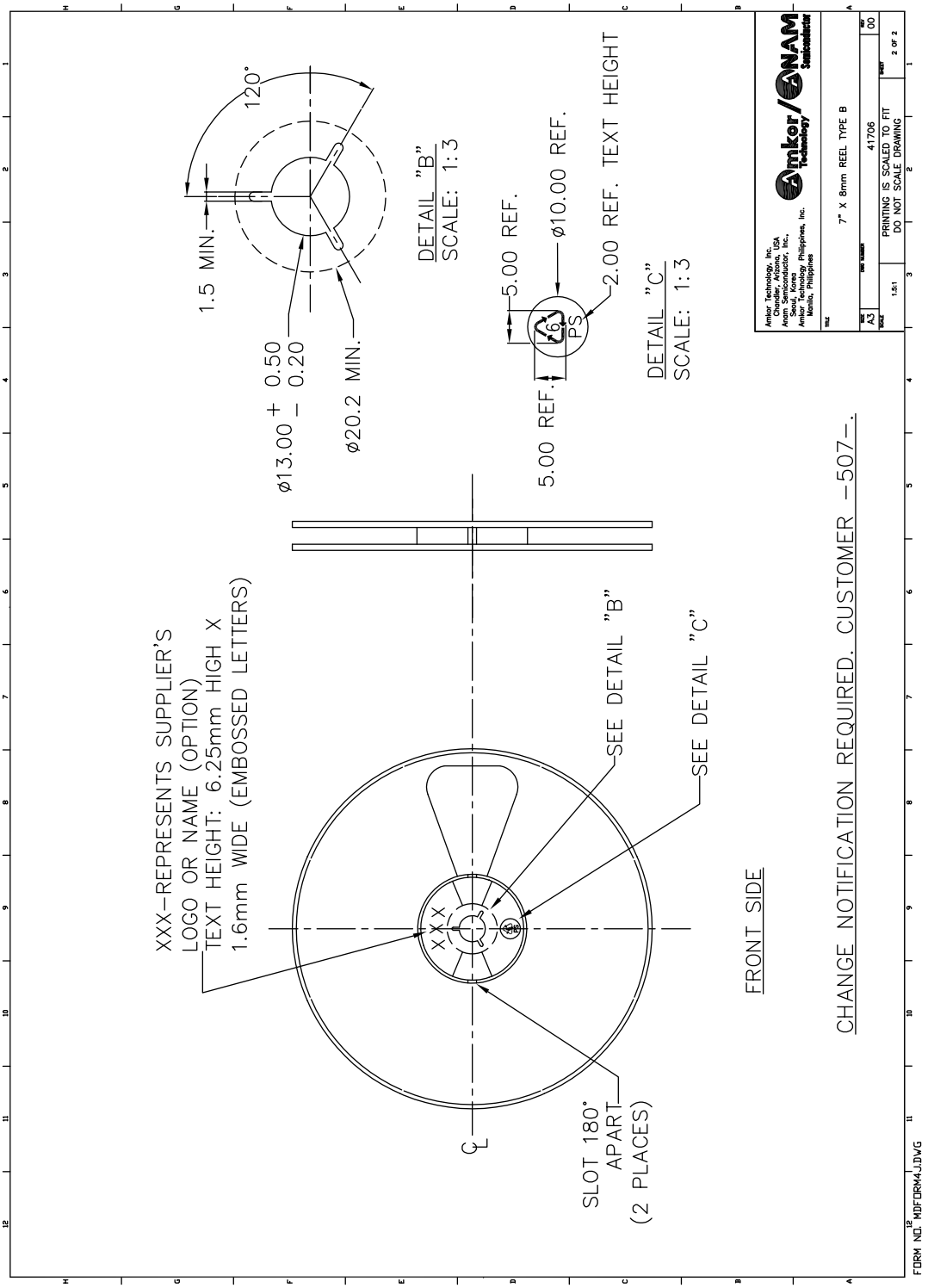


**Figure 3-15** Coprocessor Packing Reel (10,000 unit)

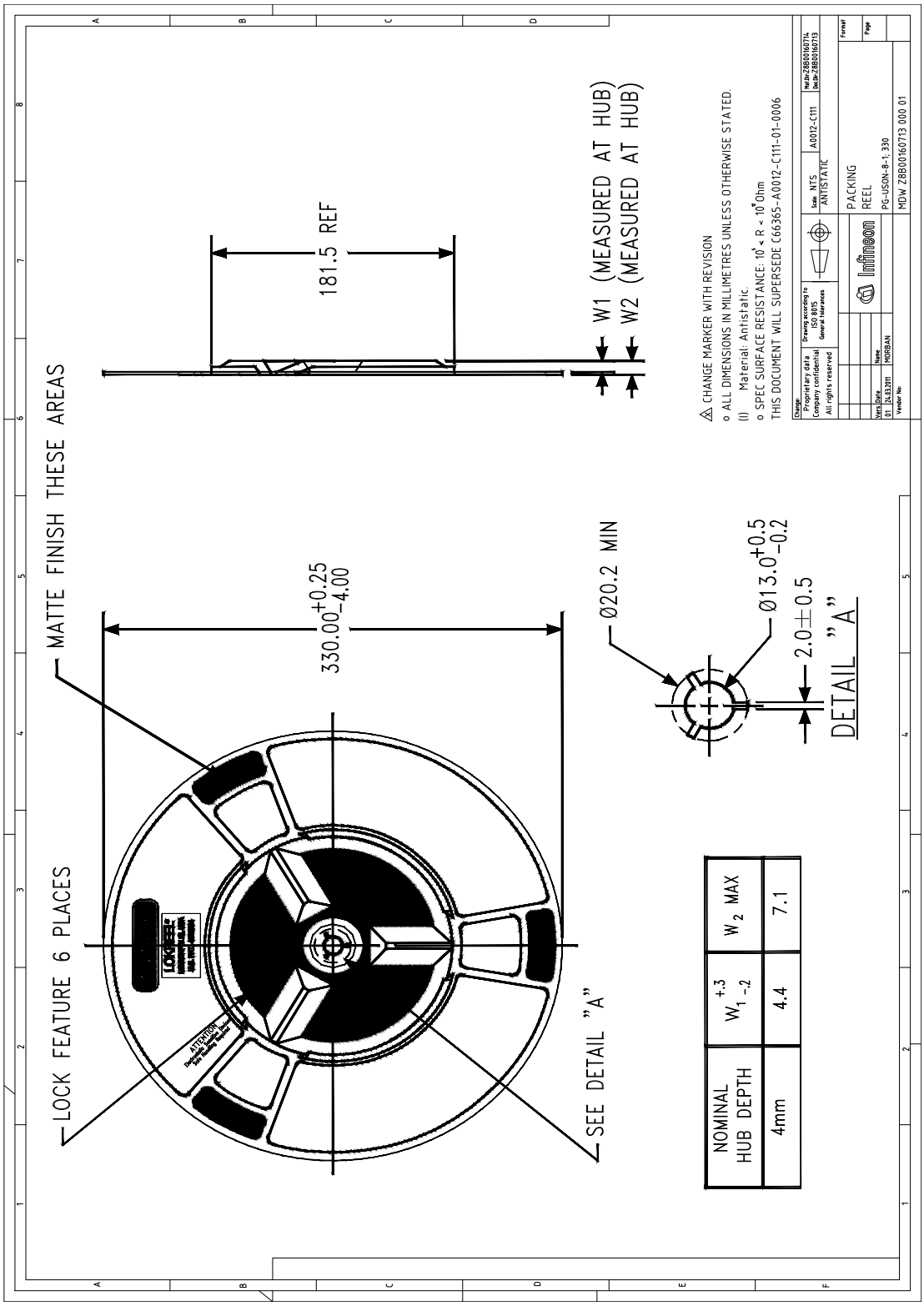
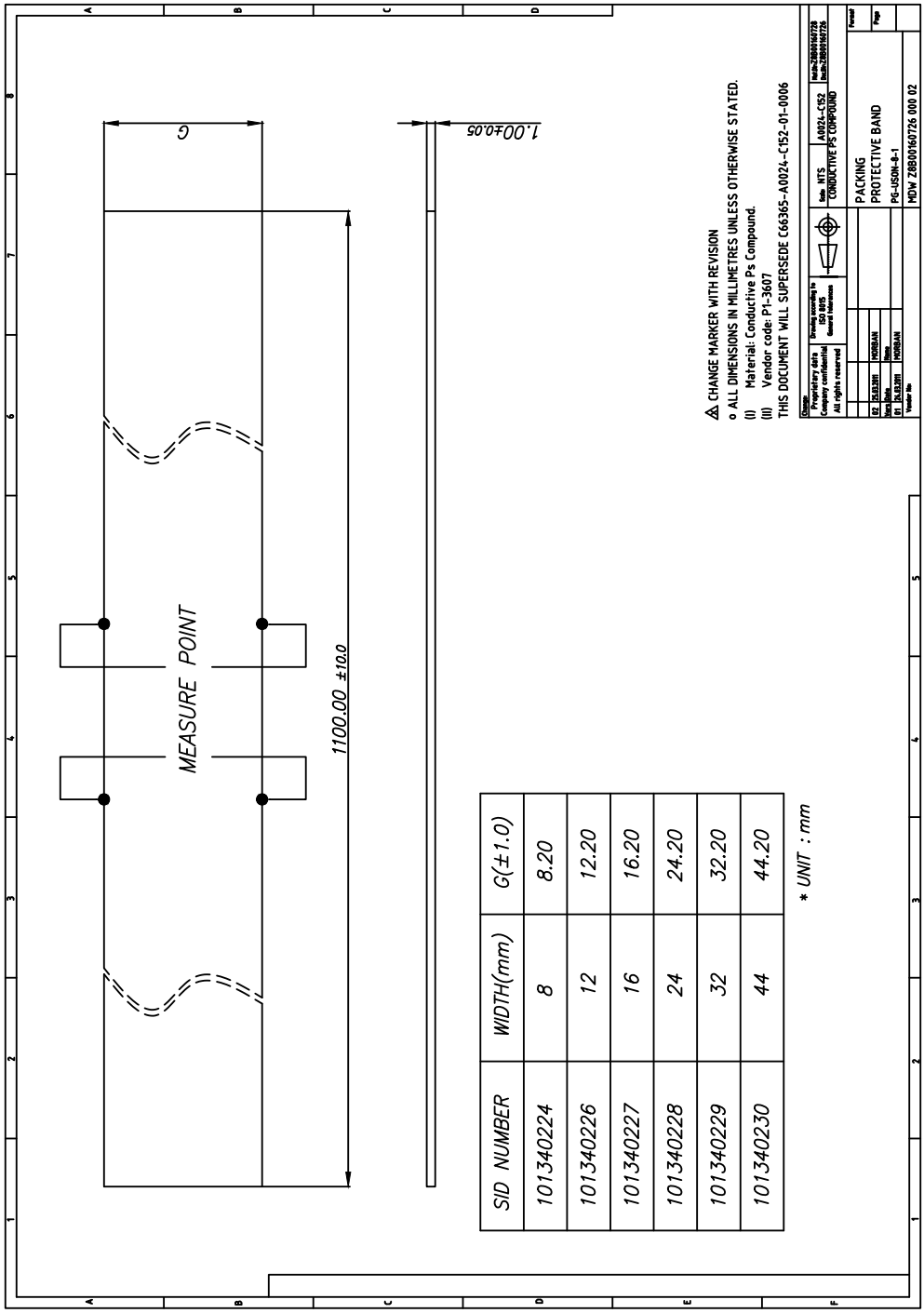


**Figure 3-16** Coprocessor Packing Protective Band




| SID NUMBER | WIDTH(mm) | G(±1.0) |
|---|---|---|
| 101340224 | 8 | 8.20 |
| 101340226 | 12 | 12.20 |
| 101340227 | 16 | 16.20 |
| 101340228 | 24 | 24.20 |
| 101340229 | 32 | 32.20 |
| 101340230 | 44 | 44.20 |

## 3.10.2 Maximum Environmental Conditions

Table 3-10 (page 90) lists the CP's absolute maximum electrical and free-air temperature ranges. Stresses to the CP chip beyond the ranges listed in Table 3-10 (page 90) may cause permanent damage. Exposure to either end of any range for extended periods may affect device reliability.

**Table 3-10** Coprocessor 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 | -40 to +125 °C |

## 3.10.3 Recommended Operating Conditions

The CP is available only in a standard temperature range configuration. Internal sensors may force it to its reset state if any of the conditions listed in Table 3-11 (page 90) are exceeded. Attempting to operate the CP in this state is not recommended and may lead to device failure or unreliability.

**Table 3-11** Coprocessor maximum electrical and temperature ranges

| Condition | Recommended Range |
|---|---|
| Operating free-air temperature | -25 to +85 °C |
| Supply voltage during program execution | 1.62 to 5.5 V |

## 3.10.4 I2C Interface Characteristics

Table 3-12 (page 90) specifies the limits of the I2C interface between the CP and other components.

**Table 3-12** Coprocessor I2C interface characteristics

| Parameter | Required Range |
|---|---|
| SCL clock frequency ($f_{SCL}$) | 10 to 400 kHz |
| External bus capacitance to ground ($C_b$) | Maximum 100 pF |

## 3.10.5 DC Electrical Characteristics

Table 3-13 (page 91), Table 3-14 (page 91) and Table 3-15 (page 91) show the DC electrical characteristics of the CP chip over its recommended voltage and temperature ranges. Unless otherwise specified in these tables, $V_{CC}$ = 1.62 to 5.5 V and $T_A$ = -25 to +85 °C.

**Table 3-13** Coprocessor supply current into $V_{CC}$, excluding external current

| Parameter | Test Conditions | Minimum | Typical | Maximum | Unit |
|---|---|---|---|---|---|
| $I_{(AM)}$ Active mode (authentication process running) | | | 6 | 7.5 | mA |
| $I_{(sleep)}$ Sleep mode | $T_A$ = 25 °C | | 35 | 80 | µA |

**Table 3-14** Coprocessor inputs

| Symbol | Parameter | Minimum | Typical | Maximum | Unit |
|---|---|---|---|---|---|
| $V_{IH}$ | High-level input voltage | $V_{CC} \times 0.7$ | | $V_{CC}$ + 0.3 | V |
| $V_{IL}$ | Low-level input voltage | -0.3 | | $V_{CC} \times 0.2$ | V |
| $I_i$ | Input current | -10 | 1 | 10 | µA |

**Table 3-15** Coprocessor outputs

| Symbol | Parameter | Test Conditions | Minimum | Maximum | Unit |
|---|---|---|---|---|---|
| $V_{OL}$ | Low-level output voltage | $I_{OL(max)}$ = -1 mA | $V_{SS}$ | $V_{SS}$ + 0.4 | V |

## 3.10.6 Timing Characteristics

When power is turned on to the CP, $V_{CC}$ must reach 90% of the CP's target supply voltage within 200 µs after it exceeds 400 mV.

Figure 3-17 (page 92) illustrates the CP's typical I/O port input signal timing and voltage limits. Table 3-16 (page 92) lists the parameter values in Figure 3-17 (page 92).

**Figure 3-17** Coprocessor typical I/O port input waveform

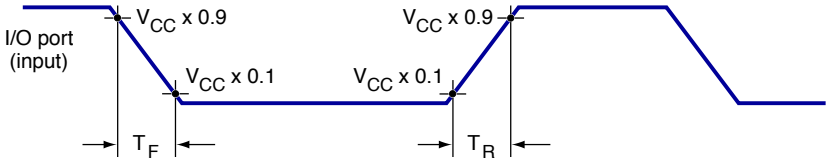



**Table 3-16** Coprocessor Values for typical I/O port input waveform

| Symbol | Description | Maximum Value |
|---|---|---|
| $T_F$ | Fall time | 1.0 µs |
| $T_R$ | Rise time | 1.0 µs |